Boundedness results for 2-adic Galois images associated to hyperelliptic Jacobians

Jeffrey Yelton

Mathematics & Science Center, Emory University, Atlanta, Georgia 30322, United States

Correspondence
Jeffrey Yelton, Mathematics, and Science Center, Emory University, Atlanta, Georgia 30322, United States.
Email: jeffrey.yelton@emory.edu

Abstract
Let $K$ be a number field, and let $C$ be a hyperelliptic curve over $K$ with Jacobian $J$. Suppose that $C$ is defined by an equation of the form $y^2 = f(x)(x - \lambda)$ for some irreducible monic polynomial $f \in \mathcal{O}_K[x]$ of discriminant $\Delta$ and some element $\lambda \in \mathcal{O}_K$. Our first main result says that if there is a prime $\mathfrak{p}$ of $K$ dividing $(f(\lambda))$ but not $(2\Delta)$, then the image of the natural 2-adic Galois representation is open in $\text{GSp} (T_2(J))$ and contains a certain congruence subgroup of $\text{Sp} (T_2(J))$ depending on the maximal power of $\mathfrak{p}$ dividing $(f(\lambda))$. We also present and prove a variant of this result that applies when $C$ is defined by an equation of the form $y^2 = f(x)(x - \lambda)(x - \lambda')$ for distinct elements $\lambda, \lambda' \in K$. We then show that the hypothesis in the former statement holds for almost all $\lambda \in \mathcal{O}_K$ and prove a quantitative form of a uniform boundedness result of Cadoret and Tamagawa.

KEYWORDS
hyperelliptic curves, $\ell$-adic Galois representations, monodromy actions

MSC (2020)
14G20, 20G25, 14H30, 14K15

1 INTRODUCTION

Let $K$ be a number field with absolute Galois group $G_K$, and let $C$ be a hyperelliptic curve defined over $K$; i.e. $C$ is a smooth projective curve defined by an equation of the form $y^2 = f(x)$ for some squarefree polynomial $f$ of degree $d \geq 3$. (Note that in the case of $d = 3$, $C$ is an elliptic curve.) It is well known that the genus of $C$ is given by $g = \lfloor (d + 1)/2 \rfloor$. We denote the Jacobian variety of $C$ by $J$; it is an abelian variety of dimension $g$. For each prime $\ell$, we let $T_\ell(J)$ denote the $\ell$-adic Tate module of $J$, which is a free $\mathbb{Z}_\ell$-module of rank $2g$. We write $\rho_\ell : G_K \to \text{Aut} (T_\ell(J))$ for the natural $\ell$-adic Galois action on this Tate module. The Tate module $T_\ell(J)$ is endowed with the Weil pairing defined with respect to the canonical principal polarization on $J$, which we write as $e_\ell : T_\ell(J) \times T_\ell(J) \to \mathbb{Z}_\ell$; it is a $\mathbb{Z}_\ell$-bilinear skew-symmetric pairing. Let $\text{Sp} (T_\ell(J))$ denote the group of symplectic automorphisms of $T_\ell(J)$ with respect to the pairing $e_\ell$, and let

$$\text{GSp} (T_\ell(J)) := \{ \sigma \in \text{Aut}_{\mathbb{Z}_\ell} (T_\ell(J)) \mid e_\ell (P^\sigma, Q^\sigma) = \chi_\ell (\sigma) e_\ell (P, Q) \forall P, Q \in T_\ell(J) \}$$

denote the group of symplectic similitudes, where $\chi_\ell : G_K \to \mathbb{Z}_\ell^\times$ is the $\ell$-adic cyclotomic character.

It is well known that the image $G_\ell$ of $\rho_\ell$ is always a closed subgroup of $\text{GSp} (T_\ell(J))$ and that in fact there is some hyperelliptic Jacobian $J$ of a given dimension $g$ such that the inclusion $G_\ell \subseteq \text{GSp} (T_\ell(J))$ has finite index (or equivalently,
that \( G_\ell \) is an open subgroup of the \( \ell \)-adic Lie group \( GSp(T_\ell(J)) \); see for instance \([20, \text{Theorem 1.1}]\). Note that the subgroup \( G_\ell \cap \text{Sp}(T_\ell(J)) \subset G_\ell \) coincides with the image of the Galois subgroup which fixes the extension obtained by adjoining all \( \ell \)-power roots of unity to \( K \). By \([4, \text{Theorem 3}]\), the Lie algebra of \( G_\ell \) contains the subalgebra of homotheties in the Lie algebra of \( GSp(T_\ell(J)) \); it follows that \( G_\ell \) has finite index in \( GSp(T_\ell(J)) \) if and only if \( G_\ell \cap \text{Sp}(T_\ell(J)) \) has finite index in \( \text{Sp}(T_\ell(J)) \).

There have been many results stating that \( G_\ell \) has finite index in \( GSp(T_\ell(J)) \) under various hypotheses for the polynomial defining the hyperelliptic curve. For instance, Y. Zarhin has proven this for large enough genus in the case of hyperelliptic curves defined by equations of the form \( y^2 = f(x)(x - \lambda) \) with \( \lambda \in K \), where the Galois group of \( f \) is the full symmetric or alternating group \([21, \text{Theorem 2.5}] \) and \([22, \text{Theorem 8.3}] \); see also \([23, \text{Theorem 1.3}] \) for a variant of this where the curve is defined using two parameters). A. Cadoret and A. Tamagawa have also proven \([6, \text{Theorems 1.1 and 5.1}] \) that for any family of hyperelliptic Jacobians over a smooth, geometrically connected, separated curve over \( K \), this openness condition will be satisfied for the \( \ell \)-adic Galois action associated to the fibers over all but finitely many of the \( K \)-points of the base, and that in fact the indices of the \( \ell \)-adic Galois images corresponding to these fibers are uniformly bounded. However, there have been very few results which give explicit bounds for the index of \( G_\ell \) in \( GSp(T_\ell(J)) \) in such cases.

Our aim in this paper is to give some similar results on the openness of the \( \ell \)-adic Galois images in the group of symplectic similitudes associated to Jacobians of hyperelliptic curves whose defining polynomials satisfy certain hypotheses, and to provide formulas giving explicit bounds for the indices of the 2-adic Galois images in these cases. (Unfortunately, our method currently cannot give us explicit bounds for the indices of the \( \ell \)-adic Galois images for odd primes \( \ell \).)

We state our main results below. In these statements as well as in the rest of the paper, we use the following notation. For any integer \( N \geq 1 \), we denote the level-\( N \) congruence subgroup of \( \text{Sp}(T_2(J)) \) by \( \Gamma(N) := \{ \sigma \in \text{Sp}(T_2(J)) \mid \sigma \equiv 1 \pmod{N} \} \). We denote the ring of integers of a number field \( K \) by \( \mathcal{O}_K \). Finally, we write \( v_2 : \mathbb{Q}^\times \to \mathbb{Z} \) for the (normalized) 2-adic valuation on \( \mathbb{Q} \).

**Theorem 1.1.** Let \( K \) be a number field, and let \( f \in \mathcal{O}_K[x] \) be an irreducible monic polynomial of degree \( d \geq 2 \) with discriminant \( \Delta \). Let \( J \) be the Jacobian of the hyperelliptic curve with defining equation \( y^2 = f(x)(x - \lambda) \) for some \( \lambda \in \mathcal{O}_K \), and define the \( \ell \)-adic Galois images \( G_\ell \) as above. Suppose that there is a prime \( \mathfrak{p} \) of \( \mathcal{O}_K \) which divides \( (f(\lambda)) \) but not \((2\Delta)\).

a) The Lie subgroup \( G_\ell \subset GSp(T_\ell(J)) \) is open for all \( \ell \) different from the residue characteristic of \( \mathfrak{p} \). In particular, the Lie subgroup \( G_2 \subset GSp(T_2(J)) \) is open.

b) We have \( G_2 \cap \text{Sp}(T_2(J)) \supseteq \Gamma(2^{v_2(m)+2}) \), where \( m \geq 1 \) is the greatest integer such that \( \mathfrak{p}^m \mid (f(\lambda)) \). In addition \( d = 3 \), then \( G_2 \cap \text{Sp}(T_2(J)) \supseteq \Gamma(2^{v_2(m)+1}) \).

**Theorem 1.2.** Assume the same notation as in the statement of \( \text{Theorem 1.1} \), except that the defining equation of the hyperelliptic curve is \( y^2 = f(x)(x - \lambda)(x - \lambda') \) for distinct elements \( \lambda, \lambda' \in \mathcal{O}_K \). Suppose that there is a prime \( \mathfrak{p} \) of \( \mathcal{O}_K \) which divides \( (f(\lambda)) \) but not \((\lambda - \lambda') \) or \((2\Delta)\) and a prime \( \mathfrak{p}' \) which divides \( (\lambda - \lambda') \) but not \((f(\lambda)) \) or \((2\Delta)\).

a) The Lie subgroup \( G_\ell \subset GSp(T_\ell(J)) \) is open for all \( \ell \) different from the residue characteristics of \( \mathfrak{p} \) and \( \mathfrak{p}' \). In particular, the Lie subgroup \( G_2 \subset GSp(T_2(J)) \) is open.

b) We have \( G_2 \cap \text{Sp}(T_2(J)) \supseteq \Gamma(2^{v_2(m)+2}) \) if \( v_2(m') \leq v_2(m) \) or \( d = 2g \) and \( G_2 \cap \text{Sp}(T_2(J)) \supseteq \Gamma(2^{v_2(m)+v_2(m')}) \) otherwise, where \( m \geq 1 \) is the greatest integer such that \( \mathfrak{p}^m \mid (f(\lambda)) \) and \( m' \geq 1 \) is the greatest integer such that \( \mathfrak{p}'^{m'} \mid (\lambda - \lambda') \). In addition \( d = 2 \), then \( G_2 \cap \text{Sp}(T_2(J)) \supseteq \Gamma(2^{v_2(m)+v_2(m')} \cdot 2^{v_2(m')}) \).

**Remark 1.3.** For a fixed irreducible monic polynomial \( f \in \mathcal{O}_K[x] \) of degree \( d \geq 2 \) with discriminant \( \Delta \), it is not hard to show using Faltings' theorem that the hypothesis in Theorems 1.1 is satisfied for almost all \( \lambda \in \mathcal{O}_K \) (in \( \S 5 \), we will prove in a similar fashion that it is satisfied for almost all \( \lambda \in K \) if \( d \geq 4 \)). It follows immediately that there are also infinitely many choices of \( (\lambda, \lambda') \in K \times K \) satisfying the hypotheses in Theorem 1.2 for this polynomial \( f \).

**Corollary 1.4.** If \( J \) is the Jacobian of a hyperelliptic curve satisfying the hypotheses of Theorem 1.1 or 1.2, then its endomorphism ring \( \text{End}(J) \) coincides with \( \mathbb{Z} \). In particular, such a Jacobian \( J \) is absolutely simple.
Proof. It is known that there is a finite algebraic extension $K'$ of $K$ over which every endomorphism of an abelian variety over a field $K$ is defined (see [17, Theorem 2.4]), so that each endomorphism in $\text{End}(J)$ commutes with the action of $\text{Gal}(K/K')$ on torsion points. The corollary now follows from noting that the only endomorphisms in $\text{End}(T_{\ell'}(J))$ which commute with everything in an open subgroup of $\text{GSp}(T_{\ell'}(J))$ are scalars. \hfill \Box

The key ingredient used in proving the above theorems is a method of describing Galois actions on $\ell'$-adic Tate modules of hyperelliptic Jacobians defined over the fraction field of a strictly Henselian DVR of residue characteristic $p \neq 2$, $\ell'$ by looking at the valuations of the differences between the roots of the defining polynomial, which is derived from results shown in joint work with H. Hasson ([9]). This way of looking at $\ell'$-adic Galois actions associated to hyperelliptic Jacobians over local fields is very similar to the “method of clusters” used by S. Anni and V. Dokchitser in [1]. Our approach seems quite powerful and should lead to many similar boundedness results in a number of situations where one can compute valuations of the differences between the roots of the defining polynomial with respect to various primes of the ground field. Unfortunately, in practice, these valuations (or even the roots themselves) may be difficult to calculate, and so our main focus here is on obtaining results such as the ones stated above where the hypotheses are very easy to verify.

