BOUNDEDNESS RESULTS FOR 2-ADIC GALOIS IMAGES ASSOCIATED TO HYPERELLIPTIC JACOBIANS

JEFFREY YELTON

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 $f \in \mathcal{O}_K$ of discriminant Δ 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 (2Δ), then the image of the natural 2-adic Galois representation is open in $\mathrm{GSp}(T_2(J))$ and contains a certain congruence subgroup of $\mathrm{Sp}(T_2(J))$ 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.

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 ℓ, we let $T_\ell(J)$ denote the ℓ-adic Tate module of J, which is a free $\mathbb{Z}_\ell$-module of rank $2g$. We write $\rho_\ell : G_K \to \mathrm{Aut}(T_\ell(J))$ for the natural ℓ-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 $\mathrm{Sp}(T_\ell(J))$ denote the group of symplectic automorphisms of $T_\ell(J)$ with respect to the pairing e_ℓ, and let

$$\mathrm{GSp}(T_\ell(J)) := \{\sigma \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(J)) \mid e_\ell(P^\sigma, Q^\sigma) = e_\ell(P,Q)^{\chi_\ell(\sigma)} \ \forall P, Q \in T_2(J)\}$$

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

It is well known that the image G_ℓ of ρ_ℓ is always a closed subgroup of $\mathrm{GSp}(T_\ell(J))$ and that in fact there is some hyperelliptic Jacobian J of a given dimension g such that the inclusion $G_\ell \subseteq \mathrm{GSp}(T_\ell(J))$ has finite index (or equivalently, that G_ℓ is an open subgroup of the ℓ-adic Lie group $\mathrm{GSp}(T_\ell(J))$); see for instance [16, Theorem 1.1]. Note that the subgroup $G_\ell \cap \mathrm{Sp}(T_\ell(J)) \subset G_\ell$ coincides with the image of the Galois subgroup which fixes the extension $K(\mu_\ell)/K$ obtained by adjoining all ℓ-power roots of unity to K. Since K is a number field, the extension $K(\mu_\ell)/K$ is infinite; it follows that $G_\ell \not\subset \mathrm{Sp}(T_\ell(J))$ and that G_ℓ has finite index in $\mathrm{GSp}(T_\ell(J))$ if and only if $G_\ell \cap \mathrm{Sp}(T_\ell(J))$ has finite index in $\mathrm{Sp}(T_\ell(J))$.

There have been many results stating that G_ℓ has finite index in $\mathrm{GSp}(T_\ell(J))$ 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 $y^2 = f(x)$ or $y^2 = f(x)(x-\lambda)$ with $\lambda \in K$, where the Galois group of f is the full symmetric or alternating group ([17, Theorem 2.5] and [18, Theorem 8.3]; see also [19, Theorem 1.3] for a variant of this where the curve is defined using two parameters). A. Cadoret and A. Tamagawa have also proven ([4, 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 ℓ-adic Galois action associated to all but finitely many fibers, and that in fact the indices of the

ℓ-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_ℓ in $\mathrm{GSp}(T_\ell(J))$ in such cases.

Our aim in this paper is to give some similar results on the openness of the 2-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 tell us anything about the ℓ-adic Galois images for odd primes ℓ. However, we are hopeful that it can be strengthened to show the openness of the ℓ-adic Galois images as well under the same or similar hypotheses as is implied by the Mumford-Tate conjecture, and to show that the ℓ-adic Galois images contain the full symplectic group for almost all ℓ.)

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 $\mathrm{Sp}(T_2(J))$ by $\Gamma(N) := \{\sigma \in \mathrm{Sp}(T_2(J)) \mid \sigma \equiv 1 \pmod{N}\}$. 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 Δ. 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 2-adic Galois image G_2 as above. Then if there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ which divides $(f(\lambda))$ but not (2Δ), the Lie subgroup $G_2 \subset \mathrm{GSp}(T_2(J))$ is open. In fact, we have $G_2 \cap \mathrm{Sp}(T_2(J)) \supsetneq \Gamma(2^{2v_2(m)+2})$, where $m \geq 1$ is the greatest integer such that $\mathfrak{p}^m \mid (f(\lambda))$. If in addition $d = 3$, then $G_2 \cap \mathrm{Sp}(T_2(J)) \supsetneq \Gamma(2^{v_2(m)+1})$.*

Theorem 1.2. *Assume the same notation as in the statement of Theorem 1.1, except that the defining equation of the hyperelliptic curve is $y^2 = f(x)(x-\lambda)(x-\lambda')$ for distinct elements $\lambda, \lambda' \in \mathcal{O}_K$. Then if there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ which divides $(f(\lambda))$ but not $(\lambda - \lambda')$ or (2Δ) and a prime $\mathfrak{p}'$ which divides $(\lambda - \lambda')$ but not $(f(\lambda))$ or (2Δ), the Lie subgroup $G_2 \subset \mathrm{GSp}(T_2(J))$ is open. In fact, we have $G_2 \cap \mathrm{Sp}(T_2(J)) \supsetneq \Gamma(2^{2v_2(m)+2})$ if $v_2(m') \leq v_2(m)$ or $d = 2g$ and $G_2 \cap \mathrm{Sp}(T_2(J)) \supsetneq \Gamma(2^{v_2(m)+v_2(m')+2})$ 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 $\mathfrak{p}'^{m'} \mid (\lambda - \lambda')$. If in addition $d = 2$, then $G_2 \cap \mathrm{Sp}(T_2(J)) \supsetneq \Gamma(2^{\max\{v_2(m), v_2(m')\}+1})$.*

Remark 1.3. For a fixed irreducible monic polynomial $f \in \mathcal{O}_K[x]$ of degree $d \geq 2$ with discriminant Δ, it is not hard to show using Faltings' Theorem that the hypotheses in Theorems 1.1 is satisfied for almost all $\lambda \in \mathcal{O}_K$, as we will see in §5 (Remark 5.2 below). 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.

Remark 1.4. 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 [13, Theorem 2.4]), so that each endomorphism commutes with the action of $\mathrm{Gal}(\bar{K}/K')$ on torsion points. Note that the only endomorphisms in $\mathrm{End}(T_\ell(J))$ which commute with everything in an open subgroup of $\mathrm{GSp}(T_\ell(J))$ are scalars. It therefore follows from the above theorems that the endomorphism ring of any hyperelliptic Jacobian J satisfying the hypotheses of Theorem 1.1 or of Theorem 1.2 coincides with $\mathbb{Z}$ and that such a J is absolutely simple.

The key ingredient used in proving the above theorems is a method of describing Galois actions on ℓ-adic Tate modules of hyperelliptic Jacobians defined over strictly Henselian local fields 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 ([7]). This way of looking at ℓ-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 [7], which show that over a strictly Henselian local field of characteristic $p \neq 2$, for primes $\ell \neq p$, the ℓ-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 2.5) 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 2-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 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). Finally, in §5, we will assume that K has class number 1 and 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 [4, Theorems 1.1 and 5.1].

The author is grateful to a MathOverflow user whose comment on question 264281 helped to inspire the arguments for the results in §5.

2. Hyperelliptic Jacobians over local fields and tame Galois actions

We retain all notation introduced in the previous section. In this section, we write $\widehat{\mathbb{Z}}$ for the profinite completion of $\mathbb{Z}$ and use the symbol $\widehat{\pi}_1$ 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. For any profinite group G, let $G^{(p')}$ denote its 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 $\mathfrak{p}$ of K of residue characteristic $p \neq 2$. Fix a strict Henselization of the localization of K at the prime $\mathfrak{p}$ and denote it by $\mathcal{R}_\mathfrak{p}$ and its fraction field by $\mathcal{K}_\mathfrak{p}$; this comes with an embedding $\mathcal{K}_\mathfrak{p} \hookrightarrow \bar{K}$. Let $\pi \in K$ be a uniformizer of the discrete valuation ring $\mathcal{R}_\mathfrak{p}$. We fix a compatible system of Nth roots of unity $\zeta_N \in \bar{K}$ for $N = 1, 2, 3, ...$; that is, we require that $\zeta_{N'N}^{N'} = \zeta_N$ 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 $G_{K,\mathfrak{p}}$ denote the absolute Galois group of $\mathcal{K}_\mathfrak{p}$, and let $G_{K,\mathfrak{p}}^{\text{tame}}$ denote its tame quotient. It follows from a special case of Abhyankar's Lemma that the maximal tamely ramified extension $\mathcal{K}_\mathfrak{p}^{\text{tame}}$ is given by $\mathcal{K}_\mathfrak{p}(\{\pi^{1/N}\}_{(N,p)=1})$, where $\pi^{1/N}$ denotes an Nth root of π, and that $G_{K,\mathfrak{p}}^{\text{tame}} \cong \widehat{\mathbb{Z}}^{(p')}$ is topologically generated by the automorphism which acts on K^{tame} by fixing K and sending each $\pi^{1/N}$ to $\zeta_N \pi^{1/N}$.

