Images of 2-adic representations associated to hyperelliptic Jacobians

Jeffrey Yelton

October 13, 2014

Abstract

Let $k$ be a subfield of $\mathbb{C}$ which contains all 2-power roots of unity, and let $K = k(\alpha_1, \alpha_2, ..., \alpha_{2g+1})$, where the $\alpha_i$’s are independent and transcendental over $k$, and $g$ is a positive integer. We investigate the image of the 2-adic Galois action associated to the Jacobian $J$ of the hyperelliptic curve over $K$ given by $y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i)$. Our main result states that the image of Galois in $\text{Sp}(T_2(J))$ coincides with the principal congruence subgroup $\Gamma(2) \triangleleft \text{Sp}(T_2(J))$. As an application, we find generators for the algebraic extension $K(J[4])/K$ generated by coordinates of the 4-torsion points of $J$.

1 Introduction

Fix a positive integer $g$. An affine model for a hyperelliptic curve over $\mathbb{C}$ of genus $g$ may be given by

$$y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i),$$

with $\alpha_i$’s distinct complex numbers. Now let $\alpha_1, ..., \alpha_{2g+1}$ be transcendental and independent over $\mathbb{C}$, and let $L$ be the subfield of $\mathbb{C}(\alpha) := \mathbb{C}(\alpha_1, ..., \alpha_{2g+1})$ generated over $\mathbb{C}$ by the elementary symmetric functions of the $\alpha_i$’s. For any positive integer $N$, let $J[N]$ denote the $N$-torsion subgroup of $J(L)$. For each $n \geq 0$, let $L_n = L(J[2^n])$ denote the extension of $L$ over which the $2^n$-torsion of $J$ is defined. Set

$$L_\infty := \bigcup_{n=1}^{\infty} L_n.$$

Note that $\mathbb{C}(\alpha_1, ..., \alpha_{2g+1})$ is Galois over $L$ with Galois group isomorphic to $S_{2g+1}$. It is well known ([5], Corollary 2.11) that $\mathbb{C}(\alpha_1, ..., \alpha_{2g+1}) = L_1$, so $\text{Gal}(L_1/L) \cong S_{2g+1}$. Fix an algebraic closure $\bar{L}$ of $L$, and write $G_L$ for the absolute Galois group $\text{Gal}(\bar{L}/L)$.

Let $C$ be the curve defined over $L$ by equation (1), and let $J/L$ be its Jacobian. For any prime $\ell$, let

$$T_\ell(J) := \lim_{\ell \rightarrow n} J[\ell^n]$$

1
denote the $ℓ$-adic Tate module of $J$; it is a free $\mathbb{Z}_ℓ$-module of rank $2g$ (see [6, §18]). For the rest of this paper, we write $ρ_ℓ : G_L \rightarrow \text{Aut}(T_ℓ(J))$ for the continuous homomorphism induced by the natural Galois action on $T_ℓ(J)$. Write $\text{SL}(T_ℓ(J))$ (resp. $\text{Sp}(T_ℓ(J))$) for the subgroup of automorphisms of the $2$-adic Tate module $T_ℓ(J)$ with determinant $1$ (resp. automorphisms of $T_ℓ(J)$ which preserve the Weil pairing). Since $L$ contains all $2$-power roots of unity, the Weil pairing on $T_2(J)$ is Galois invariant, and it follows that the image of $ρ_2$ is contained in $\text{Sp}(T_2(J))$. For each $n ≥ 0$, we denote by

$$\Gamma(2^n) := \{g ∈ \text{Sp}(T_2(J)) | g \equiv 1 \pmod{2^n}\} \triangleleft \text{Sp}(T_2(J))$$

the level-$2^n$ principal congruence subgroup of $\text{Sp}(T_2(J))$.

Our main theorem is the following.

**Theorem 1.1.** With the above notation, the image under $ρ_2$ of the Galois subgroup fixing $L_1$ is $\Gamma(2) \triangleleft \text{Sp}(T_2(J))$.

Before setting out to prove this theorem, we state some easy corollaries.

**Corollary 1.2.** Let $G$ denote the image under $ρ_2$ of all of $G_L$. Then we have the following:

a) $G$ contains $\Gamma(2) \triangleleft \text{Sp}(T_2(J))$, and $G/\Gamma(2) \cong S_{2g+1}$.

b) In the case that $g = 1$, $G = \text{Sp}(T_2(J)) = \text{SL}(T_2(J))$.

c) For each $n ≥ 1$, the homomorphism $ρ_2$ induces an isomorphism

$$\bar{ρ}_2^{(n)} : \text{Gal}(L_n/L_1) \rightarrow \Gamma(2)/\Gamma(2^n)$$

via the restriction map $\text{Gal}(\bar{L}/L_1) \rightarrow \text{Gal}(L_n/L_1)$.