The rest of this paper is organized as follows. In §2, we use the main results of [9], which show that over the fraction field of a strictly Henselian DVR of characteristic $p \neq 2$, for primes $\ell' \neq p$, the $\ell'$-adic Galois action factors through the tame quotient of the absolute Galois group and can be described in terms of Dehn twists with respect to certain loops on a complex hyperelliptic curve. In particular cases such as when exactly two roots of the defining polynomial coalesce in the reduction over the residue field, we will show (Proposition 2.6) that such a Dehn twist induces a transvection in the symplectic group. We will later put local data together to show that over a number field $K$, the $\ell'$-adic Galois image contains certain powers of several sufficiently “independent” transvections. In §3, we will demonstrate using elementary matrix algebra that the group generated by these powers of transvections is “large” and, in the $\ell' = 2$ case, contains a certain congruence subgroup. In §4, we will use what we have shown in §2 and §3 to prove Theorems 1.1 and 1.2 as well as to prove an auxiliary result that applies to a more general situation (Theorem 4.1). In §5, we will show using Theorem 1.1 that for a given $f \in \mathcal{O}_K[x]$ of degree $d \geq 3$, the 2-adic Galois image associated to the hyperelliptic curves defined by $y^2 = f(x)(x - \lambda)$ for all but finitely many $\lambda \in \mathcal{O}_K$ contains a principal congruence subgroup which depends only on $d$ (Theorem 5.1). In fact, for $d \geq 4$ even, in Theorem 5.1(c) we will provide a uniform bound for indices of the 2-adic Galois images associated to almost all fibers of such a one-parameter family over the $K$-line, as is guaranteed by [6, Theorems 1.1 and 5.1]. Finally, in §6, we will describe an alternate approach to proving the key Proposition 2.6 from §2 in the case that $\ell' = 2$.

The author is grateful to a MathOverflow user whose comment on question 264281 helped to inspire the arguments for the results in §5. The author would also like to thank the referee of an earlier version of this article, for a suggestion which has allowed him to remove an earlier hypothesis on the class number of $K$ from the statements of the results in §5. The author would also like to thank another referee who provided an enlightening strategy for the proof of (an alternate formulation of) Proposition 2.6, which is now described in §6.

### 2 HYPERELLIPTIC JACOBIANS OVER LOCAL FIELDS AND TAME GALOIS ACTIONS

We retain all notation introduced in the previous section. In this section, we write $\hat{\mathbb{Z}}$ for the profinite completion of $\mathbb{Z}$ and use the symbol $\hat{\pi}$ to denote the profinite completion of the fundamental group of a topological space. For any profinite group $G$, we write $G^{(p')}$ for its maximal prime-to-$p$ quotient. Note that since $G^{(p')}$ is a characteristic quotient of $G$, any action on $G$ induces an action on $G^{(p')}$. Now we choose a prime $p$ of $K$ of residue characteristic $p \neq 2$. Fix a strict Henselization of the localization of $K$ at the prime $p$ and denote it by $R_p$ and its fraction field by $\mathcal{K}_p$; this comes with an embedding $\mathcal{K}_p \hookrightarrow \hat{K}$. Let $\pi \in K$ be a uniformizer of the discrete valuation ring $R_p$. We fix a compatible system of $N$th roots of unity $\zeta_N \in \hat{K}$ for $N = 1, 2, 3, \ldots$; that is, we require that $\zeta_N^{N'} = \zeta_N$ for any integers $N, N' \geq 1$. Note that since $R$ is strictly Henselian, $\zeta_N \in R \subset K$ for any $N$ not divisible by $p$. Let $G^{\text{tame}}_{K,p}$ denote the absolute Galois group of $\mathcal{K}_p$, and let $G^{\text{tame}}_{K,p}$ denote its tame quotient. It follows from a special case of Abhyankar’s lemma that the maximal tamely ramified extension $\mathcal{K}_p^{\text{tame}}$ is given by $\mathcal{K}_p \left( \left( \pi^{1/N} \right)_{(N,p)=1} \right)$, where $\pi^{1/N}$ denotes an $N$th root of $\pi$, and that $G^{\text{tame}}_{K,p} \simeq \hat{\mathbb{Z}}^{(p')}$ is topologically generated by the automorphism which acts on $K^{\text{tame}}$ by fixing $K$ and sending each $\pi^{1/N}$ to $\zeta_N \pi^{1/N}$. 


We fix, once and for all, an embedding $K \hookrightarrow \mathbb{C}$ where $\xi_N$ is sent to $e^{2\pi i/N}$ for $N \geq 1$, so that we have an inclusion $\mathcal{K}_p \subset \mathbb{C}$. Let $d \geq 2$ be an integer and choose distinct integral elements $\alpha_1, \ldots, \alpha_d \in K$. Choose polynomials $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_d \in \mathbb{C}[x]$ satisfying $\tilde{\alpha}_i(\pi) = \pi$ for $1 \leq i \leq d$ and such that the $x$-adic valuation of $\tilde{\alpha}_i$ and $\tilde{\alpha}_j$ and the $\pi$-adic valuation of $\alpha_i$ and $\alpha_j$ are equal (such polynomials exist, as is shown in the discussion in [9, §3.3]). Let $\varepsilon > 0$ be a real number small enough that $\tilde{\alpha}_i(z) \neq \tilde{\alpha}_j(z)$ for all $i \neq j$ and for all $z \in B^*_z := \{z \in \mathbb{C} \mid |z| < \varepsilon\} \setminus \{0\}$. We define a family $F \to B^*_z$ of $d$-times-punctured Riemann spheres by letting

$$F = \mathbb{P}^1 \times B^*_z \setminus \bigcup_{i=1}^{d} \{(\tilde{\alpha}_i(z), z) \mid z \in B^*_z\}.$$  

Choose a basepoint $z_0 \in B^*_z$. The fundamental group $\pi_1(B^*_z, z_0)$ acts by monodromy on the fundamental group $\pi_1(F_{z_0}, \infty)$ of the fiber over $z_0$ with basepoint $\infty$. We write $\rho_{\text{top}} : \pi_1(B^*_z, z_0) \to \text{Aut}(\pi_1(F_{z_0}, \infty))$ for this action. The action $\rho_{\text{top}}$ extends uniquely to a continuous action of the profinite completion $\tilde{\pi}_1(B^*_z, z_0)$ on the profinite completion $\tilde{\pi}_1(F_{z_0}, \infty)$ (see the discussion in [9, §1.1]), which we also denote by $\rho_{\text{top}}$. We note that $\tilde{\pi}_1(B^*_z, z_0)$ is isomorphic to $\hat{\mathbb{Z}}$ and is topologically generated by the element $\delta \in \pi_1(B^*_z, z_0)$ represented by the loop given by $t \mapsto e^{2\pi \sqrt{-1}t}z_0$ for $t \in [0, 1]$.

Meanwhile, the absolute Galois group $G_{K, p}$ acts naturally by conjugation on the étale fundamental group $\pi^\text{et}_1\left(\mathbb{P}^1_k \setminus \{\alpha_1, \ldots, \alpha_d\}, \infty\right)$ via the $\mathcal{K}_p$-point lying under the geometric point $\infty : \text{Spec}(\mathbb{C}) \to \mathbb{P}^1_k \setminus \{\alpha_1, \ldots, \alpha_d\}$. After identifying $\pi^\text{et}_1\left(\mathbb{P}^1_k \setminus \{\alpha_1, \ldots, \alpha_d\}, \infty\right)^{(p')}$ with $\tilde{\pi}_1\left(\mathbb{P}^1_{\mathbb{C}} \setminus \{\alpha_1, \ldots, \alpha_d\}, \infty\right)^{(p')}$ via Riemann’s Existence Theorem and the inclusion of algebraically closed fields $\mathcal{K}_p \subset \mathbb{C}$, we write $\rho_{\text{alg}} : G_{K, p} \to \text{Aut}\left(\tilde{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{\alpha_1, \ldots, \alpha_d\}, \infty)^{(p')}\right)$ for this action.

We denote the actions on prime-to-$p$ quotients of étale fundamental groups induced by $\rho_{\text{top}}$ and $\rho_{\text{alg}}$ by $\rho_{\text{top}}^{(p')}$ and $\rho_{\text{alg}}^{(p')}$ respectively.

For the statement of Theorem 2.1(a) below, we require the terminology of Dehn twists. Let $\gamma : [0, 1] \to M$ be a simple loop on any complex manifold $M$; we will often identify $\gamma$ with its image in $M$. We define the Dehn twist on $M$ with respect to the loop $\gamma$. It is an element of the mapping class group of $M$ represented by a self-homeomorphism of $M$ which can be visualized in terms of a small tubular neighborhood of $\gamma \subset M$, in the following way: the Dehn twist keeps the outer edge of the tubular neighborhood fixed while twisting the inner edge for one full rotation counterclockwise and acts as the identity everywhere else on $M$. Since this Dehn twist depends only on the homology class $[\gamma] \in H_1(M, \mathbb{Z})$ of any loop $\gamma$, we will denote it by $D_{\gamma, 1}$. (See [7, Chapter 3] for more details.)

The following theorem is a compilation of all the necessary results describing and comparing $\rho_{\text{top}}$ and $\rho_{\text{alg}}$ that are proven in [9, Theorems 1.2 and 2.4 and Remark 4.11].

**Theorem 2.1.** In the above situation, we have the following.

a) Let $I$ be the set of all pairs $(I, n)$ where $I \subseteq \{1, \ldots, d\}$ is a subset and $n \geq 1$ is an integer such that $x^n | \tilde{\alpha}_i - \tilde{\alpha}_j \in \mathbb{C}[x]$ for all $i, j \in I$ and such that $I$ is maximal among profinite sets with this property. If $\varepsilon$ is small enough, there exist pairwise nonintersecting loops $\gamma_{I, n} : [0, 1] \to F_{z_0} \setminus \{\infty\}$ for each $(I, n) \in I$ such that $\delta \in \pi_1(B^*_z, z_0)$ acts on $\pi_1(F_{z_0}, \infty)$ in the same way that the product $\prod_{(I, n) \in I} D_{\gamma_{I, n}}$ of Dehn twists on $F_{z_0} \setminus \{\infty\}$ does. These loops $\gamma_{I, n}$ each have the property of separating the subset $\{\tilde{\alpha}_i(z_0)\}_{i \in I}$ from its complement in $\{\tilde{\alpha}_j(z_0)\}_{j \neq I} \cup \{\infty\}$, and two such loops $\gamma_{I, n}$ and $\gamma_{I', n'}$ are homologous if and only if $I = I'$.

b) The actions $\rho_{\text{top}}^{(p')}$ and $\rho_{\text{alg}}^{(p')}$ factor through $\pi_1(B^*_z, z_0)^{(p')}$ and $G_{k, p}^{\text{tame}}$ respectively.

c) We have isomorphisms $\tilde{\pi}_1(B^*_z, z_0)^{(p')} \cong G_{k, p}^{\text{tame}}$ and $\phi : \tilde{\pi}_1(F_{z_0}, \infty)^{(p')} \cong \tilde{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{\alpha_1, \ldots, \alpha_d\}, \infty)^{(p')}$ inducing an isomorphism of the actions $\rho_{\text{top}}^{(p')}$ and $\rho_{\text{alg}}^{(p')}$. Moreover, we can choose the isomorphism $\phi$ so that it takes any element represented by a loop on $F_{z_0}$ separating some singleton $\{\tilde{\alpha}_i(z_0)\}$ from its complement in $\{\tilde{\alpha}_j(z_0)\}_{j \neq I} \cup \{\infty\}$ to an element represented by a loop on $\mathbb{P}^1_{\mathbb{C}} \setminus \{\alpha_1, \ldots, \alpha_d\}$ separating the singleton $\{\alpha_i\}$ from its complement in $\{\alpha_j\}_{j \neq I} \cup \{\infty\}$.