We fix, once and for all, an embedding $\bar{K} \hookrightarrow \mathbb{C}$ where ζ_N is sent to $e^{2\pi\sqrt{-1}/N}$ for $N \geq 1$, so that we have an inclusion $\mathcal{K}_\mathfrak{p} \subset \mathbb{C}$. Let $d \geq 2$ be an integer and choose distinct integral elements $\alpha_1, ..., \alpha_d \in K$. Choose polynomials $\tilde{\alpha}_1, ..., \tilde{\alpha}_d \in \mathbb{C}[x]$ satisfying $\tilde{\alpha}_i(\pi) = \alpha_i$ for $1 \leq i \leq d$ and such that the x-adic valuation of $\tilde{\alpha}_i$ and $\tilde{\alpha}_j$ and the π-adic valuation of α_i and α_j are equal (such polynomials exist as is shown in the discussion in [7, §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 $z \in B_\varepsilon^* := \{z \in \mathbb{C} \mid |z| < \varepsilon\} \smallsetminus \{0\}$. We define a

family $\mathcal{F} \to B_\varepsilon^*$ of d-times-punctured Riemann spheres by letting

$$\mathcal{F} = \mathbb{P}^1_{\mathbb{C}} \times B_\varepsilon^* \smallsetminus \bigcup_{i=1}^{d} \{(\tilde{\alpha}_i(z), z) \mid z \in B_\varepsilon^*\}.$$

Choose a basepoint $z_0 \in B_\varepsilon^*$. The fundamental group $\pi_1(B_\varepsilon^*, z_0)$ acts by monodromy on the fundamental group $\pi_1(\mathcal{F}_{z_0}, \infty)$ of the fiber over z_0 with basepoint ∞. We write $\rho_{\text{top}} : \pi_1(B_\varepsilon^*, z_0) \to \text{Aut}(\pi_1(\mathcal{F}_{z_0}, \infty))$ for this action. The action ρ_{top} extends uniquely to a continuous action of the profinite completion $\widehat{\pi}_1(B_\varepsilon^*, z_0)$ on the profinite completion $\widehat{\pi}_1(\mathcal{F}_{z_0}, \infty)$ (see the discussion in [7, §1.1]), which we also denote by ρ_{top}. We note that $\widehat{\pi}_1(B_\varepsilon^*, z_0)$ is isomorphic to $\widehat{\mathbb{Z}}$ and is topologically generated by the element $\delta \in \pi_1(B_\varepsilon^*, z_0)$ 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 $G_{K,\mathfrak{p}}$ acts naturally on the étale fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{K}_\mathfrak{p}} \smallsetminus \{\alpha_1, ..., \alpha_d\}, \infty)$ via the $K_\mathfrak{p}$-point lying under the geometric point $\infty : \text{Spec}(\mathbb{C}) \to \mathbb{P}^1_{K_\mathfrak{p}} \smallsetminus \{\alpha_1, ..., \alpha_d\}$. After identifying $\pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{K}} \smallsetminus \{\alpha_1, ..., \alpha_d\}, \infty)^{(p')}$ with $\widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_d\}, \infty)^{(p')}$ via Riemann's Existence Theorem and the inclusion of algebraically closed fields $\bar{\mathcal{K}}_\mathfrak{p} \subset \mathbb{C}$, we write $\rho_{\text{alg}} : G_{K,\mathfrak{p}} \to \text{Aut}(\widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_d\}, \infty)^{(p')})$ for this action. We denote the actions on prime-to-p quotients of étale fundamental groups induced by ρ_{top} and ρ_{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 γ with its image in M. We define the *Dehn twist* on M with respect to the loop γ. 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 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 γ, we will denote it by $D_{[\gamma]}$. (See [5, Chapter 3] for more details.)

The following theorem is a compilation of all the necessary results describing and comparing ρ_{top} and ρ_{alg} that are proven in [7] (Theorems 1.2 and 2.3 and Remark 3.10 of that paper).

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

a) Let $\mathcal{I}$ be the set of all pairs (I, n) where $I \subseteq \{1, ..., d\}$ is a subset and $n \geq 1$ is an integer such that $x^n \mid \tilde{\alpha}_i - \tilde{\alpha}_j \in \mathbb{C}[x]$ for all $i, j \in I$ and such that I is maximal among intervals with this property. If ε is small enough, there exist pairwise nonintersecting loops $\gamma_{I,n} : [0, 1] \to \mathcal{F}_{z_0} \smallsetminus \{\infty\}$ for each $(I, n) \in \mathcal{I}$ such that $\delta \in \pi_1(B_\varepsilon^*, z_0)$ acts on $\pi_1(\mathcal{F}_{z_0}, \infty)$ in the same way that the product $\prod_{(I,d)\in\mathcal{I}} D_{[\gamma_{I,n}]}$ of Dehn twists on $\mathcal{F}_{z_0} \smallsetminus \{\infty\}$ 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 $\{\tilde{\alpha}_j(z_0)\}_{j=1}^d \cup \{\infty\}$, 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 $\pi_1(B_\varepsilon^*, z_0)^{(p')}$ and $G_{K,\mathfrak{p}}^{\text{tame}}$ respectively.

c) We have isomorphisms $\widehat{\pi}_1(B_\varepsilon^*, z_0)^{(p')} \xrightarrow{\sim} G_{K,\mathfrak{p}}^{\text{tame}}$ and $\phi : \widehat{\pi}_1(\mathcal{F}_{z_0}, \infty)^{(p')} \xrightarrow{\sim} \widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_d\}, \infty)^{(p')}$ inducing an isomorphism of the actions $\rho_{\text{top}}^{(p')}$ and $\rho_{\text{alg}}^{(p')}$. Moreover, we can choose the isomorphism ϕ so that it takes any element represented by a loop on $\mathcal{F}_{z_0}$ whose image in $\mathbb{P}^1_{\mathbb{C}}$ separates some singleton $\{\tilde{\alpha}_i(z_0)\}$ from its complement in $\{\tilde{\alpha}_j(z_0)\}_{j=1}^d \cup \{\infty\}$ to an element represented by a loop on $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_d\}$ whose image in $\mathbb{P}^1_{\mathbb{C}}$ separates the singleton $\{\alpha_i\}$ from its complement in $\{\alpha_j\}_{j=1}^d \cup \{\infty\}$.

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_ε^*; moreover, this is isomorphic to the algebraic action $\rho_{\text{alg}}^{(p')}$ 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 α_i.

We now want to relate this to the action of $G_{K,\mathfrak{p}}$ on the prime-to-p étale fundamental group of a smooth hyperelliptic curve over $K_{\mathfrak{p}}$. Let $\mathfrak{C}$ 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 $z_i \in \mathcal{K}_{\mathfrak{p}}$; if d is odd (resp. even), then $d = 2g+1$ (resp. $d = 2g+2$). The hyperelliptic curve $\mathfrak{C}$ comes with a surjective degree-2 morphism $\mathfrak{C} \to \mathbb{P}^1_{\mathbb{C}}$ defined by projecting onto the x-coordinate. It is well known that this projection ramifies at ∞ 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. Write $\mathfrak{B} \subset \mathfrak{C}(\mathbb{C})$ for the set of inverse images of these ramification points in $\mathbb{P}^1_{\mathbb{C}}$ ($\mathfrak{B}$ is the set of *branch points* of $\mathfrak{C}$). Clearly the restriction to $\mathfrak{C} \smallsetminus \mathfrak{B}$ of the above projection map yields a finite degree-2 étale morphism $\mathfrak{C} \smallsetminus \mathfrak{B} \to \mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}$. Choose a basepoint P of the topological space $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_d\}$ and a basepoint Q of the topological space $\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}$ 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

$$\widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}, P) \rhd \widehat{\pi}_1(\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}, Q) \twoheadrightarrow \widehat{\pi}_1(\mathfrak{C}(\mathbb{C}), Q) \twoheadrightarrow H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) \tag{1}$$

induced by the maps $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\} \leftarrow \mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B} \hookrightarrow \mathfrak{C}(\mathbb{C})$ and by identifying the first singular homology group of $\mathfrak{C}(\mathbb{C})$ with the abelianization of its fundamental group. The inclusion in (1) is an inclusion of a characteristic subgroup, so any automorphism of $\widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}, P)$ induces an automorphism of $\widehat{\pi}_1(\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}, P)$.