**Proof.** Since $\text{Gal}(L_1/L) \cong S_{2g+1}$, part (a) immediately follows from the theorem. If $g = 1$, then fix a basis of $T_2(J)$ so that we may identify $\text{Sp}(T_2(J))$ (resp. $\text{SL}(T_2(J))$) with $\text{Sp}_2(\mathbb{Z}_2)$ (resp. $\text{SL}_2(\mathbb{Z}_2)$). Then it is well known that $\text{Sp}_2(\mathbb{Z}_2) = \text{SL}_2(\mathbb{Z}_2)$, and that $\text{SL}_2(\mathbb{Z}_2)/\Gamma(2) \cong \text{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Since, by part (a), $G/\Gamma(2) \cong S_3$ when $g = 1$, the linear subgroup $G$ must be all of $\text{Sp}(T_2(J)) = \text{SL}(T_2(J))$, which is the statement of (b). To prove part (c), note that for any $n ≥ 0$, the image under $ρ_2$ of the Galois subgroup fixing the $2^n$-torsion points is clearly $G \cap \Gamma(2^n)$. But $G > \Gamma(2)$, so for any $n ≥ 1$, the image under $ρ_2$ of $\text{Gal}(\bar{L}/L(2^n))$ is $\Gamma(2^n)$. Then part (c) immediately follows by the definition of $\bar{ρ}_2^{(n)}$.

In §2, we will prove the main theorem by considering a family of hyperelliptic curves whose generic fiber is $C$. In §3, we will use the results of the previous two sections to determine generators for the algebraic extension $L_2/L$ (Theorem 3.1). Finally, in §4, we will generalize Theorems 1.1 and 3.1 by descending from $C$ to a subfield $k ⊂ C$ which contains all $2$-power roots of unity.
2 Families of hyperelliptic Jacobians

In order to prove Theorem 1.1, we study a family of hyperelliptic curves parametrized by all (unordered) \((2g + 1)\)-element subsets \(T = \{\alpha_i\} \subset \mathbb{C}\) whose generic fiber is \(C\). Let \(e_1 := \sum_{i=1}^{2g+1} \alpha_i, ..., e_{2g+1} := \prod_{i=1}^{2g+1} \alpha_i\) be the elementary symmetric functions of the variables \(\alpha_i\), and let \(\Delta\) be the discriminant function of these variables. Then the base of this family is the affine variety over \(\mathbb{C}\) given by

\[X := \text{Spec}(\mathbb{C}[e_1, e_2, ..., e_{2g+1}, \Delta^{-1}]).\]  

This complex affine scheme may be viewed as the configuration space of \((2g+1)\)-element subsets of \(\mathbb{C}\) (see the discussion in Section 6 of [1]). More precisely, we identify each \(\mathbb{C}\)-point \(T = (e_1, e_2, ..., e_{2g+1})\) of \(X\) with the set of roots of the squarefree degree-\((2g+1)\) polynomial \(z^{2g+1} - e_1z^{2g} + e_2z^{2g-1} - ... - e_{2g+1} \in \mathbb{C}[z]\), which is a \((2g + 1)\)-element subset of \(\mathbb{C}\). Note that the function field of \(X\) is \(L\). The (topological) fundamental group of \(X\) is isomorphic to \(B_{2g+1}\), the braid group on \(2g + 1\) strands. The braid group \(B_{2g+1}\) is generated by elements \(\sigma_1, \sigma_2, ..., \sigma_{2g}\), with relations \(\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}\) for \(1 \leq i \leq 2g\) and \(\sigma_i \sigma_j = \sigma_j \sigma_i\) for \(2 \leq i + 1 < j \leq 2g\). (See section 1.4 of [2] for more details.)

We also define the complex affine scheme

\[Y := \text{Spec}(\mathbb{C}[\alpha_1, \alpha_2, ..., \alpha_{2g+1}, \{(\alpha_i - \alpha_j)^{-1}\}_{1 \leq i < j \leq 2g+1}]).\]  

As a complex manifold, \(Y\) is the ordered configuration space, whose \(\mathbb{C}\)-points may be identified with \(2g + 1\)-element subsets of \(\mathbb{C}\) which are given an ordering (a \(\mathbb{C}\)-point is identified with its coordinates \((\alpha_1, \alpha_2, ..., \alpha_{2g+1})\)). There is an obvious covering map \(Y \rightarrow X\) which sends each point \((\alpha_1, \alpha_2, ..., \alpha_{2g+1})\) of \(Y\) to the point in \(X\) corresponding to the (unordered) subset \(\{\alpha_1, \alpha_2, ..., \alpha_{2g+1}\}\). The \textit{pure} braid group on \(2g + 1\) strands, denoted \(P_{2g+1}\), is defined to be the kernel of the surjective homomorphism from \(B_{2g+1}\) to the symmetric group \(S_{2g+1}\) which sends \(\sigma_i\) to \((i, i+1) \in S_{2g+1}\) for \(1 \leq i \leq 2g\) (see the proof of Theorem 1.8 in [1]). Then \(P_{2g+1} \triangleleft B_{2g+1}\) is the (normal) subgroup corresponding to the cover \(Y \rightarrow X\), and is therefore isomorphic to the fundamental group of \(Y\).