In other words, the prime-to-$p$ monodromy action $\rho_{\text{top}}^{(p')}$ can be described in terms of Dehn twists with respect to loops surrounding certain subsets of the removed points which coalesce at a certain rate as one approaches the center of $B^*_z$;
moreover, this is isomorphic to the algebraic action $\rho^{(p')}_{alg}$ via an isomorphism of prime-to-$p$ étale fundamental groups which takes the image of a loop wrapping around a given $a_i(z_0)$ to the image of a loop wrapping around $a_i$.

We now want to relate this to the action of $G_{K,p}$ on the prime-to-$p$ étale fundamental group of a smooth hyperelliptic curve over $\mathcal{K}_p$. Let $\mathcal{C}$ be a smooth, projective hyperelliptic curve over $\mathbb{C}$ of degree $d$ and genus $g$ defined by an equation of the form $y^2 = \prod_{i=1}^{d} (x - z_i)$ for distinct roots $z_i \in \mathcal{K}_p$; if $d$ is odd (resp. even), then $d = 2g + 1$ (resp. $d = 2g + 2$). The hyperelliptic curve $\mathcal{C}$ comes with a surjective degree-2 morphism $\mathcal{C} \to \mathbb{P}^1_{\mathbb{C}}$ defined by projecting onto the $x$-coordinate. It is well known that this projection ramifies at infinity if and only if $d = 2g + 1$; in this case, we write $z_{2g+2} = \infty$. Then the projection is ramified at exactly the $(2g + 2)$-element set of $z_i$’s. We denote this subset by $\mathcal{B} \subset \mathbb{P}^1_{\mathbb{C}}$, and by abuse of notation we also write $\mathcal{B} \subset \mathcal{C}(\mathbb{C})$ for the set of inverse images of these ramification points (the set is called the branch points of $\mathcal{C}$). Clearly the restriction to $\mathcal{C}\setminus \mathcal{B}$ of the above projection map yields a finite degree-2 étale morphism $\mathcal{C}\setminus \mathcal{B} \to \mathbb{P}^1_{\mathbb{C}}$. Choose a basepoint $P$ of the topological space $\mathbb{P}^1_{\mathbb{C}} \setminus \mathcal{B}$ and a basepoint $Q$ of the topological space $\mathcal{C}(\mathbb{C})\setminus \mathcal{B}$ such that $Q$ lies in the inverse image of $P$. Then after making identifications via Riemann’s Existence Theorem, we get an inclusion and surjections

$$\hat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \setminus \mathcal{B}, P) \supset \hat{\pi}_1(\mathcal{C}(\mathbb{C}) \setminus \mathcal{B}, Q) \twoheadrightarrow \hat{\pi}_1(\mathcal{C}(\mathbb{C}), Q) \twoheadrightarrow H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \otimes \hat{\mathbb{Z}}$$

(2.1)

induced by the maps $\mathbb{P}^1_{\mathbb{C}} \setminus \mathcal{B} \leftarrow \mathcal{C}(\mathbb{C}) \setminus \mathcal{B} \leftarrow \mathcal{C}(\mathbb{C})$ and by identifying the first singular homology group of $\mathcal{C}(\mathbb{C})$ with the abelianization of its fundamental group. The inclusion in (2.1) is an inclusion of a characteristic subgroup, so any automorphism of $\hat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \setminus \mathcal{B}, P)$ induces an automorphism of $\hat{\pi}_1(\mathcal{C}(\mathbb{C}) \setminus \mathcal{B}, P)$.

We write $\mathfrak{F}$ for the Jacobian of $\mathcal{C}$. There is a well-known identification of $H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell$ with $H_1(\mathfrak{F}(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell$ and in turn with $T_\ell(\mathfrak{F})$ for any prime $\ell$. Moreover, the intersection pairing on $H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z})$ defined above carries over to the canonical Riemann form on the complex abelian variety $\mathfrak{F}(\mathbb{C})$ and in turn to the Weil pairing $e_\ell$ on $T_\ell(\mathfrak{F})$ (see the results in [10, §IV.4 and §VIII.1] and in [12, §24]). Given an element $c \in H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z})$, we also write $c$ for the element $c \otimes 1 \in H_1(\mathfrak{F}(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell = T_\ell(\mathfrak{F})$. It is not difficult to show that the action of $G_{K,p}$ on $T_\ell(\mathfrak{F})$ induced by $\rho^{(p')}_{alg}$ via these identifications is the natural $\ell$-adic Galois action $\rho_\ell$; see, for instance, step 5 of the proof of [20, Proposition 2.2].

Definition 2.2. Given any complex hyperelliptic curve $\mathcal{C}$ as above, we define the following objects.

a) For any $c \in H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z})$, the transvection with respect to $c$, denoted $t_c \in \text{Aut}(H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}))$, is the automorphism given by $v \mapsto v + \langle v, c \rangle c$. As above, we may identify $c$ with its image in $T_\ell(\mathfrak{F})$, and then $t_c$ is identified with the automorphism of $T_\ell(\mathfrak{F})$ given by $v \mapsto v + e_\ell(v, c) c$.

b) A symplectic basis of $H_1(\mathfrak{F}(\mathbb{C}), \mathbb{Z})$ is an ordered basis $\{a'_1, \ldots, a'_g, b'_1, \ldots, b'_g\}$ satisfying the following properties:

(i) each $a'_i$ (resp. each $b'_i$) is represented by a loop on $\mathfrak{F}(\mathbb{C})$ whose image in $\mathbb{P}^1_{\mathbb{C}}$ separates $\{z_{2i-1}, z_{2i}\}$ (resp. $\{z_{2i-1}, \ldots, z_{2g+1}\}$) from its complement in $\{z_j\}_{j=1}^{2g+2}$; and

(ii) the (skew-symmetric) intersection pairing $\langle \cdot, \cdot \rangle$ on $H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z})$ is determined by $\langle a'_i, b'_j \rangle = -1$ for $1 \leq i \leq g$ and $\langle a'_i, a'_j \rangle = \langle b'_i, b'_j \rangle = \langle a'_i, b'_j \rangle = 0$ for $1 \leq i < j \leq g$. (See [7, Figure 6.1] or Figure 1 below.)

We note that a transvection in $\text{Aut}(H_1(\mathfrak{F}(\mathbb{C}), \mathbb{Z}))$ respects the intersection pairing $\langle \cdot, \cdot \rangle$; similarly, a transvection in $\text{Aut}(T_\ell(\mathfrak{F}))$ respects the Weil pairing $e_\ell$ and thus lies in $\text{Sp}(T_\ell(\mathfrak{F}))$.

From now on, given a complex hyperelliptic curve $\mathfrak{F}$, we fix a symplectic basis $\{a'_1, \ldots, a'_g, b'_1, \ldots, b'_g\}$ of $H_1(\mathfrak{F}(\mathbb{C}), \mathbb{Z})$. In order to prove Proposition 2.6 below, we require several lemmas, the first two of which are purely topological.
Lemma 2.3. Via the relations given in (2.1), there is an identification between the homology group \( H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) and the group of partitions of \( \mathcal{B} \) into 2 even-cardinality subsets (where the addition law is induced by the symmetric difference operation).

Proof. The essential ideas of this argument are contained in the proof of [13, Lemma 8.12], where the assertion is mentioned in a footnote. The maximal abelian exponent-2 quotient of \( \pi_1(P^1_\mathbb{C}\setminus \mathcal{B}, P) \) is isomorphic to \((\mathbb{Z}/2\mathbb{Z})^{2g+1}\) and is identified with the group of partitions of \( \mathcal{B} \) into two subsets (where the addition law is induced by taking symmetric differences), by sending the homology class of any loop \( \gamma \subset P^1_\mathbb{C}\setminus \mathcal{B} \to \mathcal{B} \) contained in each connected component of \( P^1_\mathbb{C}\setminus \gamma \). We have a homomorphism of homology groups (composed with reduction modulo 2) \( H_1(\mathcal{C}(\mathbb{C})\setminus \mathcal{B}, \mathbb{Z}) \to H_1(P^1_\mathbb{C}\setminus \mathcal{B}, \mathbb{Z}/2\mathbb{Z}) \) coming from the inclusion of fundamental groups in (2.1). By [3, Lemma 1], this homomorphism factors through the surjection \( H_1(\mathcal{C}(\mathbb{C})\setminus (\mathcal{B} \cup \{Q\}), \mathbb{Z}) \to H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}/2\mathbb{Z}) \) induced by the map \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \to \mathcal{C}(\mathbb{C}) \) (composed with reduction modulo 2). It is clear from this that we have an inclusion of \( H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) as the subgroup of \( H_1(P^1_\mathbb{C}\setminus \{z_1, \ldots, z_{2g+2}\}, \mathbb{Z}/2\mathbb{Z}) \) which is generated by the partitions \( \delta_i' \) \( : = \{z_{2i-1}, z_{2i}\} \cup \mathcal{B}\setminus \{z_{2i-1}, z_{2i}\} \) (the image of \( \alpha_i' \)) and \( \delta_i'' \) \( : = \{z_{2i}, \ldots, z_{2g+1}\} \cup \mathcal{B}\setminus \{z_{2i}, \ldots, z_{2g+1}\} \) (the image of \( \beta_i' \)) for \( 1 \leq i \leq g \). Now we have \( \delta_i' + \delta_j' \) \( = \sum_{j=1}^{i-1} \delta_j' + \sum_{j=i+1}^{g} \delta_j' \) \( \leq i \leq g \), for \( 1 \leq i \leq g \). The assertion now follows from checking that given any even-cardinality subset \( T \subset \mathcal{B}\setminus \{z_{2g+2}\} \), the partition \( T \cup \mathcal{B}\setminus T \) is equal to \( \sum_{z_i \in T} \{(z_i, z_{2g+2}) \cup \mathcal{B}\setminus \{z_i, z_{2g+2}\}\} \). \( \square \)

Lemma 2.4. Assume all of the above notation.

a) Let \( \gamma \subset P^1_\mathbb{C} \) be the image of a simple closed loop on \( P^1_\mathbb{C}\setminus \mathcal{B} \) which separates the set of \( a_i \)'s into two even-cardinality subsets.

Then the inverse image of \( \gamma \) under the ramified degree-2 covering map \( \mathcal{C}(\mathbb{C}) \to P^1_\mathbb{C} \) consists of two connected components, each of which are closed loops whose homology classes \( \pm c \in H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) differ by sign.

As a particular case, if \( \gamma \subset P^1_\mathbb{C} \) is the image of a loop which separates \( \{z_i, z_{2g+1}\} \) from its complement in \( \mathcal{B} \) for some \( i \), then the homology classes of the simple closed loops on \( \mathcal{C}(\mathbb{C}) \) lying above \( \gamma \) are given by \( \pm c_i' \) for some element \( c_i' \in H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) which is equivalent modulo 2 to

\[
\begin{cases}
  a'_{i+1}/2 + \cdots + a'_g + b'_{i+1}/2 & \text{if } i \text{ odd}, \\
  a'_{i}/2 + \cdots + a'_g + b'_{i}/2 & \text{if } i \text{ even}.
\end{cases}
\]

(2.2)

b) With \( \gamma \) and \( c \) as above, the Dehn twist \( D_{\gamma} \) induces an automorphism of \( H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) via the inclusion and quotient maps in (2.1), which is given by \( t_c^2 \in \text{Aut}(H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z})) \).