We write $\mathfrak{J}$ for the Jacobian of $\mathfrak{C}$. There is a well-known identification of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell$ with $H_1(\mathfrak{J}(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell$ and in turn with $T_\ell(\mathfrak{J})$ for any prime ℓ. Moreover, the intersection pairing on $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ defined above carries over to the canonical Riemann form on the complex abelian variety $\mathfrak{J}(\mathbb{C})$ and in turn to the Weil pairing e_ℓ on $T_\ell(\mathfrak{J})$ (see the results in [8, §IV.4 and §VIII.1] and in [9, §24]). Given an element $c \in H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$, we also write c for the element $c \otimes 1 \in H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell = T_\ell(\mathfrak{J})$. It is not difficult to show that the action of $G_{K,\mathfrak{p}}$ on $T_\ell(\mathfrak{J})$ induced by $\rho_{\text{alg}}^{(p')}$ via these identifications is the natural ℓ-adic Galois action ρ_ℓ: see, for instance, step 5 of the proof of [16, Proposition 2.2].

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

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

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

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

(ii) the (skew-symmetric) intersection pairing $\langle \cdot, \cdot \rangle$ on $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ is determined by $\langle a'_i, b'_i \rangle = -1$ 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, for instance, the first figure in [3]*, or* [5, Figure 6.1]*.)*

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

From now on, given a complex hyperelliptic curve $\mathfrak{C}$, we fix a symplectic basis $\{a'_1, ..., a'_g, b'_1, ..., b'_g\}$ of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$. In order to prove Proposition 2.5 below, we require a couple of lemmas, the first of which is purely topological.

Lemma 2.3. *Assume all of the above notation.*

a) Let $\gamma \subset \mathbb{P}^1_{\mathbb{C}}$ be the image of a simple closed loop on $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_{2g+2}, P\}$ which separates the set of α_i's into two even-cardinality subsets. Then the inverse image of γ under the ramified degree-2 covering map $\mathfrak{C}(\mathbb{C}) \to \mathbb{P}_{\mathbb{C}}$ consists of two connected components, each of which are simple closed

loops whose homology classes $\pm c \in H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ differ by sign. As a particular case, if $\gamma_i \subset \mathbb{P}^1_{\mathbb{C}}$ is the image of a loop which separates $\{z_i, z_{2g+1}\}$ from its complement in $\{z_j\}_{j=1}^{2g+2}$ for some i, then the homology classes of these simple closed loops on $\mathfrak{C}(\mathbb{C})$ lying above γ_i are given by $\pm c_i'$ for some element $c_i' \in H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ which is equivalent modulo 2 to

$$\begin{cases} a'_{(i+1)/2} + ... + a'_g + b'_{(i+1)/2} & i \text{ odd} \\ a'_{i/2+1} + ... + a'_g + b'_{i/2+1} & i \text{ even} \end{cases} \tag{2}$$

b) With γ and c as above, the Dehn twist $D_{[\gamma]}$ induces an automorphism of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ via the inclusion and quotient maps in (1), which is given by $T_c^2 \in \mathrm{Aut}(H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}))$.

Proof. The essential ideas of this argument are contained in the proof of [10, Lemma 8.12]. The maximal abelian exponent-2 quotient of $\pi_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}, P)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g+1}$ and is identified with the group of partitions of $\{z_i\}_{i=1}^{2g+2}$ into two subsets (where the addition law is given by symmetric differences), by sending the homology class of any loop $\gamma \subset \mathbb{P}^1_{\mathbb{C}}$ to the subsets of z_i's lying in each connected component of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \gamma$. We have a homomorphism of homology groups (composed with reduction modulo 2) $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) \to H_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}, \mathbb{Z}/2\mathbb{Z})$ coming from the inclusion of fundamental groups in (1). By [3, Lemma 1], this homomorphism factors through $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}/2\mathbb{Z})$. It is clear from this that we have an inclusion of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}/2\mathbb{Z})$ as the subgroup of $H_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}, \mathbb{Z}/2\mathbb{Z})$ which is generated by the partitions $\{z_{2i-1}, z_{2i}\} \cup \{z_1, ..., z_{2i-2}, z_{2i+1}, ..., z_{2g+2}\}$ and $\{z_{2i}, ..., z_{2g+1}\} \cup \{z_1, ..., z_{2i-1}, z_{2g+2}\}$ for $1 \leq i \leq g$. It follows from an easy combinatorial argument that this subgroup consists of the partitions of $\{z_i\}_{i=1}^{2g+2}$ into even-cardinality subsets. Thus, any loop $\gamma \in \pi_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}, P)$ whose image modulo 2 is such a partition lifts to a loop $c \in \pi_1(\mathfrak{C}(\mathbb{C}), Q)$; the only other choice of loop on $\mathfrak{C}(\mathbb{C})$ whose image is γ must be based at $\iota(Q)$ and equal to the composition of the path γ with ι, where $\iota : \mathfrak{C}(\mathbb{C}) \to \mathfrak{C}(\mathbb{C})$ is the only nontrivial deck transformation. Since ι acts on the homology group by sign change (see [5, §7.4]), this loop must be $-c$. If the image of γ 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). Thus, (a) is proved.

Every self-homeomorphism of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{z_1, ..., z_{2g+2}\}$ fixing P lifts uniquely to a self-homeomorphism of $\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}$ fixing Q under which the image of a loop wrapping around a single point in $\mathfrak{B}$ is also a loop wrapping around a single point in $\mathfrak{B}$. Since the kernel of the quotient map $\pi_1(\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}, Q) \twoheadrightarrow \pi_1(\mathfrak{C}(\mathbb{C}), Q)$ is generated by squares of homotopy classes of such loops, it follows that $D_{[\gamma]}$ induces an automorphism of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ via the maps in (1). It is clear that the unique self-homeomorphism of $\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}$ fixing Q lifting a representative of $D_{[\gamma]}$ must represent the composition of Dehn twists on $\mathfrak{C}(\mathbb{C}) \smallsetminus (\mathfrak{B} \cup \{Q\})$ with respect to the two lifts of γ on $\mathfrak{C}(\mathbb{C}) \smallsetminus (\mathfrak{B} \cup \{Q\})$, which are $\pm c$. Therefore, the induced automorphism of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) = H_1(\mathfrak{C}(\mathbb{C}) \smallsetminus \{Q\}, \mathbb{Z})$ is determined by the product of D_c and D_{-c}. Since Dehn twists do not depend on the orientation of loops, this product is D_c^2. Now (b) follows from the well known fact (see [5, Proposition 6.3]) that the Dehn twist D_c acts on $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ as the transvection T_c since $\mathfrak{C}(\mathbb{C})$ is a compact smooth manifold.

□

Lemma 2.4. *Let $\alpha_1, ..., \alpha_d$ be distinct elements in $\mathcal{R}_{\mathfrak{p}}$. There exist elements $\alpha_1', ..., \alpha_{d+1}' \in \mathcal{R}_{\mathfrak{p}}$ 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 $\alpha_{d+1}' - \alpha_i' \in \mathcal{R}_{\mathfrak{p}}^{\times}$ for $1 \leq i \leq d$.