Let \(\mathcal{O}_X\) denote the coordinate ring of \(X\), and let \(F(x) \in \mathcal{O}_X[x]\) be the degree-\((2g + 1)\) polynomial given by

\[x^{2g+1} + \sum_{i=1}^{2g+1} (-1)^i e_i x^{2g+1-i}.\]  

Now denote by \(\mathcal{C} \rightarrow X\) the affine scheme defined by the equation \(y^2 = F(x)\). Clearly, \(\mathcal{C}\) is the family over \(X\) whose fiber over a point \(T \in X(\mathbb{C})\) is the smooth affine hyperelliptic curve defined by \(y^2 = \prod_{z \in T} (x - z)\), and the generic fiber of \(\mathcal{C}\) is \(C/L\). Fix a basepoint \(T_0\) of \(X\), and a basepoint \(P_0\) of \(C_{T_0}\). Then we have a short exact sequence of fundamental groups

\[1 \rightarrow \pi_1(C_{T_0}, P_0) \rightarrow \pi_1(C, P_0) \rightarrow \pi_1(X, T_0) \rightarrow 1.\]  


We now construct a continuous section \( s : X \to C \), following the proof of Lemma 6.1 and the discussion in [10], §6. For \( i = 1, 2 \), let \( \mathcal{E}_i \to X \) be the affine scheme given by \( \text{Spec}(O_X/x,y)/(y' - F(x))/[F(x)^{-1}] \). Then \( \mathcal{E}_1 \to X \) is clearly the family of complex topological spaces whose fiber over a point \( T \in X \) can be identified with \( \mathbb{C} \setminus T \), and there is an obvious degree-2 cover \( \mathcal{E}_2 \to \mathcal{E}_1 \). Let \( t : X \to \mathcal{E}_1 \) be the continuous map of complex topological spaces which sends a point \( T \in X \) to \( \max_{z \in T} \{ |z| \} + 1 \in \mathbb{C} \setminus T = \mathcal{E}_1.T \). This section then lifts to a section \( \tilde{t} : X \to \mathcal{E}_2 \). Define \( s : X \to C \) to be the composition of \( \tilde{t} \) with the obvious inclusion map \( \mathcal{E}_2 \hookrightarrow C \). It is easy to check from the construction of \( s \) that it is a section of the family \( C \to X \).

The section \( s \) induces a monodromy action of \( \pi_1(X, T_0) \) on \( \pi_1(C_{T_0}, P_0) \), which is given by \( \sigma \in \pi_1(X) \) acting as conjugation by \( s(\sigma) \) on \( \pi_1(C_{T_0}, P_0) \). This induces an action of \( B_{2g+1} \) on the abelianization of \( \pi_1(C_{T_0}, P_0) \), the homology group \( H_1(C_{T_0}, \mathbb{Z}) \), which is isomorphic to \( \mathbb{Z}^{2g} \). We denote this action by

\[
R : B_{2g+1} \cong \pi_1(X, T_0) \to \text{Aut}(H_1(C_{T_0}, \mathbb{Z})). \tag{6}
\]

This action respects the intersection pairing on \( C_{T_0} \), so the image of \( R \) is actually contained in the corresponding subgroup of symplectic automorphisms \( \text{Sp}(H_1(C_{T_0}, \mathbb{Z})) \).

The following theorem is proven in [1] (Théorème 1), as well as in [5] (Lemma 8.12).

**Theorem 2.1.** In the representation \( R : B_{2g+1} \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z})) \), the image of \( P_{2g+1} \) coincides with \( \Gamma(2) \).

Let \( \hat{B}_{2g+1} \) denote the profinite completion of \( B_{2g+1} \cong \pi_1(X, T_0) \). Since \( X \) may be viewed as a scheme over the complex numbers, Riemann’s Existence Theorem yields an isomorphism between its étale fundamental group \( \pi_1^{\text{ét}}(X, T_0) \) and \( \hat{B}_{2g+1} \) ([3], Exposé XII, Corollaire 5.2). Meanwhile, \( \pi_1^{\text{ét}}(X, T_0) \) is isomorphic to the Galois group \( \text{Gal}(L^{\text{unr}}/L) \), where \( L^{\text{unr}} \) is the maximal extension of \( L \) unramified at all points of \( X \). The representation \( R : B_{2g+1} \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z})) \) induces a homomorphism of profinite groups

\[
R : \text{Gal}(L^{\text{unr}}/L) = \hat{B}_{2g+1} \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell) \tag{7}
\]

for any prime \( \ell \). Composing this map with the restriction homomorphism \( G_L := \text{Gal}(L/L) \to \text{Gal}(L^{\text{unr}}/L) \) yields a map which we denote \( R_\ell : G_L \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell) \). The following proposition will allow us to convert the above topological result into the arithmetic statement of Theorem 1.1.

**Proposition 2.2.** Assume the above notation, and let \( \ell \) be any prime. Then there is an isomorphism of \( \mathbb{Z}_\ell \)-modules \( T_\ell(J) \cong H_1(C_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell \) making the representations \( \rho_\ell \) and \( R_\ell \) isomorphic.