Proof. It follows from Lemma 2.3 and its proof that if \( \gamma \) is any loop in \( \pi_1(P^1_\mathbb{C}\setminus \mathcal{B}, P) \) which separates the \( z_i \)'s into 2 subsets of even cardinality, then \( \gamma \) lifts to an element \( c \in \pi_1(\mathcal{C}(\mathbb{C})\setminus \mathcal{B}, Q) \) whose image in \( H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) we also denote by \( c \). The only other choice of loop on \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) whose image in \( P^1_\mathbb{C}\setminus \mathcal{B} \) is \( \gamma \) must be based at \( d(Q) \) and equal to the composition of the path \( c \) with \( i \), where \( i : \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \to \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) is the only nontrivial deck transformation. Since \( i \) acts on the homology group by sign change (see [7, §7.4]), this loop must be \( -c \).

If the image of \( \gamma \) modulo 2 is the partition of \( \{z_i, z_{2g+1}\} \) and its complement, then the desired statement in (a) follows by the straightforward verification that this partition is equal to the symmetric sum of the partitions corresponding to the basis elements \( a_i' \) and \( b_i' \) appearing in the formulas given in (2.2). Thus, (a) is proved.

Consider a self-homeomorphism of \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) fixing \( Q \) representing the composition of (commuting) Dehn twists on \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) with respect to the two lifts \( \pm c \) of \( \gamma \) on \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \cup \{Q\} \); since Dehn twists do not depend on the orientation of loops, this composition of Dehn twists is equal to \( D_c^2 \). Note that such a self-homeomorphism of \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) (up to deformation) is the only self-homeomorphism of \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) fixing \( P \) which represents \( D_{\gamma} \). Now it follows from the functoriality of taking fundamental groups that the induced automorphism of \( \pi_1(\mathcal{C}(\mathbb{C})\setminus \mathcal{B}, Q) \) is the restriction of the automorphism \( \varphi(D_{\gamma}) \in \text{Aut}(\pi_1(P^1_\mathbb{C}\setminus \mathcal{B}, P)) \). Since any self-homeomorphism of \( \mathcal{C}(\mathbb{C})\setminus \mathcal{B} \) sends the image of a loop wrapping around a single point in \( \mathcal{B} \) to the image of a loop wrapping around a single point in \( \mathcal{B} \) and the kernel of the quotient map \( \pi_1(\mathcal{C}(\mathbb{C})\setminus \mathcal{B}, Q) \to \pi_1(\mathcal{C}(\mathbb{C}), Q) \) is generated by squares of homotopy classes of such loops, this restriction of \( \varphi(D_{\gamma}) \) stabilizes the kernel and induces an automorphism of \( \pi_1(\mathcal{C}(\mathbb{C}), Q) \). Thus, \( D_{\gamma} \) induces an automorphism of \( H_1(\mathcal{C}(\mathbb{C}), \mathbb{Z}) \) via the maps in (2.1), as claimed, and this automorphism is the one induced by the element \( D_c^2 \) of the mapping class group.
of $C(C)$. Now (b) follows from the well-known fact (see [7, Proposition 6.3]) that the Dehn twist with respect to any loop on a compact smooth manifold acts on homology as the transvection with respect to that loop. □

**Lemma 2.5.** Let $\alpha_1, \ldots, \alpha_d$ be distinct elements in $R_p$. There exist elements $\alpha'_1, \ldots, \alpha'_{d+1} \in R_p$ satisfying the following:

(i) The elements $\alpha'_i - \alpha'_j$ and $\alpha_i - \alpha_j$ have equal valuation for $1 \leq i < j \leq d$, and $\alpha'_{d+1} - \alpha'_1 \in R_p^\times$ for $1 \leq i \leq d$.

(ii) Let $\alpha_{d+1} = \infty \in \mathbb{P}_1$. There is a $K_p$-isomorphism

$$\psi : \mathbb{P}_1 \setminus \{\alpha_1, \ldots, \alpha_{d+1}\} \rightarrow \mathbb{P}_1 \setminus \{\alpha'_1, \ldots, \alpha'_{d+1}\}$$

such that the induced isomorphism $\psi_* : \pi_1(\mathbb{P}_1 \setminus \{\alpha_1, \ldots, \alpha_{d+1}\}, \psi^{-1}(\infty)) \rightarrow \pi_1(\mathbb{P}_1 \setminus \{\alpha'_1, \ldots, \alpha'_{d+1}\}, \infty)$ yields an isomorphism of $\rho_{alg}$ with the analogously defined representation $\rho'_{alg}$. The isomorphism $\psi_*$ takes any element represented by a loop on $\mathbb{P}_1 \setminus \{\alpha_1, \ldots, \alpha_{d+1}\}$ separating some singleton $\{\alpha_i\}$ from its complement in $\{\alpha_j\}_{j=1}^{d+1}$ to an element represented by a loop on $\mathbb{P}_1 \setminus \{\alpha'_1, \ldots, \alpha'_{d+1}\}$ separating the singleton $\{\alpha'_i\}$ from its complement in $\{\alpha'_j\}_{j=1}^{d+1}$.

**Proof.** Choose $\beta \in R_p^\times$ satisfying $\beta \neq \alpha_j \pmod{\pi}$ for $1 \leq j \leq d$ (this is always possible because the residue field $R_p/(\pi)$ is infinite). Let $\alpha'_j = \alpha_j \beta/(\beta - \alpha_j) \in R_p$ for $1 \leq j \leq d$ and $\alpha'_{d+1} = \beta \in R_p$, and let $\psi$ be the $K_p$-morphism given by $x \mapsto x\beta/(\beta - x)$. Then property (i) follows from straightforward computations. Since $\psi$ is defined over $K_p$, the isomorphism $\psi_*$ is equivariant with respect to the action of $G_{K, p}$ on $\mathbb{P}_1$. Moreover, after base change to $C$, $\psi$ is a homeomorphism of punctured Riemann spheres, and the property given in (ii) follows. □

We are finally ready to state and prove the main result of this section, which is essentially a more concrete version of a particular case of Grothendieck’s criterion for semistable reduction ([8, Proposition 3.5(iv)]). For the statement of the below proposition, we fix a symplectic basis $\{a_1, \ldots, a_g, b_1, \ldots, b_g\}$ of $H_1(C(C), \mathbb{Z})$ (see Figure 1 for an example); the image $\{a_1, \ldots, a_g, b_1, \ldots, b_g\} \subset T_\ell(J)$ forms a symplectic basis of $T_\ell(J)$ with respect to the Weil pairing.

**Proposition 2.6.** Let $C$ be a hyperelliptic curve of genus $g$ over $K_p$ given by an equation of the form $y^2 = h(x)$ for some squarefree polynomial $h$ of degree $d = 2g + 1$ or $d = 2g + 2$ with distinct roots $\alpha_1, \ldots, \alpha_d \in R_p$, and let $J$ be its Jacobian. Suppose that exactly 2 of the roots, $\alpha_1$ and $\alpha_2$, are equivalent modulo $\pi$, and let $m \geq 1$ be the maximal integer such that $\pi^m | (\alpha_1 - \alpha_2)$. Then for any prime $\ell \neq p$, the image of the natural action of $G_{K, p}$ on $T_\ell(J)$ is topologically generated by the element $\tau_{2m} \in \text{Sp}(T_\ell(J))$ for some $c \in T_\ell(J)$ determined by a loop on $\mathbb{P}_1$ whose image separates $\{\alpha_1, \alpha_2\}$ from the rest of the roots.

As a particular case, if $i \leq 2g$ and $j = 2g + 1$, then this $\ell$-adic Galois image is topologically generated by $\tau_{2m}^{2g}$ for some $c_i \in H_1(C(C), \mathbb{Z})$ equivalent modulo 2 to $a_{i+1}/2 + \cdots + a_g + b_{i+1}/2$ (resp. $a_{i+2}/2 + \cdots + a_g + b_{i+2}/2$) if $i$ is odd (resp. even).

**Proof.** We first assume that $d = 2g + 2$. Let $\alpha_1, \ldots, \alpha_{2g+2} \in C[x]$ be the elements constructed from the $\alpha_i$’s as above, and define the family $\mathcal{F} \rightarrow B^*_{\ell}$ as above. It is clear from the hypothesis on the roots $\alpha_i$ that the set $I$ in the statement of Theorem 2.1 consists of only the elements $(I, 2g + 1, n)$ for $1 \leq n \leq m$. Theorem 2.1(a) then implies that a topological generator of $\pi_1(B^*_{\ell}, z_0)$ acts on $\pi_1(F_{\ell}, \infty)$ via the monodromy action $\rho_{top}$ as $D_{\ell}^{m}$, where $\gamma_1$ is a loop on $F_{\ell}$ separating the subset $\{\alpha_1(z_0), \alpha_{2g+1}(z_0)\}$ from its complement in $\{\alpha_j(z_0)\}_{j=1}^{2g+2}$. Let $\mathcal{C}$ be the complex hyperelliptic curve of degree $d = 2g + 2$ ramified over $\mathbb{P}_1$ at the points $\alpha_1(z_0), \ldots, \alpha_{2g+2}(z_0) \in C$, which has a symplectic basis $\{a'_1, \ldots, a'_g, b'_1, \ldots, b'_g\}$ of $H_1(C(C), \mathbb{Z})$. By Lemma 2.4, the automorphism of $\pi_1(F_{\ell}, \infty)$ determined by $D_{\ell}^{m}$ induces the automorphism of $H_1(C(C), \mathbb{Z}) \otimes \mathbb{Z}$ given by $\tau_{2m} : v \mapsto v + 2m \langle v, c'_i \rangle c'_i$, where $c'_i \in H_1(C(C), \mathbb{Z})$ is equivalent modulo 2 to the formula in (2.2). Now parts (b) and (c) of Theorem 2.1 say that there is an isomorphism $\phi : \pi_1(F_{\ell}, \infty) \rightarrow \pi_1(\mathbb{P}_1 \setminus \{\alpha_1, \ldots, \alpha_{d+1}\}, \infty)$ making the action $\rho_{top}$ isomorphic to the Galois action $\rho_{alg}$. Since $p \neq 2$ and $C(C) \otimes \mathbb{F} \otimes \mathbb{C}(C) \setminus \{(\alpha_i, 0)\}_{i=1}^{2g+2}$ are the only degree-2 covers of $F_{\ell}$ and $\mathbb{P}_1 \setminus \{\alpha_1, \ldots, \alpha_{2g+2}\}$ respectively, we see that the isomorphism $\phi$ induces an isomorphism $H_1(C(C), \mathbb{Z}) \otimes \mathbb{Z} \rightarrow H_1(C(C), \mathbb{Z}) \otimes \mathbb{Z}$ which we also denote by $\phi$. It is
clear from the property of $\phi$ given in Theorem 2.1(c) and from our characterization of homology groups with coefficients in $\mathbb{Z}/2\mathbb{Z}$ in the proof of Lemma 2.4 that $\phi(a'_j) \equiv a_j$ and $\phi(b'_j) \equiv b_j \pmod{2}$ for $1 \leq j \leq g$.

In the case that $d = 2g + 1$, we get the same results by applying Lemma 2.5, which allows us to replace $\alpha_1, \ldots, \alpha_{2g+1}, \alpha_{2g+2} := \infty$ with elements $\alpha'_1, \ldots, \alpha'_{2g+2} \in \mathcal{R}_p$ whose differences have the same valuations with respect to $\pi$.