(ii) Let $\alpha_{d+1} = \infty \in \mathbb{P}^1_{\mathcal{K}_{\mathfrak{p}}}$. There is a $\mathcal{K}_{\mathfrak{p}}$-isomorphism

$$\psi : \mathbb{P}^1_{\bar{\mathcal{K}}_{\mathfrak{p}}} \smallsetminus \{\alpha_1, ..., \alpha_{d+1}\} \xrightarrow{\sim} \mathbb{P}^1_{\bar{\mathcal{K}}_{\mathfrak{p}}} \smallsetminus \{\alpha_1', ..., \alpha_{d+1}'\}$$

such that the induced isomorphism $\psi_* : \widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_{d+1}\}, \psi^{-1}(\infty)) \xrightarrow{\sim} \widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha'_1, ..., \alpha'_{d+1}\}, \infty)$ *yields an isomorphism of* ρ_{alg} *with the analogously defined representation* ρ'_{alg}*. The isomorphism* ψ_* *takes any element represented by a loop on* $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_{d+1}\}$ *whose image in* $\mathbb{P}^1_{\mathbb{C}}$ *separates some singleton* $\{\alpha_i\}$ *from its complement in* $\{\alpha_j\}_{j=1}^{d+1}$ *to an element represented by a loop on* $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha'_1, ..., \alpha'_{d+1}\}$ *whose image in* $\mathbb{P}^1_{\mathbb{C}}$ *separates the singleton* $\{\alpha'_i\}$ *from its complement in* $\{\alpha'_j\}_{j=1}^{d+1}$*.*

Proof. Choose $\beta \in \mathcal{R}_{\mathfrak{p}}^{\times}$ satisfying $\beta \not\equiv \alpha_j \pmod{\pi}$ for $1 \leq j \leq d$ (this is always possible because the residue field $\mathcal{R}_{\mathfrak{p}}/(\pi)$ is infinite). Let $\alpha'_j = \alpha_j\beta/(\beta - \alpha_j) \in \mathcal{R}_{\mathfrak{p}}$ for $1 \leq j \leq d$ and $\alpha'_{d+1} = \beta \in \mathcal{R}_{\mathfrak{p}}$, and let ψ be the $\mathcal{K}_{\mathfrak{p}}$-morphism given by $x \mapsto x\beta/(\beta - x)$. Then property (i) follows from straightforward computation. Since ψ is defined over $\mathcal{K}_{\mathfrak{p}}$, the isomorphism ψ_* is equivariant with respect to the action of $G_{K,\mathfrak{p}} = \mathrm{Gal}(\bar{\mathcal{K}}_{\mathfrak{p}}/\mathcal{K}_{\mathfrak{p}})$. Moreover, after base change to $\mathbb{C}$, ψ 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 ([6, Proposition 3.5(iv)]). For the statement of the below proposition, we fix a symplectic basis $\{a_1, ..., a_g, b_1, ..., b_g\}$ of $H_1(C(\mathbb{C}), \mathbb{Z})$; the image $\{a_1, ..., a_g, b_1, ..., b_g\} \subset T_\ell(J)$ forms a symplectic basis of $T_\ell(J)$ with respect to the Weil pairing.

Proposition 2.5. *Let* C *be a hyperelliptic curve of genus* g *over* $\mathcal{K}_{\mathfrak{p}}$ *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* $\alpha_1, ..., \alpha_d \in \mathcal{R}_{\mathfrak{p}}$*, and let* J *be its Jacobian. Suppose that exactly* 2 *of the roots,* α_i *and* α_j*, are equivalent modulo* π*, and let* $m \geq 1$ *be the maximal integer such that* $\pi^m \mid (\alpha_i - \alpha_j)$*. Then for any prime* $\ell \neq 2, p$*, the image of the natural action of* $G_{K,\mathfrak{p}}$ *on* $T_\ell(J)$ *is topologically generated by the element* $T_c^{2m} \in \mathrm{Sp}(T_\ell(J))$ *for some* $c \in T_\ell(J)$ *determined by a loop on* $\mathbb{P}^1_{\mathbb{C}}$ *whose image separates* $\{\alpha_i, \alpha_j\}$ *from the rest of the roots. As a particular case, if* $i \leq 2g$ *and* $j = 2g + 1$*, then this* ℓ*-adic Galois image is topologically generated by* $T_{c_i}^{2m}$ *for some* $c_i \in H_1(C(\mathbb{C}), \mathbb{Z})$ *equivalent modulo* 2 *to* $a_{(i+1)/2} + ... + a_g + b_{(i+1)/2}$ *(resp.* $a_{i/2+1} + ... + a_g + b_{i/2+1}$*) if* i *is odd (resp. even).*

Proof. We first assume that $d = 2g + 2$. Let $\tilde{\alpha}_1, ..., \tilde{\alpha}_{2g+2} \in \mathbb{C}[x]$ be the elements constructed from the α_i's as above, and define the family $\mathcal{F} \to B_\varepsilon^*$ as above. It is clear from the hypothesis on the roots α_j that the set $\mathcal{I}$ 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 $\widehat{\pi}_1(B_\varepsilon^*, z_0)$ acts on $\widehat{\pi}_1(\mathcal{F}_{z_0}, \infty)$ via the monodromy action ρ_{top} as $D_{[\gamma_i]}^m$, where γ_i is a loop on $\mathcal{F}_{z_0} \smallsetminus \{\infty\}$ whose image in $\mathbb{P}^1_{\mathbb{C}}$ separates the subset $\{\tilde{\alpha}_i(z_0), \tilde{\alpha}_{2g+1}(z_0)\}$ from its complement in $\{\tilde{\alpha}_j(z_0)\}_{j=1}^{2g+2}$. Let $\mathfrak{C}$ be the complex hyperelliptic curve of degree $d = 2g + 2$ ramified over $\mathbb{P}^1_{\mathbb{C}}$ at the points $\tilde{\alpha}_1(z_0), ..., \tilde{\alpha}_d(z_0) \in \mathbb{C}$, which has a symplectic basis $\{a'_1, ..., a'_g, b'_1, ..., b'_g\}$ of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$. By Lemma 2.3, the automorphism of $\widehat{\pi}_1(\mathcal{F}_{z_0}, \infty)$ determined by $D_{[\gamma_i]}^m$ induces the automorphism of $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) \otimes \widehat{\mathbb{Z}}$ given by $T_{c_i}^{2m} : v \mapsto v + 2m\langle v, c'_i\rangle c'_i$, where $c'_i \in H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z})$ is equivalent modulo 2 to the formula in (2). Now parts (b) and (c) of Theorem 2.1 say that there is an isomorphism $\phi : \widehat{\pi}_1(\mathcal{F}_{z_0}, \infty)^{(p')} \xrightarrow{\sim} \widehat{\pi}_1(\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_d\}, \infty)^{(p')}$ making the action ρ_{top} isomorphic to the Galois action ρ_{alg}. Since $p \neq 2$ and $\mathfrak{C}(\mathbb{C}) \smallsetminus \mathfrak{B}$ and $C(\mathbb{C}) \smallsetminus \{(\alpha_i, 0)\}_{i=1}^{2g+2}$ are the only degree-2 covers of $\mathcal{F}_{z_0}$ and $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{\alpha_1, ..., \alpha_{2g+2}\}$ respectively, we see that the isomorphism ϕ induces an isomorphism $H_1(\mathfrak{C}(\mathbb{C}), \mathbb{Z}) \otimes \widehat{\mathbb{Z}}^{(p')} \xrightarrow{\sim} H_1(C(\mathbb{C}), \mathbb{Z}) \otimes \widehat{\mathbb{Z}}^{(p')}$ which we also denote by ϕ. It is clear from the property of ϕ 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 2.3 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 2.4, which allows us to replace $\alpha_1, ..., \alpha_{2g+1}, \alpha_{2g+2} := \infty$ with elements $\alpha'_1, ..., \alpha'_{2g+2} \in \mathcal{R}_{\mathfrak{p}}$ whose differences have the same valuations with respect to π.

Putting this all together, we see that the tame Galois action on $H_1(C(\mathbb{C}),\mathbb{Z})\otimes\widehat{\mathbb{Z}}^{(p')}$ induced by ρ_{alg} sends a generator of $G_{K,\mathfrak{p}}^{\text{tame}}$ to the automorphism of $H_1(C(\mathbb{C}),\mathbb{Z})\otimes\widehat{\mathbb{Z}}^{(p')}$ given by $v\mapsto v+2m\langle v,c_i\rangle_\phi c_i$ for some $c_i\in H_1(C(\mathbb{C}),\infty)\otimes\widehat{\mathbb{Z}}^{(p')}$ which is equivalent modulo 2 to the formula given in the statement. Here $\langle\cdot,\cdot\rangle_\phi$ is the skew-symmetric pairing on $H_1(C(\mathbb{Z}),\mathbb{Z})\otimes\widehat{\mathbb{Z}}^{(p')}$ induced by the interection pairing on $H_1(\mathfrak{C},\mathbb{Z})$ via ϕ; note that $\langle\cdot,\cdot\rangle_\phi$ is normalized so that $\langle H_1(C(\mathbb{C}),\mathbb{Z}),H_1(C(\mathbb{C}),\mathbb{Z})\rangle_\phi=\mathbb{Z}$. As above, we identify the maximal pro-ℓ quotient of $H_1(C(\mathbb{C}),\mathbb{Z})\otimes\widehat{\mathbb{Z}}^{(p')}$ with $T_\ell(J)$ and see that the natural ℓ-adic Galois action ρ_ℓ factors through $G_{K,\mathfrak{p}}^{\text{tame}}$ and takes a generator to the automorphism of $T_\ell(J)$ given by $v\mapsto v+2m\langle v,c_i\rangle_\phi c_i$. But this automorphism must lie in $\text{Sp}(T_\ell(J))$ by the Galois equivarience of the Weil pairing e_ℓ and the fact that $\mathcal{K}_\mathfrak{p}$ contains all ℓ-power roots of unity. It is now an easy exercise to verify that this implies that $\langle v,c_i\rangle_\phi=\pm e_\ell(v,c_i)$ for all $v\in T_\ell(J)$, and so the image of ρ_ℓ is generated by $T_{c_i}^{2m}:v\mapsto v+e_\ell(v,c_i)c_i$, as desired.