**Proof.** We proceed in five steps.

**Step 1:** We switch from the affine curve \( C \) to a smooth compactification of \( C \), which is defined as follows. Let \( C' \) be the (smooth) curve defined over \( L \) by
the equation
\[ y'^2 = x' \prod_{i=1}^{2g+1} (1 - \alpha_i x'). \] (8)

We glue the open subset of \( C \) defined by \( x \neq 0 \) to the open subset of \( C' \) defined by \( x' \neq 0 \) via the mapping
\[ x' \mapsto \frac{1}{x}, \quad y' \mapsto \frac{y}{x^{g+1}}, \]
and denote the resulting smooth, projective scheme by \( \bar{C} \). (See \[ 3 \], §1 for more details of this construction.) Let \( \infty \in \bar{C}(L) \) denote the “point at infinity” given by \( (x', y') = (0, 0) \in C' \). The curve \( \bar{C} \) has smooth reduction over every point \( T \in X \) and therefore can be extended in an obvious way to a family \( \bar{C} \to X \) whose generic fiber is \( C/L \) and \( \bar{C}/C \). Note that \( \bar{C}_T \) is a smooth compactification of \( C_T \) for each \( T \in X \). There is a surjective map \( \pi_1(\bar{C}_T, P_0) \to \pi_1(\bar{C}_{\infty}, \infty) \) induced by the inclusion \( \bar{C} \to \bar{C} \). Note also that the section \( s : X \to \bar{C} \subset \bar{C} \) can be continuously deformed to the “constant section” \( \bar{s} : X \to \bar{C} \) sending each \( T \in X \) to the point at infinity \( \infty_T \in \bar{C}_{\infty} \). Therefore, \( \bar{s}_* : \pi_1(X, T_0) \to \pi_1(\bar{C}_{\infty}, \infty) \) is the composition of \( s_* \) with the map \( \pi_1(\bar{C}_T) \to \pi_1(\bar{C}_{\infty}) \). In this way, we may view the action of \( \pi_1(X, T_0) \) on \( \pi_1(\bar{C}_{T_0}, P_0)^{ab} = \pi_1(\bar{C}_{\infty}, \infty)^{ab} \) as being induced by \( \bar{s}_* \).

**Step 2:** We switch from (topological) fundamental groups to \( \acute{e}tale \) fundamental groups. Since \( X \) and \( C \), as well as \( \bar{C}_T \) for each \( T \in X \), can be viewed as a scheme over the complex numbers, Riemann’s Existence Theorem implies that the \( \acute{e}tale \) fundamental groups of \( X, C \), and each \( \bar{C}_T \) (defined using a choice of geometric base point \( T_0 \) over \( T_0 \)) are isomorphic to the profinite completions of their respective topological fundamental groups. Taking profinite completions induces a sequence of \( \acute{e}tale \) fundamental groups
\[ 1 \to \pi^\acute{e}t_1(C_{T_0}, 0_{T_0}) \to \pi^\acute{e}t_1(C, 0_{T_0}) \to \pi^\acute{e}t_1(X, T_0) \to 1, \] (9)
which is a short exact sequence by \[ 3 \], Corollaire X.2.2. Moreover, the section \( \bar{s} : X \to \bar{C} \) similarly gives rise to an action of \( \pi^\acute{e}t_1(X, T_0) \) on \( \pi^\acute{e}t_1(\bar{C}_{T_0}, \infty) \).

**Step 3:** We switch from \( \bar{C} \) to its Jacobian. Define \( \mathcal{J} \to X \) to be the abelian scheme representing the Picard functor of the scheme \( \bar{C} \to X \) (see \[ 4 \], Theorem 8.1). Note that \( \mathcal{J}_T \) is the Jacobian of \( C_T \) for each \( \bar{C} \)-point \( T \) of \( X \), and the generic fiber of \( \mathcal{J} \) is \( \bar{J}/L \), the Jacobian of \( C/L \). Let \( f_\infty : \bar{C} \to \bar{J} \) be the morphism (defined over \( L \)) given by sending each point \( P \in \bar{C}(L) \) to the divisor class \([P] - (\infty)] \) in \( \text{Pic}^0(L)(\bar{C}) \), which is identified with \( J(L) \). By \[ 4 \], Proposition 9.1, the induced homomorphism of \( \acute{e}tale \) fundamental groups \( (f_\infty)_* : \pi^\acute{e}t_1(\bar{C}, \infty) \to \pi^\acute{e}t_1(\bar{J}, 0) \) factors through an isomorphism \( \pi^\acute{e}t_1(\bar{C}, \infty)^{ab} \cong \pi^\acute{e}t_1(\bar{J}, 0) \). This induces an isomorphism \( \pi^\acute{e}t_1(\bar{C}, \infty)^{ab} \cong \pi^\acute{e}t_1(\bar{J}, 0) \) for each \( T \in X \). Note that the composition of the section \( \bar{s} : X \to \bar{C} \) with \( f_\infty \) is the “zero section” \( o : X \to \mathcal{J} \) mapping each \( T \) to the identity element \( 0_T \in \mathcal{J}_T \). Thus, the action of \( \pi^\acute{e}t_1(X, T_0) \) on \( \pi^\acute{e}t_1(\bar{C}_{T_0}, \infty)^{ab} \) coming from the splitting of \[ 3 \] is the same as the action of \( \pi^\acute{e}t_1(X, T_0) \) on \( \pi^\acute{e}t_1(\mathcal{J}_{T_0}, 0_{T_0}) \) coming from the splitting of \[ 9 \] induced by the section \( o_* : \pi^\acute{e}t_1(X, T_0) \to \pi^\acute{e}t_1(\mathcal{J}, 0_{T_0}). \)
**Step 4:** We now show that this action on $\pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0})$ is isomorphic to a Galois action on $\pi_1^{et}(J_L,0)$ (and therefore on its $\ell$-adic quotient $T_\ell(J)$). Let $\eta : \text{Spec}(L) \to X$ denote the generic point of $X$. Note that we may identify $\pi_1^{et}(L,\bar{L})$ with $G_L$, and that $\eta_*: G_L \to \pi_1^{et}(X,\bar{\eta})$ is a surjection (in fact, it is the restriction homomorphism of Galois groups corresponding to the maximal algebraic extension of $L$ unramified at all points of $X$). Also, the point $0 \in J_L$ may be viewed as a morphism $0 : \text{Spec}(L) \to J_L$ which induces $0_* : G_L = \pi_1^{et}(L,\bar{L}) \to \pi_1^{et}(J_L,0)$. Let $T_0$ and $\bar{\eta}$ be geometric points over $T_0$ and $\eta$ respectively. Then we have ([3], Corollaire X.1.4) an exact sequence of étale fundamental groups
\[ \pi_1^{et}(J,0_{\bar{\eta}}) \to \pi_1^{et}(J,0_{\bar{\eta}}) \to \pi_1^{et}(X,\bar{\eta}) \to 1. \]