Putting this all together, we see that the tame Galois action on $H_1(C(\mathbb{C}), \mathbb{Z}) \otimes \hat{\mathbb{Z}}(p')$ induced by $\rho_{\text{alg}}$ sends a generator of $G^\text{tame}_{\mathbb{R}, p}$ to the automorphism of $H_1(C(\mathbb{C}), \mathbb{Z}) \otimes \hat{\mathbb{Z}}(p')$ given by $v \mapsto v + 2m\langle v, c_i \rangle c_i$ for some $c_i \in H_1(C(\mathbb{C}), \infty) \otimes \hat{\mathbb{Z}}(p')$ which is equivalent modulo 2 to the formula given in the statement. Here $\langle \cdot, \cdot \rangle$ is the skew-symmetric pairing on $H_1(C(\mathbb{Z}), \mathbb{Z}) \otimes \hat{\mathbb{Z}}(p')$ induced by the intersection pairing on $H_1(C(\mathbb{Z}), \mathbb{Z})$ via $\phi$; note that $\langle \cdot, \cdot \rangle$ is normalized so that $\langle H_1(C(\mathbb{Z}), Z), H_1(C(\mathbb{Z}), Z) \rangle \phi = Z$. As above, we identify the maximal pro-$\ell$ quotient of $H_1(C(\mathbb{Z}), \mathbb{Z}) \otimes \hat{\mathbb{Z}}(p')$ with $T_\ell(J)$ and see that the natural $\ell$-adic Galois action $\rho_\ell$ factors through $G^\text{tame}_{\mathbb{R}, p}$ and takes a generator to the automorphism of $T_\ell(J)$ given by $v \mapsto v + 2m\langle v, c_i \rangle c_i$. But this automorphism must lie in $\text{Sp}(T_\ell(J))$ by the Galois equivariance of the Weil pairing $e_\ell$ and the fact that $K_p$ contains all $\ell$-power roots of unity. It is now an easy exercise to verify that this implies that $\langle v, c_i \rangle \phi = \pm e_\ell\langle v, c_i \rangle$ for all $v \in T_\ell(J)$, and so the image of $\rho_\ell$ is generated by $t^{2m}_{c_i} : v \mapsto v + 2me_\ell\langle v, c_i \rangle c_i$, as desired.

In order to prove Theorems 1.1 and 1.2, we will put some local data together to show using Proposition 2.6 that the $\ell$-adic Galois image contains $\{t^{2m}_{c_1}, \ldots, t^{2m}_{c_{2g}}\}$ for homology classes $c_i$ as above and a certain integer $m$. Therefore, it is of interest to investigate the subgroup of $\text{Sp}(T_\ell(J))$ that this set generates. We will see that this subgroup is always open, but unfortunately, since the $c_i$’s are only known modulo 2, not much more can be deduced except if $\ell = 2$. In this case, the subgroup of $\text{Sp}(T_2(J))$ generated by the above set can be determined precisely, which is the goal of the next section.

### 3 SUBGROUPS GENERATED BY POWERS OF TRANVECTIONS

For this section, we let $M$ be a free $\mathbb{Z}$-module of rank $2g$, equipped with a nondegenerate skew-symmetric $\mathbb{Z}$-bilinear pairing $\langle \cdot, \cdot \rangle : M \times M \to \mathbb{Z}$. For any ring $A$, this pairing induces in an obvious way a nondegenerate skew-symmetric $A$-bilinear pairing on the free $A$-module $M \otimes A$ which we also denote by $\langle \cdot, \cdot \rangle$. We write $\text{Sp}(M \otimes A)$ for the symplectic group of $A$-automorphisms of $M \otimes A$ which respect this pairing; for any integer $N \geq 1$, we write $\Gamma(N)$ for the level-$N$ congruence subgroup of $\text{Sp}(M \otimes A)$ as defined in §1. For any element $c \in M \otimes A$, we write $t_c \in \text{Sp}(M \otimes A)$ for the transvection with respect to $c$ and the pairing $\langle \cdot, \cdot \rangle$, as in Definition 2.2(a). We fix a basis $\{a_1, \ldots, a_g, b_1, \ldots, b_g\}$ of $M$ and assume that the pairing is determined by $\langle a_i, b_j \rangle = -1$ for $1 \leq i \leq g$ and $\langle a_i, a_j \rangle = \langle b_i, b_j \rangle = \langle a_i, b_j \rangle = 0$ for $1 \leq i < j \leq g$. We also write $a_i, b_i \in M \otimes A$ for the elements $a_i \otimes 1$ and $b_i \otimes 1$ respectively for $1 \leq i \leq g$. When $A$ is a field, we write $\mathfrak{sp}(M \otimes A)$ for the Lie algebra of endomorphisms of $M \otimes A$ corresponding to the Lie group $\text{Sp}(M \otimes A)$ which is equipped with the Lie bracket $[\cdot, \cdot]$; it is well known that $\mathfrak{sp}(M \otimes A)$ is a $2g^2$-dimensional vector space over $A$. Our main goal is to prove the following purely algebraic result.

**Proposition 3.1.** Let $c_1, \ldots, c_{2g} \in M$ be elements such that $c_i$ is equivalent modulo 2 to

$$
\begin{align*}
&\begin{cases}
a_{(i+1)/2} + \cdots + a_{i/2} + b_{(i+1)/2} & \text{if } i \text{ odd,} \\
a_{i/2} + \cdots + a_{i/2} + b_{i/2} & \text{if } i \text{ even,}
\end{cases}
\end{align*}
$$

for $1 \leq i \leq 2g$, and let $\ell$ be any prime. Let $G'_\ell \subseteq \text{Sp}(M \otimes \mathbb{Z}_\ell)$ be the subgroup topologically generated by the elements $t_{c_1}^{m_1}, \ldots, t_{c_{2g}}^{m_{2g}}$ for some integers $m_i \in \mathbb{Z} \setminus \{0\}$. Then $G'_\ell$ is open as a Lie subgroup of $\text{Sp}(M \otimes \mathbb{Z}_\ell)$.

In the case that $\ell = 2$, assume moreover that for some integers $n, n' \geq 1$, we have $v_2(m_i) \leq n$ for $1 \leq i \leq 2g - 1$ and $v_2(m_{2g}) = n'$. Then $G'_2$ contains $\Gamma(2^{2n})$ (resp. $\Gamma(2^{n+n'})$) if $n' \leq n$ (resp. if $n' > n$).

Note that for any prime $\ell$, the image of any transvection $t \in \text{Sp}(M \otimes \mathbb{Q}_\ell)$ under the logarithm map is $t - 1 \in \mathfrak{sp}(M \otimes \mathbb{Q}_\ell)$ and that the Lie algebra of $G'_\ell$ is generated as a Lie algebra by the logarithms of the transvections $t_{c_i}$, which are given by $T_i := t_{c_i} - 1$. Therefore, in order to prove the first statement of this proposition, it suffices to show
that \( \{ T_i \}_{1 \leq i \leq g} \) generates the full \( \ell \)-adic symplectic Lie algebra \( \mathfrak{sp} ( M \otimes \mathbb{Q}_\ell ) \). However, in order to get both statements, we will prove something slightly stronger which is implied by the following lemma.

**Lemma 3.2.** Let \( T_i \in \mathfrak{sp} ( M \otimes \mathbb{F}_2 ) \) denote the image modulo 2 of \( t_i - 1 \in \mathfrak{sp} ( M \otimes \mathbb{Z}_2 ) \). Then an \( \mathbb{F}_2 \)-basis for \( \mathfrak{sp} ( M \otimes \mathbb{F}_2 ) \) is given by the set \( \{ T_i \}_{1 \leq i \leq g} \cup \{ [ T_i , T_j ] \}_{1 \leq i < j \leq g} \).

**Proof.** Since the vector space \( \mathfrak{sp} ( M \otimes \mathbb{F}_2 ) \) has dimension \( 2g^2 + g \) over \( \mathbb{F}_2 \) and there are \( 2g^2 + g \) elements listed in the set of \( T_i \)'s and their commutators, it suffices to prove that this set is linearly independent over \( \mathbb{F}_2 \).

Assume that for some scalars \( \gamma_{i,j} = \gamma_{j,i} \in \mathbb{F}_2 \) for \( 1 \leq i \leq j \leq 2g \), we have

\[
0 = \sum_{i=1}^{2g} \gamma_{i,i} T_i + \sum_{1 \leq i < j \leq 2g} \gamma_{i,j} [ T_i , T_j ] = 0.
\]

Let \( \bar{c}_i \) denote the reduction modulo 2 of \( c_i \in M \) for \( 1 \leq i \leq 2g \); from the characterization of the \( c_i \)'s modulo 2 we see that the set of elements \( \bar{c}_i \) is linearly independent over \( M \otimes \mathbb{F}_2 \). Note that each commutator \( [ T_i , T_j ] \) is the map given by \( v \mapsto \langle v , c_i \rangle \bar{c}_j + \langle v , c_j \rangle \bar{c}_i \). Therefore, the Lie algebra of \( G' \), which clearly contains the \( T_i \)'s and their commutators, coincides with \( \mathfrak{sp} ( M \otimes \mathbb{Q}_\ell ) \). The first statement of the proposition immediately follows.

Now we assume that \( \ell = 2 \) and prove the second statement. Note that it is meaningful to raise transvections to the powers of elements in \( \mathbb{Z}_2 \); therefore, since \( 2^{n'} / m_2g , 2^{n} / m_1 \in \mathbb{Z}_2 \) for \( 1 \leq i \leq 2g - 1 \), it suffices to prove the statement under the assumption that \( m_1 = \cdots = m_{2g-1} = 2^n \) and \( m_{2g} = 2^{n'} \).

For ease of notation, we write \( n'' = \max \{ n , n' \} \) and \( N = n + n'' \), so that the desired statement is that \( G'_2 \) contains the congruence subgroup \( \Gamma ( 2^N ) \). Since \( G'_2 \) is closed, it suffices to show that the image of \( G \) modulo \( 2^{N+m} \) contains \( \Gamma ( 2^N ) / \Gamma ( 2^{N+m} ) \) for each integer \( m \geq 1 \). We claim that in fact we only need to show this for \( m = 1 \). Indeed, for any \( m \geq 1 \), the restriction of the logarithm map to \( \Gamma ( 2 ) \) sends each element \( t \in \Gamma ( 2^{N+m-1} ) \) to an element of \( \mathfrak{sp} ( M \otimes \mathbb{Z}_2 ) \) which is equivalent to \( t \) modulo \( 2^{N+m} \) since \( ( t - 1 )^2 \equiv 0 \) modulo \( 2^{N+m} \). In this way, one verifies that there is an isomorphism from the additive group \( \mathfrak{sp} ( M \otimes \mathbb{F}_2 ) \) to \( \Gamma ( 2^{N+m-1} ) / \Gamma ( 2^{N+m} ) \), given by sending each element \( T \in \mathfrak{sp} ( M \otimes \mathbb{F}_2 ) \) to \( 1 + 2^{N+m-1}T \in \mathfrak{sp} ( M \otimes \mathbb{Z}_2 ) \), where \( T \) is any operator in \( \text{End} ( M \otimes \mathbb{Z} / 2^{N+m} \mathbb{Z} ) \) whose image modulo 2 is \( T \). In particular, each \( \Gamma ( 2^{N+m-1} ) / \Gamma ( 2^{N+m} ) \) is an elementary abelian group of exponent 2 and rank \( 2g^2 + g \) (this is also known from the proof of [15, Corollary 2.2]). Moreover, it is easy to check that for each \( m \geq 1 \), the map sending each matrix in \( \Gamma ( 2^{N+m} ) \) to its \( 2^m \)-th power induces a group isomorphism \( \Gamma ( 2^{N+m} ) \cong \Gamma ( 2^{N+m} ) \). It follows that if the image of \( G'_2 \) modulo \( 2^{N+1} \) contains \( \Gamma ( 2^{N} ) / \Gamma ( 2^{N+1} ) \), then the image of \( G'_2 \) modulo \( 2^{N+m} \) contains \( \Gamma ( 2^{N} ) / \Gamma ( 2^{N+m} ) \) for all \( m \geq 1 \). Thus, in order to prove the proposition, it suffices to show that the image of \( G'_2 \) modulo \( 2^{N+1} \) contains \( \Gamma ( 2^{N} ) / \Gamma ( 2^{N+1} ) \).