□

In order to prove Theorems 1.1 and 1.2, we will put some local data together to show using Proposition 2.5 that the ℓ-adic Galois image contains $\{T_{c_1}^{2m},...,T_{c_{2g}}^{2m}\}$ for homology classes c_i as above and a certain integer m. Therefore, it is of interest to investigate the subgroup that this set generates. Unfortunately, since the c_i's are only known modulo 2, not much 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, which is the goal of the next section.

3. Subgroups generated by powers of transvections

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 $\{a_1,...,a_g,b_1,...,b_g\}$ of M and assume that the pairing is determined by $\langle a_i,b_i\rangle=-1$ 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 $1\leq i\leq g$. Our main goal is to prove the following purely algebraic result.

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

$$\begin{cases} a_{(i+1)/2}+...+a_g+b_{(i+1)/2} & i \text{ odd} \\ a_{i/2+1}+...+a_g+b_{i/2+1} & i \text{ even} \end{cases} \tag{3}$$

for $1\leq i\leq 2g$. Then given integers $n,n'\geq 1$, the subgroup $G\subset\Gamma(2^n)\subset\text{Sp}(M\otimes\mathbb{Z}_2)$ generated by the elements $T_{c_1}^{2^n},...,T_{c_{2g-1}}^{2^n},T_{c_{2g}}^{2^{n'}}\in\Gamma(2^n)$ contains $\Gamma(2^{2n})$ (resp. $\Gamma(2^{n+n'})$) if $n'\leq n$ (resp. if $n'>n$). In particular, as a topological subgroup of $\text{Sp}(M\otimes\mathbb{Z}_2)$, G is open, and its associated Lie algebra $\mathfrak{g}$ coincides with the 2-adic symplectic Lie algebra $\mathfrak{sp}(M\otimes\mathbb{Q}_2)$.

Note that the image of any transvection $T\in\text{Sp}(M\otimes\mathbb{Z}_2)$ under the logarithm map is $T-1\in\mathfrak{sp}(M\otimes\mathbb{Q}_2)$ and that $\mathfrak{g}$ is generated as a Lie algebra by the logarithms of the transvections T_{c_i}. Therefore, in order to prove the second statement of this proposition, it suffices to show that $\{T_{c_s}-1\}_{1\leq s\leq 2g}$ generates the full Lie algebra $\mathfrak{sp}(M\otimes\mathbb{Q}_2)$. However, in order to get both statements, we will prove something slightly stronger which is given by the following lemma.

Lemma 3.2. *Let $t_i=T_{c_i}-1\in\mathfrak{sp}(M\otimes\mathbb{Q}_2)$ and let $\bar{t}_i$ denote the reduction of t_i modulo 2 for $1\leq i\leq 2g$. Then an $\mathbb{F}_2$-basis for $\mathfrak{sp}(M\otimes\mathbb{F}_2)$ is given by the set $\{\bar{t}_i\}_{1\leq i\leq 2g}\cup\{[\bar{t}_i,\bar{t}_j]\}_{1\leq i<j\leq 2g}$.*

Proof. Let $\bar{c}_i$ denote the reductions modulo 2 of the basis element c_i for $1 \leq i \leq 2g$. We know from the characterization of the c_i's modulo 2 given in the statement that $\{\bar{c}_1, ..., \bar{c}_{2g}\}$ is an ordered basis of $M \otimes \mathbb{F}_2$ with $\langle \bar{c}_i, \bar{c}_j \rangle = \langle \bar{c}_j, \bar{c}_i \rangle = 1 \in \mathbb{F}_2$ for $1 \leq i < j \leq 2g$. With respect to this basis, we may view $\mathfrak{sp}(M \otimes \mathbb{F}_2)$ as the Lie algebra $\mathfrak{sp}_{2g}(\mathbb{F}_2)$. Now it is well known that $\mathfrak{sp}_{2g}(\mathbb{F}_2)$ is a $(2g^2+g)$-dimensional vector space over $\mathbb{F}_2$. Since there are $2g^2+g$ elements listed in the set of $\bar{t}_s$'s and their commutators, it suffices to prove that this set is linearly independent over $\mathbb{F}_2$, using only the fact that $\langle \bar{c}_i, \bar{c}_j \rangle = \langle \bar{c}_j, \bar{c}_i \rangle = 1$ for $1 \leq i < j \leq 2g$. In order to do this, we first note that for any elements $a, b \in M \otimes \mathbb{F}_2$, the commutator of the logarithms of the transvections with respect to a and to b is the $\mathbb{F}_2$-linear operator in $\mathfrak{sp}_{2g}(\mathbb{F}_2)$ given by $v \mapsto \langle v, a \rangle \langle a, b \rangle b + \langle v, b \rangle \langle b, a \rangle a$ for all $v \in M \otimes \mathbb{F}_2$. Therefore, for $1 \leq i < j \leq 2g$, the linear operator $[\bar{t}_i, \bar{t}_j] = [\bar{t}_j, \bar{t}_i]$ is given by

$$v \mapsto \langle v, \bar{c}_i \rangle \bar{c}_j + \langle v, \bar{c}_j \rangle \bar{c}_i. \tag{4}$$

We compute using this formula that the upper left-hand 2×2 submatrices of $\bar{t}_1$, $\bar{t}_2$, and $[\bar{t}_1, \bar{t}_2]$ respectively are

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tag{5}$$

and therefore these elements of $\mathfrak{sp}_{2g}(\mathbb{F}_2)$ are linearly independent over $\mathbb{F}_2$. This in particular proves the statement for $g = 1$.

Now assume inductively that $g \geq 2$ and that the statement is true for $g-1$. Clearly, $\{\bar{c}_3, ..., \bar{c}_{2g}\}$ generates a $2(g-1)$-dimensional subspace $\mathfrak{g}'$ of $M \otimes \mathbb{F}_2$ which it generates, and the intersection pairing of any two distinct elements of this set is 1. Therefore, the inductive assumption implies that the $(2(g-1)^2 + (g-1))$-element set $\{\bar{t}_i\}_{3 \leq i \leq g} \cup \{[\bar{t}_i, \bar{t}_j]\}_{3 \leq i < j \leq 2g}$ is linearly independent; in fact, $\mathfrak{g}'$ is a copy of $\mathfrak{sp}_{2g-2}(\mathbb{F}_2)$ lying inside $\mathfrak{sp}_{2g}(\mathbb{F}_2)$.

We first claim that the subset $S_1 := \{\bar{t}_i\}_{1 \leq i \leq 2g} \cup \{[\bar{t}_1, \bar{t}_2]\} \cup \{[\bar{t}_i, \bar{t}_j]\}_{3 \leq i < j \leq 2g}$ is linearly independent. To see this, note that we have already shown that $\{\bar{t}_1, \bar{t}_2, [\bar{t}_1, \bar{t}_2]\}$ is linearly independent, and from the fact that the matrices in $\mathfrak{g}'$ have all 0's in their first and second rows, it is clear that $\bar{t}_1, \bar{t}_2, [\bar{t}_1, \bar{t}_2] \notin \mathfrak{g}'$. The elements of S_1 generating $\mathfrak{g}'$ are linearly independent by the inductive assumption, and so the claim follows.