Changing the geometric basepoint of $X$ from $T_0$ to $\bar{\eta}$ (resp. changing the geometric basepoint of $J$ from $0_{\bar{\eta}}$ to $0_{\bar{T}_0}$) non-canonically induces an isomorphism $\pi_1^{et}(X,\bar{\eta}) \sim \pi_1^{et}(X,T_0)$ (resp. an isomorphism $\pi_1^{et}(J,0_{\bar{\eta}}) \sim \pi_1^{et}(J,0_{\bar{T}_0})$). Fix such an isomorphism $\varphi : \pi_1^{et}(X,\bar{\eta}) \sim \pi_1^{et}(X,T_0)$. Then we have the following commutative diagram, where all horizontal rows are exact:

$$
\begin{array}{cccccc}
1 & \to & \pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0}) & \to & \pi_1^{et}(J,0_{\bar{T}_0}) & \to & \pi_1^{et}(X,T_0) & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0}) & \to & \pi_1^{et}(J,0_{\bar{T}_0}) & \to & \pi_1^{et}(X,\bar{\eta}) & \to & \pi_1^{et}(X,T_0) & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \to & \pi_1^{et}(J,L,0) & \to & \pi_1^{et}(J,L,0) & \to & \pi_1^{et}(L,\bar{L}) & \to & 1
\end{array}
$$

Here the vertical arrow from $\pi_1^{et}(J,0_{\bar{\eta}})$ to $\pi_1^{et}(J,0_{\bar{T}_0})$ is a change-of-basepoint isomorphism chosen to make the lower right square commute, and $\text{sp} : \pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0}) \to \pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0})$ is the surjective homomorphism induced by a diagram chase on the bottom two horizontal rows. Grothendieck’s Specialization Theorem ([3], Corollaire X.3.9) states that $\text{sp}$ is an isomorphism, which implies that the second row is also a short exact sequence. Thus, the action of $\pi_1^{et}(X,T_0)$ on $\pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0})$ arising from the splitting of the lower row by $\alpha_*$ is isomorphic to the action of $\pi_1^{et}(X,\bar{\eta})$ on $\pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0})$ arising from the splitting of the middle row by $\alpha_*$, via the isomorphism $\text{sp} : \pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0}) \to \pi_1^{et}(J_{\bar{T}_0},0_{\bar{T}_0})$. In turn, a simple diagram chase confirms that this action, after pre-composing with $\eta_* : \pi_1^{et}(L,\bar{L}) \to \pi_1^{et}(X,\bar{\eta})$, can be identified with the action of $\pi_1^{et}(L,\bar{L})$ on $\pi_1^{et}(J_L,0)$ arising from the splitting of the top row by $0_*$. We denote this action by $\bar{R} : G_L = \pi_1^{et}(L,\bar{L}) \to \text{Aut}(\pi_1^{et}(J_L,0))$. Since the Tate module $T_\ell(J)$ may be identified with the maximal pro-$\ell$ quotient of $\pi_1^{et}(J_L,0)$, $\bar{R}$ induces an action of $G_L$ on $T_\ell(J)$, which we denote by $R_\ell : G_L \to \text{Aut}(T_\ell(J))$. One can identify the symplectic pairing on $\pi_1(J_{\bar{T}_0},0_{\bar{T}_0})$ with the Weil pairing on $T_\ell(J)$ via the results in [6], Chapter IV, §24. Therefore, the image of $R_\ell$ is a subgroup of $\text{Sp}(T_\ell(J))$. 6
By the above construction, we may identify the maximal pro-$\ell$ quotient of $\pi_1^{et}(\bar{J}_{T_0}, 0_{\bar{T}_0})$ with $H_1(C_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell$. Note that the isomorphism $sp : \pi_1^{et}(\bar{J}_{T_0}, 0_{\bar{T}_0}) \to \pi_1^{et}(J_{T_0}, 0_{T_0})$ induces an isomorphism of their maximal pro-$\ell$ quotients $sp_\ell : T_1(J) \cong H_1(C_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell$. By construction, the representation $\tilde{R}_\ell$ is isomorphic to the representation $R_\ell$ via $sp_\ell$.