As above, let \( T_i \) denote \( t_i - 1 \) for \( 1 \leq i \leq 2g \). Since Lemma 3.2 says that the image modulo 2 of \( \{ T_i \}_{1 \leq i \leq g} \cup \{ [ T_i , T_j ] \}_{1 \leq i < j \leq g} \) is a basis of \( \mathfrak{sp} ( M \otimes \mathbb{F}_2 ) \), it suffices to show that the image of \( G'_2 \) modulo \( 2^{N+1} \) contains the images of the elements in \( \{ 1 + 2^N T_i \}_{1 \leq i \leq 2g} \cup \{ 1 + 2^N [ T_i , T_j ] \}_{1 \leq i < j \leq 2g} \) under \( \Gamma ( 2^{N+1} ) \). Clearly \( G'_2 \) is generated by \( \{ 1 + 2^N T_i \}_{1 \leq i \leq g} \cup \{ 1 + 2^N T_{2g} \} \). We verify using the property \( T_i^2 = 0 \) that \( ( 1 + 2^N T_i )^{2^{N+1}} \equiv 1 + 2^N T_i ( \text{mod} \ 2^{N+1} ) \) for \( 1 \leq i \leq 2g - 1 \), that
\[
(1 + 2^n T_{2k})^{2^n n'' - n'} \equiv 1 + 2^N T_{2k} \pmod{2^{N+1}}, \text{ and that}
\]
\[
(1 + 2^n T_1)(1 + 2^n T_j)(1 + 2^n T_j)^{-1}(1 + 2^n T_j)^{-1} \equiv 1 + 2^N [T_i, T_j] \pmod{2^{N+1}}
\]
for \(1 \leq i < j \leq 2g\). Thus, \(G'_2 \supset \Gamma(2^N)\), as desired.

We now state and prove another proposition which will be needed only for the last statements of Theorems 1.1 and 1.2, which pertain to the case that the hyperelliptic curve has degree 4.

**Proposition 3.3.** Assume the notation and assumptions of Proposition 3.1 and that \(g = 1\) and \(n' = n\), and let \(c_3 \in M\) be an element which is equivalent modulo 2 to \(a_1\). Then the subgroup of \(\Gamma(2^n)\) generated by \(G_2\) and the element \(t_{c_3}^{2^n}\) coincides with \(\Gamma(2^n)\).

**Proof.** By the arguments used at the beginning of the proof of Proposition 3.1, we only need to show that the images of \(t_{c_3}^{2^n}, t_{c_3}^{2^n}, t_{c_3}^{n}\) generate \(\Gamma(2^n)\) modulo \(\Gamma(2^{n+1})\). Using the isomorphism from the additive group \(\mathfrak{sp}(M \otimes \mathbb{F}_2)\) to \(\Gamma(2^n)\) established in that proof, we see that it suffices to show that \(\{T_1, T_2, T_3\}\) is linearly independent and thus generates the rank-3 elementary abelian group \(\mathfrak{sp}(M \otimes \mathbb{F}_2)\), where \(T_i\) denotes the image modulo 2 of \(c_i - 1\) for \(1 \leq i \leq 3\). But this is clear from noting that \(c_3 \equiv c_1 + c_2 \pmod{2}\) and writing out these linear operators as matrices with respect to an ordered basis of \(M \otimes \mathbb{F}_2\) consisting of the images of \(c_1\) and \(c_2\).

**Remark 3.4.** It is possible to prove a more general version of Proposition 3.1 whose statement is as follows. Let \(c_1, \ldots, c_{2g} \in M\) be elements which form a basis of \(M\), and choose a prime \(\ell\) and integers \(m_1, \ldots, m_{2g}\) and define \(G'_\ell \subseteq \text{Sp}(M \otimes \mathbb{Z}_\ell)\) as in the statement of the proposition. Consider the simple graph \(\Gamma\) whose vertices are given by the basis elements \(c_i\) and whose edge set is defined so that two vertices \(c_i\) and \(c_j\) are connected by an edge if and only if \(\langle c_i, c_j \rangle \equiv 1 \pmod{2}\). Then if the graph \(\Gamma\) is connected, we have that \(G'_\ell\) is open as a subgroup of \(\text{Sp}(M \otimes \mathbb{Z}_\ell)\). If we assume moreover that \(\ell = 2\), given an integer \(n \geq 1\) such that \(v_2(m_i) \leq n\) for \(1 \leq i \leq 2g\), we have \(G'_2 \supset \Gamma(2^{\delta(n+1)})\), where \(\delta\) is the diameter of the graph \(\Gamma\). These claims can be proved using a similar strategy as in the proof of Proposition 3.1, which treats the special case where \(\Gamma\) is a complete graph and thus is connected with diameter \(\delta = 1\).

## 4. PROOF OF MAIN THEOREMS AND A FURTHER RESULT

The main goal of this section is to prove Theorems 1.1 and 1.2. Our strategy for this is to put together local results with respect to several primes of \(K\) using Proposition 2.6 to get several elements in \(G_\ell\) and then to use Proposition 3.1 to determine that the subgroup of \(G_\ell\) generated by these elements is open and, when \(\ell = 2\), contains a certain congruence subgroup of the symplectic group. This is realized by the following theorem, which can be used in a far more general situation than is required for Theorems 1.1 and 1.2 and is therefore a useful result in its own right.

**Theorem 4.1.** Let \(J\) be the Jacobian of the hyperelliptic curve \(C\) over \(K\) of genus \(g\) and degree \(d'\) with defining equation \(y^2 = \prod_{i=1}^{d'} (x - a_i)\) for some elements \(a_i \in \mathcal{O}_K\) for \(1 \leq i \leq d'\), and define the 2-adic Galois image \(G_2\) as above. Suppose that there are distinct primes \(p_1, \ldots, p_{d'-1}\) of \(K\) not lying over (2) and such that for \(1 \leq i \leq d' - 1\), the only two \(\alpha_i\)’s which are equivalent modulo \(p_i\) are \(\alpha_i\) and \(\alpha_{d'}\); let \(m_i \geq 1\) be the maximal integer such that \(p_i^{m_i} \mid (\alpha_{d'} - \alpha_i)\). Let \(n = \max \{v_2(m_i)\}_{i=1}^{d'-2}\).

a) For any prime \(\ell\) different from all of the residue characteristics of the \(p_i\)’s, the Lie subgroup \(G_\ell \subseteq \text{GSp}(T_2(J))\) is open. In particular, \(G_2 \subseteq \text{GSp}(T_2(J))\) is open.

b) If \(n' := v_2(m_{d'-1}) \leq n\) or if \(d' = 2g + 2\), we have \(\Gamma(2) \supset G_2 \cap \text{Sp}(T_2(J)) \supset \Gamma(2^{2n+2})\). Otherwise, we have \(\Gamma(2) \supset G_2 \cap \text{Sp}(T_2(J)) \supset \Gamma(2^{\max(n,n'+1)})\). Moreover, if \(d' = 4\), then \(G_2 \cap \text{Sp}(T_2(J)) \supset \Gamma(2^{\max(n,n'+1)})\).

**Proof.** Using the embedding \(K \hookrightarrow \mathbb{C}\) fixed at the beginning of §2, we identify \(T_\ell(J)\) with \(H_1(C, \mathbb{Z}) \otimes \mathbb{Z}_\ell\) as we did in §2. Let \(\{a_1, \ldots, a_g, b_1, \ldots, b_g\}\) be a symplectic basis of \(H_1(C, \mathbb{Z})\) as in Definition 2.2(b) with \((z_1, \ldots, z_{2g+2}) = (\alpha_1, \ldots, \alpha_{2g+1}, \infty)\) if \(d'\) is odd and \((z_1, \ldots, z_{2g+2}) = (\alpha_1, \ldots, \alpha_{2g}, \alpha_{2g+2}, \alpha_{2g+1})\) if \(d'\) is even. Then Proposition 2.6 says that
for $1 \leq i \leq 2g$, the image of $G_{K,p_i} \subset G_K$ in $GSp(T(\ell)(J))$ contains $t_{ci}^{2mi}$, where $t_{ci} \in Sp(T(\ell)(J))$ is the transvection with respect to an element $c_i \in T(\ell)(J)$ which is equivalent modulo 2 to the formula given in (2.2). Meanwhile, if $d'$ is even, the image of $G_{K,p_{2g+1}}$ contains $t_{ci}^{2\ell d_{2g+1}}$ for some other element $c_i' \in T(\ell)(J)$ corresponding to the lift of a loop separating $\{\alpha_{2g+1}, \alpha_{2g+2}\}$ from its complement in $\{\alpha_i\}_{i=1}^{2g+2}$. In any case, we have $t_{ci}^{2mi}, t_{ci}^{2m_{2g}} \in G_\ell$ for all $\ell$. It then follows from Proposition 3.1 applied to $M := H_{\ell}(C(\mathbb{C}), Z)$ for any $\ell$ and over $\mathbb{F}_p$, because otherwise for such an $\ell$, it is generally not difficult to compute the order of $G_\ell$. It follows that $\mathfrak{p} \not| (2\Delta)$.

Remark 4.2. We note that it is generally not difficult to compute the order of $G_{2}/\Gamma(2n+2)$ or $G_{2}/\Gamma(2n+n'2)$, where $G_2 \subset G_2$ is the subgroup generated by the powers of transvections given in the proof above. Therefore, one may improve the upper bound for $[\Gamma(2) : G_2]$ which directly follows from the statement of Theorem 4.1. For example, we have $[\Gamma(2) : G_2] \leq 2(2n+1)(2g^2+g)-(n+1)(d'-1)$ in the case that $n = n'$.

Example 4.3 (Legendre curve). For any $\lambda \in \Theta_K \setminus \{0, 1\}$, let $E_\lambda$ be the elliptic curve over $K$ given by $y^2 = x(x - 1)(x - \lambda)$. Suppose that there exist (necessarily distinct) primes $p_1$ and $p_2$ of $K$ not lying over $(2)$ and integers $m_1, m_2 \geq 1$ such that $p_1^{m_1}$ exactly divides $\lambda$ and $p_2^{m_2}$ exactly divides $(\lambda - 1)$. Then Theorem 4.1 tells us that the 2-adic Galois image $G_2$ (strictly) contains $\Gamma\left(\frac{\sqrt{\alpha}^2\nu}{(m_1)} + \frac{\nu(2)}{2(m_2)}\right)$. In the case that $m_1 = m_2 = 1$ (e.g. $K = \mathbb{Q}$, $\lambda = 6$, $p_1 = (3)$, $p_2 = (5)$), we get $\Gamma(2) \supset G_2 \cap \text{Sp}(T(2(E_\lambda))) \supset \Gamma(4)$ and can therefore directly compute the precise subgroup $G_2 \cap \text{Sp}(T(2(E_\lambda))) \subset \Gamma(2)$ using the well-known fact that the 4-division field $K(E_\lambda[4])$ is generated over $K$ by $\left\{\sqrt{1}, \sqrt{\lambda}, \sqrt{\lambda - 1}\right\}$.

It is also possible to prove the statement of Proposition 2.6, thus determining $G_2$, in the particular cases of $C = E_\lambda$ over $K_{p_1}$ and over $K_{p_2}$ using formulas for generators of 2-power division fields of $E_\lambda$ found in [18], as the author has done in [19, §3.4].

We now prove Theorems 1.1 and 1.2 together.

Proof of Theorems 1.1 and 1.2. First assume the notation and hypotheses of Theorem 1.1. Let $\alpha_1, \ldots, \alpha_d$ denote the roots of $f$, and write $L = K(\alpha_1, \ldots, \alpha_d)$ for the splitting field of $f$ over $K$. Note that $\text{Gal}(L/K)$ acts transitively on the $\alpha_i$’s since $f$ is irreducible. It then follows from the well-known description of the 2-division field of a hyperelliptic Jacobian (see for instance [13, Corollary 2.11]) that $G_2$ does not fix the 2-torsion points of $J$ and so $G_2$ is not contained in $\Gamma(2)$, while the image of $\text{Gal}(L/K)$ under $G_2$ coincides with $G_2 \cap \Gamma(2)$.