We next claim that the subset $S_2 := \{[\bar{t}_1, \bar{t}_i]\}_{3 \leq i \leq 2g} \cup \{[\bar{t}_2, \bar{t}_i]\}_{3 \leq i \leq 2g}$ is linearly independent. In order to show this, consider a linear combination of elements of the set S_2 written as $\sum_{i=3}^{2g} \beta_i [\bar{t}_1, \bar{t}_i] + \sum_{i=3}^{2g} \gamma_i [\bar{t}_2, \bar{t}_i]$ with $\beta_i, \gamma_i \in \mathbb{F}_2$. Using the formula in (4), we see that this is the linear operator $u \in \mathfrak{sp}_{2g}(\mathbb{F}_2)$ given by

$$u : v \mapsto \sum_{i=3}^{2g} \beta_i (\langle v, \bar{c}_i \rangle \bar{c}_1 + \langle v, \bar{c}_1 \rangle \bar{c}_i) + \sum_{i=3}^{2g} \gamma_i (\langle v, \bar{c}_i \rangle \bar{c}_2 + \langle v, \bar{c}_2 \rangle \bar{c}_i)$$

$$= \langle v, \sum_{i=3}^{2g} \beta_i \bar{c}_i \rangle \bar{c}_1 + \langle v, \bar{c}_1 \rangle \sum_{i=3}^{2g} \beta_i \bar{c}_i + \langle v, \sum_{i=3}^{2g} \gamma_i \bar{c}_i \rangle \bar{c}_2 + \langle v, \bar{c}_2 \rangle \sum_{i=3}^{2g} \gamma_i \bar{c}_i. \tag{6}$$

Suppose that $u = 0$. Assume that $\sum_{i=3}^{2g} \beta_i \bar{c}_i \neq 0$. Then by the nondegeneracy of the symplectic pairing, we can choose $v \in M \otimes \mathbb{F}_2$ such that $\langle v, \sum_{i=3}^{2g} \beta_i \bar{c}_i \rangle = 1$. Then $u(v)$ written as a linear combination using the basis $\{\bar{c}_1, ..., \bar{c}_{2g}\}$ has $\bar{c}_1$-coefficient equal to 1, a contradiction because $u(v) = 0$. Therefore, $\sum_{i=3}^{2g} \beta_i \bar{c}_i = 0$, which implies that $\beta_3 = ... = \beta_{2g} = 0$. Now assume that $\sum_{i=3}^{2g} \gamma_i \bar{c}_i \neq 0$. Then similarly, we can choose $w \in M \otimes \mathbb{F}_2$ such that $\langle w, \sum_{i=3}^{2g} \gamma_i \bar{c}_i \rangle = 1$ and get that $u(w)$ has $\bar{c}_2$-coefficient equal to 1, a contradiction because $u(w) = 0$. Therefore, $\sum_{i=3}^{2g} \gamma_i \bar{c}_i = 0$, which implies that $\gamma_3 = ... = \gamma_{2g} = 0$, and so S_2 is linearly independent.

We finally claim that if a linear combination of elements in S_1 is equal to a linear combination of elements in S_2, then these linear combinations must be trivial. Since the full set of t_i's and their

commutators coincides with $S_1 \cup S_2$, this implies the statement of the proposition. Let $u \in \mathfrak{sp}_{2g}(\mathbb{F}_2)$ be a linear combination of elements in S_2, written as in (6) with $\beta_i, \gamma_i \in \mathbb{F}_2$, and assume that u also lies in the subspace generated by S_1. Now it is clear that each of the matrices in S_1 has the property that the $(1,j)$th entries are all equal and the $(2,j)$th entries are all equal for $3 \leq j \leq 2g$. Thus, we see by putting $\bar{c}_3, ..., \bar{c}_{2g}$ into our formula for u that $\beta_3 = ... = \beta_{2g}$ and $\gamma_3 = ... = \gamma_{2g}$. But then we have

$$\langle \bar{c}_1, \sum_{i=3}^{2g} \beta_i \bar{c}_i \rangle = \langle \bar{c}_1, \sum_{i=3}^{2g} \gamma_i \bar{c}_i \rangle = \langle \bar{c}_2, \sum_{i=3}^{2g} \beta_i \bar{c}_i \rangle = \langle \bar{c}_2, \sum_{i=3}^{2g} \gamma_i \bar{c}_i \rangle = 0, \tag{7}$$

and we get that the upper left-hand 2×2 submatrix of u is the 0 matrix. This is also true of any matrix in $\mathfrak{g}'$, so we know from what was given in (5) that t_1, t_2, and $[t_1, t_2]$ do not appear when u is written as a linear combination of elements in S_1, and therefore we have $u \in \mathfrak{g}'$. As was noted above, every matrix in $\mathfrak{g}'$ has all 0's in its first and second rows. Thus, for any $v \in M \otimes \mathbb{F}_2$, when $u(v)$ is written as a linear combination of $\bar{c}_i$'s, the $\bar{c}_1$-coefficient and the $\bar{c}_2$-coefficient are both 0. Now by the same argument that was used for the previous claim, we have $\beta_3 = ... = \beta_{2g} = \gamma_3 = ... = \gamma_{2g} = 0$. Therefore $u = 0$, as desired.

□

Proof (of Proposition 3.1) . For ease of notation, we write $n'' = \max\{n, n'\}$ and $N = n + n''$, so that the desired statement is that G contains the congruence subgroup $\Gamma(2^N)$. Since G 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 $\mathfrak{sp}_{2g}(\mathbb{Z}_2)$ which is equivalent to $T - 1$ 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 an element $t \in \mathfrak{sp}(M \otimes \mathbb{F}_2)$ to $1 + 2^{N+m-1}\tilde{t} \in \mathrm{Sp}(M \otimes \mathbb{Z}_2)$, where $\tilde{t}$ is any operator in $\mathrm{Sp}(M \otimes \mathbb{Z}/2^{N+m}\mathbb{Z})$ 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 [11, Corollary 2.2]). Moreover, it is easy to check that for each $m \geq 1$, the map sending each matrix in $\Gamma(2^N)$ to its 2^{m-1}th power induces a group isomorphism $\Gamma(2^N)/\Gamma(2^{N+1}) \xrightarrow{\sim} \Gamma(2^{N+m-1})/\Gamma(2^{N+m})$. It follows that if the image of G modulo 2^{N+1} contains $\Gamma(2^N)/\Gamma(2^{N+1})$, then the image of G 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 modulo 2^{N+1} contains $\Gamma(2^N)/\Gamma(2^{N+1})$.

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

$$(1 + 2^n t_i)(1 + 2^{n''} t_j)(1 + 2^n t_i)^{-1}(1 + 2^{n''} t_j)^{-1} \equiv 1 + 2^N [t_i, t_j] \pmod{2^{N+1}}$$

for $1 \leq i < j \leq 2g$. Thus, $G \supset \Gamma(2^N)$, 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 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 and the element $T_{c_3}^{2^n}$ coincides with $\Gamma(2^n)$.*

Proof. By the argument used at the beginning of the proof of Proposition 3.1, we only need to show that the images of $T_{c_1}^{2^n}, T_{c_2}^{2^n}, T_{c_3}^{2^n}$ modulo 2^{n+1} generate $\Gamma(2^n)/\Gamma(2^{n+1})$. Using the isomorphism from the additive group $\mathfrak{sp}(M \otimes \mathbb{F}_2)$ to $\Gamma(2^n)/\Gamma(2^{n+1})$ which was established in that proof, we see that it suffices to show that $\{\bar{t}_1, \bar{t}_2, \bar{t}_3\}$ is linearly independent and thus generates the rank-3 elementary abelian group $\mathfrak{sp}(M \otimes \mathbb{F}_2)$, where $\bar{t}_i$ denotes the image modulo 2 of $T_{c_i} - 1$ 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.

□

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 2.5 to get several elements in G_2 and then to use Proposition 3.1 to determine that the subgroup of G_2 generated by these elements 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 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 $y^2 = \prod_{i=1}^{d'}(x - \alpha_i)$ for some elements $\alpha_i \in \mathcal{O}_K$ for $1 \leq i \leq d'$, and define the 2-adic Galois image G_2 as above. Suppose that there are distinct primes $\mathfrak{p}_1$, ... , $\mathfrak{p}_{d'-1}$ of K not lying over (2) and such that for $1 \leq i \leq d'-1$, the only two α_j's which are equivalent modulo $\mathfrak{p}_i$ are α_i and $\alpha_{d'}$; let $m_i \geq 1$ be the maximal integer such that $\mathfrak{p}_i^{m_i} \mid (\alpha_{d'} - \alpha_i)$. Let $n = \max\{v_2(m_i)\}_{i=1}^{d'-2}$. If $n' := v_2(m_{d'-1}) \leq n$ or if $d' = 2g+2$, we have $\Gamma(2) \supseteq G_2 \supsetneq \Gamma(2^{2n+2})$. Otherwise, we have $\Gamma(2) \supseteq G_2 \supsetneq \Gamma(2^{n+n'+2})$. Moreover, if $d' = 4$, then $G_2 \supseteq \Gamma(2^{\max\{n,n'\}+1})$.*