Step 5: It now suffices to show that $\tilde{R}_\ell = \rho_\ell$. To determine $\tilde{R}_\ell$, we are interested in the action of $G_L$ on the group $\text{Aut}_{\ell}(\mathbb{Z})$ for each $\ell$-power-degree covering $Z \to J_L$. But each such covering is a subcovering of $[\ell^n] : J_L \to J_L$, so it suffices to determine the action of $G_L$ on the group of translations $\{t_P | P \in J[\ell^n]\}$ for each $n$. Recall that $\sigma_n : G_L \to \pi_1^{et}(J_L, 0)$ is induced by the inclusion of the $\ell$-point $0 \in J_L$. Thus, for any $\sigma \in G_L$, $0_\sigma(\sigma)$ acts on any connected etale cover of $J_L$ via $\sigma$ acting on the coordinates of the points. Since $\tilde{R}(\sigma)$ is conjugation by $0_\sigma(\sigma)$ on $\pi_1^{et}(J_L, 0) \lhd \pi_1^{et}(J_L, 0)$, one sees that for each $n$, $0_\sigma(\sigma)$ acts on $\{t_P | P \in J[\ell^n]\}$ by sending each $t_P$ to $\sigma^{-1} t_P \sigma = t_{P^\sigma}$. Thus, $G_L$ acts on the Galois group of the covering $[\ell^n] : J_L \to J_L$ via the usual Galois action on $J[\ell^n]$. This lifts to the usual action of $G_L$ on $T_\ell(J)$, and we are done.

It is now easy to prove the main theorem.

Proof (of Theorem 1.1). Recall that $\tilde{P}_{2g+1}$ is the normal subgroup of $B_{2g+1} \cong \pi_1(X, T_0)$ corresponding to the cover $Y \to X$, and the function field of $Y$ is $\mathbb{C}(\alpha_1, ..., \alpha_{2g+1}) = L_1$. It follows that the image of $\text{Gal}(\bar{L}/L_1)$ under $\eta_*$ is $\tilde{P}_{2g+1} \lhd \tilde{B}_{2g+1} \cong \pi_1^{et}(X, \bar{T}_0)$ (where $\tilde{P}_{2g+1}$ denotes the profinite completion of $P_{2g+1}$). Therefore, the statement of Theorem 2.1 with $\ell = 2$ implies that the image of $\text{Gal}(\bar{L}/L_1)$ under $R_2$ is $\Gamma(2) \lhd \text{Sp}(H_1(C_{T_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell)$. It then follows from the statement of Lemma 2.2 that the image of $\text{Gal}(\bar{L}/L_1)$ under $\rho_2$ is $\Gamma(2) \lhd \text{Sp}(T_2(J))$.

3 Fields of 4-torsion

One application of Theorem 1.1 is that it allows us to obtain an explicit description of $L_2$. We will follow Yu’s argument in [10].

Proposition 3.1. We have

$$L_2 = L_1(\frac{1}{\sqrt{\alpha_i - \alpha_j}})_{1 \leq i < j \leq 2g+1}.$$  

Proof. For $n \geq 1$, let $B_n$ denote the set of bases of the free $\mathbb{Z}/2^n\mathbb{Z}$-module $J_{T_0}[2^n]$. Then it was shown in the proof of Theorem 1.1 that $G_L$ acts on $B_n$ through the map $R : \pi_1(X, T_0) \to \text{Sp}(H_1(C_{T_0}, \mathbb{Z})) = \text{Sp}(H_1(J_{T_0}, \mathbb{Z}))$ in the statement of Theorem 2.1 and the subgroup fixing all elements of $B_n$ corresponds to $R^{-1}(\Gamma(2^n)) \lhd \pi_1(X, T_0)$. Hence, by covering space theory, there is a connected cover $X_n \to X$ corresponding to an orbit of $B_n$ under the action of $\pi_1(X, T_0)$, and the function field of $X_n$ is the extension of $L$ fixed by the subgroup of $G_L$ which fixes all bases of $J[2^n]$. Clearly, this extension is $L_n$.  

7
Thus, the Galois cover $X_n \to X$ is an unramified morphism of connected affine schemes corresponding to the inclusion $L \to L_n$ of function fields.

Note that, setting $n = 1$, we get that $X_1$ is the Galois cover of $X$ whose étale fundamental group can be identified with $R^{-1}(\Gamma(2)) \triangleleft \pi_1(X, T_0)$. Theorem 2.4 implies that $R^{-1}(\Gamma(2))$ is isomorphic to $\hat{P}_{2g+1}$, the profinite completion of $P_{2g+1}$. For $n \geq 1$, the étale morphism $X_n \to X_1$ corresponds to the function field extension $L_n \supset L_1$, which by Corollary 4.2(c) has Galois group isomorphic to $\Gamma(2)/\Gamma(2^n)$. Therefore, $X_n$ is the cover of $X_1$ whose étale fundamental group can be identified with a normal subgroup of $P_{2g+1}$ with quotient isomorphic to $\Gamma(2)/\Gamma(2^n)$.