The fact that $\mathfrak{p} \not| (2\Delta)$ implies that the extension $L/K$ is not ramified at $\mathfrak{p}$, and so $\mathfrak{p}$ splits into a product $p_1 \ldots p_r$ of distinct primes in $L$, for some integer $r$ dividing $[L : K]$. Then since $\mathfrak{p}^m$ exactly divides $(f(\lambda)) = \prod_{i=1}^{d} (\lambda - \alpha_i)$, we have $p_i \not| (\lambda - \alpha_i)$ for any $i$, we assume without loss of generality that $p_i \not| (\lambda - \alpha_1)$. Then $p_i$ cannot divide $(\lambda - \alpha_i)$ for any $i \in \{2, \ldots, d\}$, because otherwise for such an $i$ we would have $p_i \not| (\alpha_i - \alpha_1) \not| (\Delta)$, which contradicts the hypothesis that $\mathfrak{p} \not| (2\Delta)$. It follows that $\mathfrak{p}^m$ exactly divides $(\lambda - \alpha_1)$. Then by applying elements of $\text{Gal}(L/K)$ that take $\alpha_1$ to each $\alpha_i$, we get other primes lying over $\mathfrak{p}$ whose mth powers exactly split the ideals $\left(\frac{\lambda - \alpha_i}{\mathfrak{p}}\right)$; we assume without loss of generality that $\mathfrak{p}^m$ exactly divides $(\lambda - \alpha_i)$ for $1 \leq i \leq d$. Now since the $\mathfrak{p} \not| (2\Delta)$ hypothesis implies that none of the $p_i$’s lie over $2$, we can apply Theorem 4.1 with $K$ replaced by $L$, $d' = d + 1, \alpha_{d'} = \lambda$, and $m_1 = \cdots = m_{d'} - 1 = m$ to get the statements of Theorem 1.1.

Now assume the notation and hypotheses of Theorem 1.2. Then the argument for proving Theorem 1.2 is the same except that when applying Theorem 4.1 we choose $p_{d'-1}$ to be a prime of $L$ lying over $p'$, and we put $d' = d + 2, \alpha_{d'} = \lambda$, $\alpha_{d'-1} = \lambda', m = m_1 = \cdots = m_{d'-2}$, and $m' = m_{d'-1}$.

5 | REALIZING UNIFORM BOUNDEDNESS ALONG ONE-PARAMETER FAMILIES

Fix an irreducible monic polynomial $f \in \Theta_K[x]$ of degree $d \geq 2$. It follows from Cadoret and Tamagawa’s results [6, Theorems 1.1 and 5.1] that for all but finitely many $\lambda \in K$, the $\ell$-adic Galois image $G_{\ell,\lambda}$ associated to the Jacobian of the curve given by $y^2 = f(x)(x - \lambda)$ is open in the $\ell$-adic Galois image $G_{\ell,\lambda}$ associated to the generic fiber of the family parametrized...
by $\lambda$. These theorems also assert that there is some integer $B \geq 1$ depending only on $f$ and $\ell$ such that the index of $G_{\ell, A}$ in $G_{\ell, z}$ is bounded by $B$ for all but finitely many $A \in K$. The following theorem treats the $\ell = 2$ case: we recover the openness result when $d \geq 4$ and explicitly provide the aforementioned uniform bound when $d$ is even. (Note that for the elliptic curve case, where $d \in [2, 3]$, such openness results are already known from the celebrated Open Image Theorem of Serre given by [16, IV-11], while uniform bounds are given by [2, Theorem 1.3].) It is interesting to note that Faltings’ theorem is used both in the proof of [6, Theorem 1.1] and in our proof of the theorem below.

**Theorem 5.1.** Let $f \in O_K[x]$ be an irreducible monic polynomial of degree $d \geq 3$ with discriminant $\Delta$. For each $\lambda \in K$, let $J_\lambda$ denote the Jacobian of the hyperelliptic curve $C_\lambda$ with defining equation $y^2 = f(x)(x - \lambda)$, and write $G_{2, \lambda} \subseteq GSp(T_2(J_\lambda))$ for the image of the associated 2-adic Galois representation.

a) If $d \geq 4$, the Lie subgroup $G_{2, \lambda} \subseteq GSp(T_2(J_\lambda))$ is open for all but finitely many $\lambda \in K$.

b) If $d = 3$ (resp. if $d \geq 5$), then $G_{2, \lambda} \cap Sp(T_2(J_\lambda)) \supseteq \Gamma(4)$ for all but finitely many $\lambda \in O_K[2(\Delta)^{-1}] \cdot (K^\times)^4$ (resp. all but finitely many $\lambda \in O_K[2(\Delta)^{-1}] \cdot (K^\times)^2$).

c) If $d = 4$, then we have $G_{2, \lambda} \cap Sp(T_2(J_\lambda)) \supseteq \Gamma(16)$ for all but finitely many $\lambda \in K$. If $d \geq 6$ is even, then we have $G_{2, \lambda} \cap Sp(T_2(J_\lambda)) \supseteq \Gamma(4)$ for all but finitely many $\lambda \in K$.

**Proof.** Fix a set of integral ideal representatives for the group of ideal classes of $K$, and let $S$ be the (finite) set of primes of $K$ which divide the ideals in this set. Let $\Sigma \subset K^\times$ denote the multiplicative subgroup generated by the elements $\xi \in O_K$ such that the ideal $(\xi)$ is divisible only by primes which lie in $S$ or divide $(\Delta)$. We claim that $\Sigma$ is finitely generated. Indeed, there is an obvious map from $\Sigma$ to the free $Z$-module formally generated by the (finite) set of prime ideals of $O_K$ which lie in $S$ or divide $(\Delta)$, and its kernel is the unit group $O_K^\times$, which is also well known to be finitely generated.

Choose any $\lambda \in K$, which we may write as $\mu/\nu$ for some $\mu, \nu \in O_K$ such that the common prime divisors of the ideals $(\mu)$ and $(\nu)$ all lie in $S$. Let $h(x) = \nu^d f(\nu^{-1}x)$, which is a monic polynomial in $O_K[x]$; note that the discriminant of $h$ is equal to $\nu^{2d-2} \Delta$. Then there is a $K(\sqrt{\nu})$-isomorphism from $C_\lambda$ to the hyperelliptic curve $C'_{\lambda}$ whose defining equation is $y^2 = \nu^d f(\nu^{-1}x)(x - \mu) \in O_K[x]$, given by $(x, y) \mapsto (\nu x, \nu^{d+1/2} y)$. Thus, letting $J'_{\lambda}$ denote the Jacobian of $C'_{\lambda}$, the 2-adic Tate modules $T_2(J_{\lambda})$ and $T_2(J'_{\lambda})$ are isomorphic as $\text{Gal}(\overline{K}/K(\sqrt{\nu}))$-modules. In this light of this, it suffices to replace $G_{2, \lambda}$ with the 2-adic Galois image associated to $J'_{\lambda}$.

Now Theorem 1.1 implies that if there is a prime element $p$ dividing $(\nu^d f(\lambda))$ but not $(2\nu^{2d-2} \Delta)$, then $G_{2, \lambda} \subseteq GSp(T_2(J'_{\lambda})) \supseteq GSp(T_2(J_{\lambda}))$ is open. It follows from the fact that $\mu$ and $\nu$ are coprime away from $S$ that $(\nu^d f(\lambda))$ is not divisible by any prime dividing $(\nu)$ which does not lie in $S$, so a prime $p$ satisfying the above condition does not divide $(2\Delta)$ and is not in $S$. The existence of such a prime is equivalent to the condition that $\nu^d f(\lambda) \not\in \Sigma$, so to prove part (a) it suffices to show that $f(\lambda) \in \Sigma \cdot (K^\times)^d$ for only finitely many $\lambda \in K$. Note that any such $\lambda$ yields a solution $(x = \lambda, y) \in K \times K$ to an equation of the form $\xi y^d = f(x)$ with $\xi \in \Sigma'$, where $\Sigma' \subset \Sigma$ is a set of representatives of elements in $\Sigma/\Sigma^d$. If $d \geq 4$, then an application of the Riemann–Hurwitz formula shows that such an equation defines a smooth curve of genus $\geq 2$, and then Faltings’ theorem implies that there are only finitely many solutions defined over $K$ to each such equation. Therefore, to prove (a) it suffices to show that there are only finitely many choices of $\xi$. But this follows from the fact that $\Sigma/\Sigma^d$ is finite because $\Sigma$ is finitely generated.

Now assume that $d = 3$ or $d \geq 5$ and that $\lambda \in O_K[(2\Delta)^{-1}] \cdot (K^\times)^s$, with $s = 4$ if $d = 3$ and $s = 2$ otherwise. Then if we write $\lambda = \mu/\nu$ as above, we have $\nu \in \Sigma \cdot (K^\times)^s$. Suppose that $\nu^d f(\lambda) \not\in \Sigma \cdot (K^\times)^s$, which is equivalent to saying that $f(\lambda) \not\in \Sigma \cdot (K^\times)^s$. Then there is a prime element $p$ dividing $(\nu^d f(\lambda))$ but not $(2\nu^{2d-2} \Delta)$ (so $p \nmid (2\Delta)$ and $p \not\in S$ as before) and such that the maximum integer $m \geq 1$ with $p^m \mid (\nu^d f(\lambda))$ satisfies $v_p(m) \leq v_p(s) - 1$. Then Theorem 1.1 implies that $G_{2, \lambda} \cap Sp(T_2(J_{\lambda})) \supseteq \Gamma(4)$ both when $d = 3$ and when $d \geq 5$. Therefore, to prove (b) it suffices to show that $f(\lambda) \in \Sigma \cdot (K^\times)^s$ for only finitely many $\lambda \in K$. This follows from the same argument as above, on observing by Riemann–Hurwitz that the curves given by $\xi y^s = f(x)$ have genus $\geq 2$.

Finally, assume that $d \geq 4$ is even and choose any $\lambda = \mu/\nu \in K$ as before. Let $s = 4$ if $d = 4$ and let $s = 2$ otherwise. Suppose that $\nu^d f(\lambda) \not\in \Sigma \cdot (K^\times)^s$, which in both cases is equivalent to saying that $f(\lambda) \not\in \Sigma \cdot (K^\times)^s$. Then there is a prime element $p$ dividing $(\nu^d f(\lambda))$ but not $(2\nu^{2d-2} \Delta)$ (so $p \nmid (2\Delta)$ and $p \not\in S$ as before) and such that the maximum integer $m \geq 1$ with $p^m \mid (\nu^d f(\lambda))$ satisfies $v_p(m) \leq v_p(s) - 1$. Then Theorem 1.1 implies that $G_{2, \lambda} \cap Sp(T_2(J_{\lambda}))$ strictly contains $\Gamma(16)$ (resp. $\Gamma(4)$). Therefore, to prove (c) it suffices to show that $f(\lambda) \in \Sigma \cdot (K^\times)^s$ for only finitely many $\lambda \in K$, which likewise follows from checking that the curves given by $\xi y^s = f(x)$ have genus $\geq 2$. □
Remark 5.2. Parts (b) and (c) of Theorem 5.1 say that for a given polynomial $f$ of degree $d \neq 4$, there are many elements $\lambda \in K$ such that $G_{2,\lambda} \cong \Gamma(4)$. In these cases, it is always possible to compute the full structure of $G_2$ and determine its index in $GSp_2(J_\delta)$ by considering the Galois action on the 4-torsion subgroup of $J$ and using formulas for the generators of the 4-division field $K(J[4])$ over $K$. Such formulas are provided by [20, Proposition 3.1] in the case that $d$ is odd and are found in [19, §2.4] in the case that $d$ is even.

6. AN ALTERNATE APPROACH TO PRODUCING THE TRANSVECTIONS

In this final section, we briefly discuss another method of proving Proposition 2.6 in the $\ell = 2$ case, suggested by one of the referees, which involves Néron models of Jacobians with semi-abelian reduction rather than Galois actions on étale fundamental groups of punctured projective lines.