Proof. Using the embedding $\bar{K} \hookrightarrow \mathbb{C}$ fixed at the beginning of §2, we identify $T_\ell(J)$ with $H_1(C(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_\ell$ as we did in §2. Let $\{a_1, ..., a_g, b_1, ..., b_g\}$ be a symplectic basis of $H_1(C(\mathbb{C}), \mathbb{Z})$ as in Definition 2.2(b) with $(z_1, ..., z_{2g+2}) = (\alpha_1, ..., \alpha_{2g+1}, \infty)$ if d' is odd and $(z_1, ..., z_{2g+2}) = (\alpha_1, ..., \alpha_{2g}, \alpha_{2g+2}, \alpha_{2g+1})$ if d' is even. Then Proposition 2.5 says that for $1 \leq i \leq 2g$, the image of $G_{K,\mathfrak{p}_i} \subset G_K$ in $\mathrm{GSp}(T_2(J))$ contains $T_{c_i}^{2m_i}$, where $T_{c_i} \in \mathrm{Sp}(T_2(J))$ is the transvection with respect to an element $c_i \in T_2(J)$ which is equivalent modulo 2 to the formula given in (2). Meanwhile, if d' is even, the image of $G_{K,\mathfrak{p}_{2g+1}}$ contains $T_{c_{d'}}^{2m_{2g+1}}$ for some other element $c_{d'} \in T_2(J)$ corresponding to the lift of a loop separating $\{\alpha_{2g+1}, \alpha_{2g+2}\}$ from its complement in $\{\alpha_j\}_{j=1}^{2g+2}$. In any case, we have $T_{c_1}^{2m_1}, ..., T_{c_{2g}}^{2m_{2g}} \in G_2$; note that $m_i/2^{v_2(m_i)} \in \mathbb{Z}_2^\times$ and so by taking suitable powers we get that $T_{c_1}^{2^{v_2(m_1)+1}}, ..., T_{c_{2g}}^{2^{v_2(m_{2g})+1}} \in G_2$. It then follows from Proposition 3.1 applied to $M := H_1(C(\mathbb{C}), \mathbb{Z})$ that $G_2 \supset \Gamma(2^{2n+2})$ if $n' \leq n$ or if $d' = 2g+2$ and $G_2 \supset \Gamma(2^{n+n'+2})$ otherwise.

If $d' = 4$, then in particular, we have $T_{c_1}^{2^{\max\{n,n'\}+1}}, T_{c_2}^{2^{\max\{n,n'\}+1}}, T_{c_3}^{2^{\max\{n,n'\}+1}} \in G_2$ with c_1, c_2, c_3 as described above. Clearly we have $c_1 \equiv a_1 + b_1$, $c_2 \equiv b_1$, and $c_3 \equiv a_1 \pmod 2$, and so Proposition 3.3 implies that $G_2 \supseteq \Gamma(2^{\max\{n,n'\}+1})$.

□

Remark 4.2. We note that it is generally not difficult to compute the order of $G/\Gamma(2^{2n+2})$ or $G/\Gamma(2^{n+n'+2})$, where $G \subseteq G_2$ 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 $\lambda \in \mathcal{O}_K \smallsetminus \{0, 1\}$, let E_λ be the elliptic curve over K given by $y^2 = x(x-1)(x-\lambda)$. Suppose that there exist (necessarily distinct) primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K not lying over (2) and integers

$m_1, m_2, \geq 1$ such that $\mathfrak{p}_1^{m_1}$ exactly divides (λ) and $\mathfrak{p}_2^{m_2}$ exactly divides $(\lambda - 1)$. Then Theorem 4.1 tells us that the 2-adic Galois image G_2 (strictly) contains $\Gamma(2^{v_2(m_1)+v_2(m_2)+2})$. In the case that $m_1 = m_2 = 1$ (e.g. $K = \mathbb{Q}$, $\lambda = 6$, $\mathfrak{p}_1 = (3)$, $\mathfrak{p}_2 = (5)$), we get $\Gamma(2) \supset G_2 \supsetneq \Gamma(4)$ and can therefore directly compute the precise subgroup $G_2 \cap \mathrm{Sp}(T_2(E_\lambda)) \subset \Gamma(2)$ using the well-known fact that the 4-division field $K(E_\lambda[4])$ is generated over K by $\{\sqrt{-1}, \sqrt{\lambda}, \sqrt{\lambda - 1}\}$.

It is also possible to prove the statement of Proposition 2.5, and hence the subgroup G_2 for this example for the particular cases of $C = E_\lambda$ over $\mathcal{K}_{\mathfrak{p}_1}$ and over $\mathcal{K}_{\mathfrak{p}_2}$ using formulas for generators of 2-power division fields of E_λ over K found in [14], as the author has done in [15, §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 $\alpha_1, ..., \alpha_d$ denote the roots of f, and write $L = K(\alpha_1, ..., \alpha_d)$ for the splitting field of f over K. Note that $\mathrm{Gal}(L/K)$ acts transitively on the α_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 [10, Corollary 2.11]) that G_K does not fix the 2-torsion points of J and so G_2 is not contained in $\Gamma(2)$, while the image of $\mathrm{Gal}(\bar{K}/L)$ under ρ_2 coincides with $G_2 \cap \Gamma(2)$.

The fact that $\mathfrak{p} \nmid (2\Delta)$ implies that the extension L/K is not ramified at $\mathfrak{p}$, and so $\mathfrak{p}$ splits into a product $\mathfrak{p}_1 ... \mathfrak{p}_r$ 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 $\mathfrak{p}_i \mid (\lambda - \alpha_i)$ for some i; we assume without loss of generality that $\mathfrak{p}_1 \mid (\lambda - \alpha_1)$. Then $\mathfrak{p}_1$ cannot divide $(\lambda - \alpha_i)$ for any $i \in \{2, ..., d\}$, because otherwise for such an i we would have $\mathfrak{p}_1 \mid (\alpha_i - \alpha_1) \mid (\Delta)$, which contradicts the hypothesis that $\mathfrak{p} \nmid (2\Delta)$. It follows that $\mathfrak{p}_1^m$ exactly divides $(\lambda - \alpha_1)$. Then by applying elements of $\mathrm{Gal}(L/K)$ that take α_1 to each α_i, we get other primes lying over $\mathfrak{p}$ whose mth powers exactly divide the ideals $(\lambda - \alpha_i)$; we assume without loss of generality that $\mathfrak{p}_i^m$ exactly divides $(\lambda - \alpha_i)$ for $1 \leq i \leq d$. Now since the $\mathfrak{p} \nmid (2\Delta)$ hypothesis implies that none of the $\mathfrak{p}_i$'s lie over (2), we can apply Theorem 4.1 with K replaced by L, $d' = d + 1$, $\alpha_{d'} = \lambda$, and $m_1 = ... = m_{d'-1} = m$ to get the statement 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 $\mathfrak{p}_{d'-1}$ to be a prime of L lying over $\mathfrak{p}'$, and we put $d' = d+2$, $\alpha_{d'} = \lambda$, $\alpha_{d'-1} = \lambda'$, $m = m_1 = ... = m_{d'-2}$, and $m' = m_{d'-1}$. □

5. Realizing uniform boundedness along one-parameter families

Fix an irreducible monic polynomial $f \in \mathcal{O}_K[x]$ of degree $d \geq 2$. Cadoret and Tamagawa have shown in [4, Theorems 1.1 and 5.1] that for all but finitely many $\lambda \in K$, the ℓ-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 ℓ-adic Galois image $G_{\ell,\eta}$ associated to the generic fiber of the family parametrized by λ. These theorems also assert that there is some integer $B \geq 1$ depending only on f and ℓ such that the index of $G_{\ell,\lambda}$ in $G_{\ell,\eta}$ is bounded by B for all but finitely many $\lambda \in K$. The following theorem recovers the openness result for $\ell = 2$ when $d \geq 4$ and explicitly provides the aforementioned uniform bound when d is even, under the assumption that K has class number 1. (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 [12, 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 [4, Theorem 1.1] and in our proof of the theorem below.