In the proof of Corollary 2.2 of [8], it is shown that $\Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$, and thus,

$$\text{Gal}(L_2/L_1) \cong \Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}. \quad (11)$$

It is also clear from looking at a presentation of the pure braid group $P_{2g+1}$ (see for instance [2], Lemma 1.8.2) that the abelianization of $P_{2g+1}$ is a free abelian group of rank $2g^2 + g$. Therefore, its maximal abelian quotient of exponent 2 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$. Thus, $\hat{P}_{2g+1}$ has a unique normal subgroup inducing a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g^2+g}$. It follows that there is only one Galois cover of $X_1$ with Galois group isomorphic to $\Gamma(2)/\Gamma(4)$, namely $X_2$. The field extension $L_1(\{\alpha_i - \alpha_j\}_{i<j}) \supset L_1$ is unramified away from the hyperplanes defined by $(\alpha_i - \alpha_j)$ with $i \neq j$ and is obtained from $L_1$ by adjoining $2g^2 + g$ independent square roots of elements in $L_1^\times \setminus (L_1^\times)^2$. Therefore, $L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{i<j})$ is the function field of a Galois cover of $X(2)$ with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g^2+g} \cong \Gamma(2)/\Gamma(4)$. It follows that this cover of $X_1$ is $X_2$, and that $L_1(\{\sqrt{\alpha_i - \alpha_j}\}_{i<j})$ is $L_2$, the function field of $X_2$.

\[ \square \]

4 Generalizations

As in Section 1, let $k$ be an algebraic extension of $\mathbb{Q}$ which contains all 2-power roots of unity, and let $K$ be the transcendental extension obtained by adjoining the coefficients of $L$ to $k$. We will also fix the following notation. Let $C_K$ be the hyperelliptic curve defined over $K$ given by the equation $L$, and let $J_K$ be its Jacobian. For each $n \geq 0$, let $K_n$ be the extension of $K$ over which the $2^n$-torsion of $J_K$ is defined. Note that, analogous to the situation with $C/L$, the extension $K_2$ is $k(\alpha_1, ..., \alpha_{2g+1})$, which is Galois over $K$ with Galois group isomorphic to $S_{2g+1}$. Let $\rho_{2,K} : \text{Gal}(K_\infty/K) \to \text{Sp}(T_2(J_K))$ be the homomorphism arising from the Galois action on the Tate module of $J_K$. We now investigate what happens to the Galois action when we descend from working over $\mathbb{C}$ to working over $k$. (In what follows, we canonically identify $T_2(J)$ with $T_2(J_K)$ and $\Gamma(2^n)$ with the level-$2^n$ congruence subgroup of $\text{Sp}(T_2(J_K))$ for each $n \geq 0$.)

Proposition 4.1. The statements of Theorem 1.1, Corollary 1.2, and Proposition 2.1 are true when $L$ and $\rho_2$ are replaced by $K$ and $\rho_{2,K}$ respectively.
Proof. For any $n \geq 0$, let $\theta_n : \text{Gal}(L_∞/L_n) \to \text{Gal}(K_∞/K_n)$ be the composition of the obvious inclusion $\text{Gal}(L_∞/L_n) \hookrightarrow \text{Gal}(L_∞/K_n)$ with the obvious restriction map $\text{Gal}(L_∞/K_n) \to \text{Gal}(K_∞/K_n)$. Let $\bar{\rho}_2(∞)$ (resp. $\bar{\rho}_{2,K}(∞)$) be the representation of $\text{Gal}(L_∞/L)$ (resp. $\text{Gal}(K_∞/K)$) induced from $\rho_2$ (resp. $\rho_{2,K}$) by the restriction homomorphism of the Galois groups. It is easy to check that $\bar{\rho}_2(∞) = \bar{\rho}_{2,K}(∞) \circ \theta_0$. It will suffice to show that $\theta_0$ is an isomorphism.

First, note that for any $n \geq 0$, $\theta_n$ is injective by the linear disjointness of $K_∞$ and $L_n$ over $K_n$. Now suppose that $n \geq 1$. Then, as in the proof of Corollary 1.2, the image under $\bar{\rho}$ of $\text{Gal}(L_∞/L_n)$ is the entire congruence subgroup $\Gamma(2^n)$. Therefore, since $\theta_n$ is injective, the image under $\bar{\rho}_K$ of $\text{Gal}(K_∞/K_n)$ contains $\Gamma(2^n)$. But since $K$ contains all 2-power roots of unity, the Weil pairing is Galois invariant, and so the image of $\text{Gal}(K_∞/K_n)$ must also be contained in $\Gamma(2^n)$. Therefore, $\theta_n$ is an isomorphism for $n \geq 1$. Now, using Corollary 1.2(a) and the fact that $\text{Gal}(K(\alpha_1, \ldots, \alpha_{2g+1})/K) \cong S_{2g+1}$, we get the commutative diagram below, whose top and bottom rows are short exact sequences.