We assume all of the notation of §2, in particular that we have a strictly Henselian DVR $R_p$ with uniformizer $\pi$ and are considering the hyperelliptic curve $C$ defined over its field of fractions $K_p$; to simplify notation, we write $R$ and $K$ for $R_p$ and $K_p$ respectively, and we write $k$ for the residue field $R/p$. As in §2, our curve $C$ is defined by the equation $y^2 = \prod_{i=1}^d (x - \alpha_i)$, where the roots $\alpha_i$ all lie in $R$; for $1 \leq i \leq d$, let $\bar{\alpha}_i$ denote the image modulo $p$ of $\alpha_i$. We assume that the elements $\bar{\alpha}_i \in k$ are all distinct except that $\bar{\alpha}_1 = \bar{\alpha}_2$ and let $m \geq 1$ be the greatest integer such that $\pi^m | (\alpha_1 - \alpha_2)$; this precisely is the main hypothesis of Proposition 2.6, except that we are assuming without loss of generality that $\alpha_1$ and $\alpha_2$ are the two roots which coalesce in the reduction. If $d = 2g + 1$, the curve has a single point at infinity which we denote by $\infty \in C(K)$; if $d = 2g + 2$, the curve has two points at infinity which we denote by $\infty_1, \infty_2 \in C(K)$.

The Jacobian $J/k$ of $C$ admits a Néron model $J/R$, which is a smooth, commutative group scheme. Writing and $J_k$ for the special fiber of $J$, we see that $J_k$ is a (not necessarily connected) commutative group variety over $k$; we denote the connected component containing the identity by $J_k^0$. The hypothesis that only the roots $\alpha_1$ and $\alpha_2$ are equivalent modulo $p$ implies that $C$ has semistable reduction at $p$. Therefore, the Jacobian $J/k$ has semiabelian reduction by [5, Corollary 9.7.2], which means that $J_k^0$ decomposes as an extension of an abelian variety by a torus $T \subseteq J_k$.

Lemma 6.1. The group of connected components $J_k / J_k^0$ is isomorphic to $\mathbb{Z}/2m\mathbb{Z}$.

Proof. Let $C'/R$ be the projective curve defined over $R$ by the same equations defining $C/K$. It is easy to verify that the special fiber of $C'$ has a node of thickness $2m$ at the point $(\bar{\alpha}_1, 0)$, where $\bar{\alpha}_1 = \bar{\alpha}_2$ is the image in $k$ of $\alpha_1$, $\alpha_2 \in R$. Let $C/R$ be the minimal desingularization of $C'$. By [11, Corollary 10.3.25], the special fiber of $C$ has $2m$ irreducible components, configured in such a way that its dual graph $\Gamma(C)$ (which corresponds to intersections between irreducible components and whose edges correspond to intersections between intersections between irreducible components) consists of a single cycle of length $2m$. It then follows from [5, Remark 9.6.12] that $J_k / J_k^0 \cong \mathbb{Z}/2m\mathbb{Z}$.

Let $T_2(J_k)$ denote the 2-adic Tate module of the commutative algebraic group $J_k$; we identify it with the submodule $T_2(J)^{G_K} \subset T_2(J)$ of invariants under the absolute Galois group $G_K^0$ of $K$ (to see this identification, recall that since $R$ is strictly Henselian, the absolute Galois group of $K$ coincides with its inertia subgroup, and use [8, Proposition 2.2.5]). Letting $T_2(T)$ be the 2-adic Tate module of the torus $T$, we now have a filtration $T_2(T) \subseteq T_2(J)^{G_K} \subset T_2(J)$.

Lemma 6.2. The submodule $T_2(T) \subset T_2(J)$ has rank 1 and is generated over $\mathbb{Z}_2$ by an element whose image in $T_2(J)/T_2(T) = J[2]$ is the class of the divisor $D$ given by $(\alpha_1, 0) + (\alpha_2, 0) - 2(\infty) \in \text{Div}^0(C)$ if $d = 2g + 1$ and by $(\alpha_1, 0) + (\alpha_2, 0) - (\infty_1) - (\infty_2) \in \text{Div}^0(C)$ if $d = 2g + 2$.

Proof. By [5, Corollary 9.7.2], the identity component $J_k^0$ (whose special fiber is $J_k^0$ and whose generic fiber is $J$) can be identified with the degree-0 Picard scheme $\text{Pic}^0(C)/R$ of the relative curve $C/R$. In particular, the special fibers $J_k^0$ and $\text{Pic}^0(C_k)$ are isomorphic; let $\nu : C_k \to C_k$ be a normalization of $C_k$, and let $\nu^* : \text{Pic}^0(C_k) \to \text{Pic}^0(C_k)$ be the induced pullback. Now [5, Example 9.2.8] implies that the torus $T \subseteq J_k^0$ is identified under the isomorphism $J_k^0 \cong \text{Pic}^0(C_k)$ with the kernel of $\nu^*$, and that moreover, $T$ has rank equal to the rank of the singular cohomology group $H^1(\Gamma(C_k), \mathbb{Z})$, where $\Gamma(C_k)$ is the dual graph as in the proof of Lemma 6.1. It was shown in that proof that $\Gamma(C_k)$ consists of a single cycle, so this rank is 1 and the first claim is proved.
Now to prove the second claim, it is enough to show that the divisor class \([D]\) \(\in\text{Pic}^0(C)\) extends to a divisor class in \(\text{Pic}^0(C)\) whose restriction to \(\text{Pic}^0(C)\) lies in the kernel of \(\nu^*\). If \(d = 2g + 1\) (resp. if \(d = 2g + 2\)), then the divisor \(D\) is linearly equivalent to \(D' := \sum_{3\leq i \leq 2g+1} \alpha_i(0) + (2g-1)(\infty) \in \text{Div}^0(C)\) (resp. \(D := \sum_{3\leq i \leq 2g+2} \alpha_i(0) + g(\infty_1) - g(\infty_2) \in \text{Div}^0(C)\)) if \(d = 2g + 1\); thus, we have \([D] = [D']\). Now it is clear that the divisor \(D'\) extends to a divisor of \(C\) over \(R\); we denote its restriction to \(C_k\) also by \(D'\). Moreover, since the normalization \(\tilde{C}_k\) can be defined by the equation \(y^2 = \prod_{3\leq i \leq d} (x - \tilde{\alpha}_i)\) with \(\nu\) taking \((x, y)\) to \((x, y(x - \tilde{\alpha}_i)^{-1})\), it is clear that the pullback of \(D\) with respect to \(\nu\) is the divisor of the function \(y \in k(\tilde{C}_k)\) and therefore \(\nu^*((D')) = 0 \in \text{Pic}^0(\tilde{C}_k)\). Since \(2D \in \text{Div}^0(C)\) is the divisor of the function \((x - \tilde{\alpha}_1)(x - \tilde{\alpha}_2) \in \text{Div}^0(C)\) while an application of the Riemann–Roch formula shows that \(D\) itself is not principal, we see that \([D]\) generates \(\nu^*\) restricted to the 2-torsion subgroup of \(\text{Pic}^0(\tilde{C}_k)\), and it follows that \(T_2(T)\) is generated by an element whose image modulo 2 is the class of \(D\).

The statement of the following proposition essentially implies that of Proposition 2.6 for the \(\ell = 2\) case, given the well-known equivalence between the algebraic and topological characterizations of the 2-torsion subgroup of \(\text{Pic}^0(C)\) (as discussed in the footnote to the proof of [13, Lemma 8.12]).

**Proposition 6.3.** With all of the above notations and assumptions, the image of the natural action of \(G_K\) on \(T_2(J)\) is topologically generated by the element \(t_{c}^{2m} \in \text{Sp}(T_2(J))\) for some \(c \in T_2(J)\) whose image in \(T_2(J)/2T_2(J) = J[2]\) is the class of the divisor \((\alpha_1, 0) + (\alpha_2, 0) - 2(\infty) \in \text{Div}^0(C)\) (resp. \((\alpha_1, 0) + (\alpha_2, 0) - (\infty_1) - (\infty_2) \in \text{Div}^0(C)\)) if \(d = 2g + 1\) (resp. if \(d = 2g + 2\)).

**Proof.** Grothendieck’s Orthogonality Theorem [8, Théorème 2.4] says that the \(Z^2\)-submodules \(T_2(T), T_2(J)^{G_K} \subset T_2(J)\) are orthogonal to each other under the \(2\)-adic Weil pairing. It easily follows from this and from the fact that the action of \(G_K\) respects the Weil pairing that for any \(\sigma \in G_K\), the operator \(\rho_2(\sigma) - 1 \in \text{End}(T_2(J))\) has kernel containing \(T_2(J)^{G_K}\) and image contained in \(T_2(T)\) so that this operator induces a homomorphism \(T_2(J)/T_2(J)^{G_K} \rightarrow T_2(T)\); in fact, this yields a homomorphism

\[ N : G_K \rightarrow \text{Hom}_{Z_2}(T_2(J)/T_2(J)^{G_K}, T_2(T)) \]

given by sending an element \(\sigma \in G_K\) to the homomorphism \(T_2(J)/T_2(J)^{G_K} \rightarrow T_2(T)\) induced by \(\rho_2(\sigma) - 1\). Since the above group of \(Z_2\)-module homomorphisms is clearly itself a pro-2 group, the homomorphism \(N\) factors through the maximal pro-2 (tame) quotient \(G^{(2)}_K \cong Z_2\) of \(G_K\). The image of a generator of \(G^{(2)}_K\) under \(N\) can be interpreted in terms of the so-called *monodromy pairing* associated to \(T\) — see [14, §3.2] for a concise explanation. Now [8, Théorème 11.5] implies that the image under \(N\) of a generator of \(G^{(2)}_K\), viewed as a homomorphism in \(\text{Hom}_{Z_2}(T_2(J)/T_2(J)^{G_K}, T_2(T))\), has cokernel isomorphic to the 2-power part of \(J_K/J^0_K\). Lemma 6.1 implies that this cokernel is isomorphic to \(Z/2^{2(2m)}Z\). It follows from the above set-up that for some \(c \in T_2(J)\) which generates the rank-1 submodule \(T_2(T)\), the operator \(t_{c}^{2m} \in \text{Sp}(T_2(J))\) lies in the 2-adic Galois image associated to \(J\); by taking an appropriate power of this operator, we get that \(t_{c}^{2m}\) lies in this Galois image. Now Lemma 6.2 implies that the image of \(c\) modulo 2 is identified with the divisor class given in the statement of the proposition, and the proposition is proved.

**REFERENCES**

[1] S. Anni and V. Dokchitser, *Constructing hyperelliptic curves with surjective Galois representations*, arXiv preprint arXiv:1701.05915 (2017).

[2] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, J. Théor. Nombres Bordeaux 20 (2008), no. 1, 23–43.

[3] V.I. Arnold, *A remark on the ramification of hyperelliptic integrals as functions of parameters*, Vladimir I. Arnold-Collected Works, Springer, 1968, pp. 115–118.

[4] F.A. Bogomolov, *Points of finite order on an abelian variety*, Izv. Akad. Nauk SSSR Ser. Mat. 17 (1981), no. 1, 55–72.

[5] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, vol. 21, Springer Science & Business Media, 2012.

[6] A. Cadoret and A. Tamagawa, *A uniform open image theorem for \(\ell\)-adic representations, I*, Duke Math. J. 161 (2012), no. 13, 2605–2634.

[7] B. Farb and D. Margalit, *A primer on mapping class groups* (PMS-49), Princeton University Press, 2011.

[8] A. Grothendieck and M. Raynaud, *Modeles de Néron et monodromie*, Groupes de Monodromie en Géométrie Algébrique, Springer, 1972. pp. 313–523 (French).

[9] H. Hasson and J. Yelton, *Prime-to-pétale fundamental groups of punctured projective lines over strictly Henselian fields*, Trans. Amer. Math. Soc., 2020, (to appear).
How to cite this article: Yelton J. Boundedness results for 2-adic Galois images associated to hyperelliptic Jacobians. Mathematische Nachrichten. 2021;294:1629–1643. https://doi.org/10.1002/mana.201800244