Theorem 5.1. *Assume that $\mathcal{O}_K$ is a PID. Let $f \in \mathcal{O}_K[x]$ be an irreducible monic polynomial of degree $d \geq 3$ with discriminant Δ. For each $\lambda \in K$, let J_λ denote the Jacobian of the hyperelliptic curve C_λ with defining equation $y^2 = f(x)(x - \lambda)$, and write $G_{2,\lambda} \subseteq \mathrm{GSp}(T_2(J_\lambda))$ for the image of the associated 2-adic Galois representation.*

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

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

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

Proof. Let $\Sigma \subset K^\times$ denote the multiplicative subgroup generated by the elements $\xi \in \mathcal{O}_K$ such that ξ is divisible only by primes which divide 2Δ. We claim that Σ is finitely generated. Indeed, there is an obvious map from Σ to the free $\mathbb{Z}$-module formally generated by the (finite) set of prime ideals of $\mathcal{O}_K$ which divide 2Δ, and its kernel is the unit group $\mathcal{O}_K^\times$, which is also well known to be finitely generated.

Choose any $\lambda \in K$, which we may write as μ/ν for some coprime $\mu, \nu \in \mathcal{O}_K$, because $\mathcal{O}_K$ is a PID. Let $h(x) = \nu^d f(\nu^{-1}x)$, which is a monic polynomial in $\mathcal{O}_K[x]$; note that the discriminant of h is equal to $\nu^{2d^2-d}\Delta$. Then there is a $K(\sqrt{\nu})$-isomorphism from C_λ to the hyperelliptic curve C'_λ whose defining equation is $y^2 = \nu^d f(\nu^{-1}x)(x-\mu) \in \mathcal{O}_K[x]$, given by $(x, y) \mapsto (\nu x, \nu^{(d+1)/2}y)$. Thus, letting J'_λ denote the Jacobian of C'_λ, the 2-adic Tate modules $T_2(J_\lambda)$ and $T_2(J'_\lambda)$ are isomorphic as $\mathrm{Gal}(\bar{K}/K(\sqrt{\nu}))$-modules. In light of this, we replace K with $K(\sqrt{\nu})$ and consider the 2-adic Galois image $G_{2,\lambda}$ associated to J'_λ. Now Theorem 1.1 says that if there is a prime element $\mathfrak{p}$ dividing $\nu^d f(\lambda)$ but not $2\nu^{d^2-d}\Delta$, then $G_{2,\lambda} \subset \mathrm{GSp}(T_2(J_\lambda)) \cong \mathrm{GSp}(T_2(J'_\lambda))$ is open. It follows from the fact that μ and ν are coprime that $\nu^d f(\lambda)$ is not divisible by any prime element dividing ν, so a prime $\mathfrak{p}$ satisfying the above condition does not divide 2Δ. The existence of such a prime is equivalent to the condition that $\nu^d f(\lambda) \notin \Sigma$, 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 λ 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 Σ/Σ^d. If $d \geq 4$, then an application of the Riemann-Hurwitz formula shows that such an equation defines a smooth curve of genus ≥ 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 ξ. But this follows from the fact that Σ/Σ^d is finite because Σ is finitely generated.

Now assume that $d = 3$ or $d \geq 5$ and that $\lambda \in \mathcal{O}_K[(2\Delta)^{-1}] \cdot (K^\times)^s$, 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 $\nu^d f(\lambda) \notin \Sigma \cdot (K^\times)^s$, which is equivalent to saying that $f(\lambda) \notin \Sigma \cdot (K^\times)^s$. Then there is a prime element $\mathfrak{p}$ dividing $\nu^d f(\lambda)$ but not $2\nu^{d^2-d}\Delta$ (so $\mathfrak{p} \nmid 2\Delta$ as before) and such that the maximum integer $m \geq 1$ with $\mathfrak{p}^m \mid \nu^d f(\lambda)$ satisfies $v_2(m) \leq v_2(s) - 1$. Then Theorem 1.1 implies that $G_{2,\lambda} \cap \mathrm{Sp}(T_2(J_\lambda)) \supsetneq \Gamma(4)$ 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, once we observe by Riemann-Hurwitz that the curves given by $\xi y^s = f(x)$ have genus ≥ 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 $\nu^d f(\lambda) \notin \Sigma \cdot (K^\times)^s$, which in both cases is equivalent to saying that $f(\lambda) \notin \Sigma \cdot (K^\times)^s$. Then there is a prime element $\mathfrak{p}$ dividing $\nu^d f(\lambda)$ but not $2\nu^{d^2-d}\Delta$ (so $\mathfrak{p} \nmid 2\Delta$ as before) and such that the maximum integer $m \geq 1$ with $\mathfrak{p}^m \mid \nu^d f(\lambda)$ satisfies $v_2(m) \leq v_2(s) - 1$. Then Theorem 1.1 implies that $G_{2,\lambda} \cap \mathrm{Sp}(T_2(J_\lambda))$ 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 ≥ 2.

□

Remark 5.2. a) If we drop the assumption that $\mathcal{O}_K$ is a PID in the statement of Theorem 5.1, then we observe from the proof above that we still get the statement of (a) when "all but finitely many $\lambda \in K$" is replaced by "all but finitely many $\lambda \in \mathcal{O}_K$" (and this statement holds for $d \in \{2, 3\}$ as well). In particular, this shows that the elements $\lambda \in \mathcal{O}_K$ which satisfy the hypothesis in Theorem 1.1 account for all but finitely many of the elements $\lambda \in \mathcal{O}_K$ such that $G_{2,\lambda}$ is open.

b) In any case, the hypothesis "$\mathcal{O}_K$ is a PID" may be weakened to "the Hilbert class field tower of K terminates". This follows from the fact that under this hypothesis, there is a finite extension of K with class number 1, and it clearly suffices to prove the assertions of Theorem 5.1 when K is replaced with a finite extension of K.

Remark 5.3. 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 $G_{2,\lambda} \supsetneq \Gamma(4)$. In these cases, it is always possible to compute the full structure of G_2 and determine its index in $\mathrm{GSp}(T_2(J_\lambda))$ 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 [16, Proposition 3.1] in the case that d is odd and are found in [15, §2.4] in the case that d is even.

References

[1] Samuele Anni and Vladimir Dokchitser. Constructing hyperelliptic curves with surjective Galois representations. *arXiv preprint arXiv:1701.05915*, 2017.

[2] Keisuke Arai. On uniform lower bound of the Galois images associated to elliptic curves. *Journal de théorie des nombres de Bordeaux*, 20(1):23–43, 2008.

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

[4] Anna Cadoret and Akio Tamagawa. A uniform open image theorem for ℓ-adic representations, I. *Duke Mathematical Journal*, 161(13):2605–2634, 2012.

[5] Benson Farb and Dan Margalit. *A Primer on Mapping Class Groups (PMS-49)*. Princeton University Press, 2011.

[6] Alexandre Grothendieck and Michel Raynaud. Modeles de néron et monodromie. In *Groupes de Monodromie en Géométrie Algébrique*, pages 313–523. Springer, 1972.

[7] Hilaf Hasson and Jeffrey Yelton. Prime-to-p étale fundamental groups of punctured projective lines over strictly henselian fields. *arXiv preprint arXiv:1707.00649*, 2017.

[8] Serge Lang. *Introduction to algebraic and abelian functions*, volume 89. Springer Science & Business Media, 2012.

[9] David Mumford. *Abelian varieties*, volume 108. Oxford Univ Press, 1974.

[10] David Mumford. Tata lectures on theta II. *Progress in Mathematics*, 43, 1984.

[11] Masatoshi Sato. The abelianization of the level d mapping class group. *Journal of Topology*, 3(4):847–882, 2010.

[12] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*. Addison-Wesley, Advanced Book Program (Redwood City, Calif.), 1989.

[13] Alice Silverberg. Fields of definition for homomorphisms of abelian varieties. *Journal of pure and applied algebra*, 77(3):253–262, 1992.

[14] Jeffrey Yelton. Dyadic torsion of elliptic curves. *European Journal of Mathematics*, 1(4):704–716, 2015.

[15] Jeffrey Yelton. *Hyperelliptic Jacobians and their associated ℓ-adic Galois representations*. PhD thesis, The Pennsylvania State University, 2015.

[16] Jeffrey Yelton. Images of 2-adic representations associated to hyperelliptic Jacobians. *Journal of Number Theory*, 151:7–17, 2015.

[17] Yuri G. Zarhin. Very simple 2-adic representations and hyperelliptic Jacobians. *Moscow Math. J*, 2(2):403–431, 2002.

[18] Yuri G. Zarhin. Families of absolutely simple hyperelliptic Jacobians. *Proceedings of the London Mathematical Society*, 100(1):24–54, 2010.

[19] Yuri G. Zarhin. Two-dimensional families of hyperelliptic Jacobians with big monodromy. *arXiv preprint arXiv:1310.6532*, 2013.