$$
\begin{array}{cccc}
1 & \longrightarrow & \text{Gal}(L_∞/L_1) & \longrightarrow & \text{Gal}(L_∞/L) & \longrightarrow & S_{2g+1} & \longrightarrow & 1 \\
\downarrow \theta_1 & & \downarrow \theta_0 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \text{Gal}(K_∞/K_1) & \longrightarrow & \text{Gal}(K_∞/K) & \longrightarrow & S_{2g+1} & \longrightarrow & 1
\end{array}
$$

By the Short Five Lemma, since $\theta_1$ is an isomorphism, so is $\theta_0$.

\[\square\]

**Remark 4.2.** a) Suppose we drop the assumption that $k$ contains all 2-power roots of unity. Then $\rho_{2,K}(G_K)$ is no longer contained in $\text{Sp}(T_2(J))$ in general. However, the Galois equivariance of the Weil pairing forces the image of $\rho_{2,K}$ to be contained in the group of symplectic similitudes

$$
\text{GSp}(T_2(J)) := \{ \sigma \in \text{Aut}(T_2(J)) \mid E_2(P^\sigma, Q^\sigma) = \chi_2(\sigma)E_2(P, Q) \ \forall P, Q \in T_2(J) \},
$$

where $E_2 : T_2(J) \times T_2(J) \to \lim_{n \to \infty} \mu_{2^n} \cong \mathbb{Z}_2$ is the Weil pairing on the 2-adic Tate module of $J$, and $\chi_2 : G_K \to \mathbb{Z}_2^\times$ is the cyclotomic character on the absolute Galois group of $K$. Galois equivariance of the Weil pairing also implies that $K_∞$ contains all 2-power roots of unity. Thus, $K_∞ \supset K(\mu_{2^n})$, and the statements referred to in Proposition 4.1 still hold when we replace $K$ with $K(\mu_{2^n})$.

Furthermore, if $K$ contains $\sqrt{-1}$, the Weil pairing on $J[4]$ is Galois invariant, so the image of $\text{Gal}(K_2/K_1)$ coincides with $\Gamma(2)/\Gamma(4) \subset \text{Sp}(J[4])$ and is therefore isomorphic to $\text{Gal}(L_2/L_1)$. It follows that Proposition 4.1 still holds over $K(\sqrt{-1})$; that is,

$$
K_2 = K_1(\sqrt{-1}, \{ \sqrt{\alpha_i - \alpha_j} \}_{1 \leq i < j \leq 2g+1}). \quad (12)
$$

b) In addition, suppose that $k$ is finitely generated over $\mathbb{Q}$ (for example, a number field). We may specialize by assigning an element of $k$ to each coefficient of the degree-$(2g+1)$ polynomial in $T$, and defining the corresponding Jacobian
$J_k/k$ and Galois representation $\rho_{2,k} : G_k \to \text{Sp}(T_2(J_k))$. Then we may use Proposition 1.3 of [7] and its proof (see also [9]) to see that for infinitely many choices of $e_1, \ldots, e_{2g+1} \in k$, $\rho_{2,k}(G_k)$ can be identified with $\rho_{2,K}(G_K)$ from part (a). We have $\rho_{2,k}(\text{Gal}(\bar{k}/k(\mu_{2^\infty}))) = \rho_{2,k}(G_k) \cap \text{Sp}(T_2(J_k))$, and therefore, the statements referred to in Proposition 4.1 still hold over $k(\mu_{2^\infty})$. Similarly, Proposition 5.1 still holds over $k(\sqrt{-1})$.

Acknowledgements

I am grateful to Yuri Zarhin for his many ideas and suggestions. I would also like to thank the referee, who suggested that this material be presented in a separate paper, and whose corrections were helpful in improving the exposition.

References

[1] Norbert A’Campo. Tresses, monodromie et le groupe symplectique. Commentarii Mathematici Helvetici, 54(1):318–327, 1979.

[2] Joan S Birman. Braids, links, and mapping class groups, volume 82. Princeton University Press, 1974.

[3] Alexander Grothendieck et al. Revêtements étalés et groupe fondamental (SGA 1), Lecture Notes in Mathematics, 224. Springer-Verlag, 1971.

[4] James S Milne. Jacobian varieties. In Arithmetic geometry, pages 167–212. Springer, 1986.

[5] David Mumford. Tata lectures on theta II: Jacobian theta functions and differential equations. Progress in Mathematics, 43, 1984.

[6] David Mumford. Abelian varieties, 2nd edition. Oxford University Press, 1974.

[7] Rutger Noot. Abelian varieties – Galois representations and properties of ordinary reduction. Compositio Mathematica, 97(1):161–172, 1995.

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

[9] J.-P. Serre. Lettres à Ken Ribet du 1/1/1981 et du 29/1/1981, Collected Papers, Vol. IV. Springer-Verlag, Berlin-Heidelberg, 1996, pp. 1-20.

[10] Jiu-Kang Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case. preprint, 1997.