AN ABELIAN SUBEXTENSION OF THE DYADIC DIVISION FIELD OF A HYPERELLIPTIC JACOBIAN

JEFFREY YELTON

Abstract. Given a field $k$ of characteristic different from 2 and an integer $d \geq 3$, let $J$ be the Jacobian of the “generic” hyperelliptic curve given by $y^2 = \prod_{i=1}^{d}(x - \alpha_i)$, where the $\alpha_i$’s are transcendental and independent over $k$; it is defined over the transcendental extension $K/k$ generated by the symmetric functions of the $\alpha_i$’s. We investigate certain subfields of the field $K_\infty$ obtained by adjoining all points of 2-power order of $J(K)$. In particular, we explicitly describe the maximal abelian subextension of $K_\infty/K(J[2])$ and show that it is contained in $K(J[8])$ (resp. $K(J[16])$) if $d \geq 2$ (resp. if $d = 1$). On the way we obtain an explicit description of the abelian subextension $K(J[4])$, and we describe the action of a particular automorphism in $\text{Gal}(K_\infty/K)$ on these subfields.

1. Introduction

Let $k$ be any field of characteristic different from 2; let $\alpha_1, ..., \alpha_d$ be transcendental and independent over $k$ for some integer $d \geq 3$; and let $K$ denote the extension of $k$ obtained by adjoining the symmetric functions of the $\alpha_i$’s with separable closure denoted $\bar{K}$. The equation given by

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

defines a hyperelliptic curve $C$ of genus $g := [(d - 1)/2]$ over $K$. Its Jacobian, denoted by $J$, is a principally polarized abelian variety over $K$ of dimension $g$. For each integer $n \geq 1$, we write $J[2^n] \subset J(\bar{K})$ for the $2^n$-torsion subgroup of $J$ and $K_n := K(J[2^n])$ for the (finite algebraic) extension $K$ obtained by adjoining the coordinates of the points in $J[2^n]$ to $K$; we denote the (finite algebraic) extension $\bigcup_{n=1}^{\infty} K_n$ by $K_\infty = K(J[2^\infty])$. Let $T_2(J)$ denote the 2-adic Tate module of $J$; it is a free $\mathbb{Z}_2$-module of rank $2g$ given by the inverse limit of rank-2 $\mathbb{Z}/2^n\mathbb{Z}$-modules $J[2^n]$ with respect to the multiplication-by-2 map. The canonical principal polarization on $J$ defines the Weil pairing $e_2 : T_2(J) \times T_2(J) \rightarrow \mathbb{Z}_2$; it is a nondegenerate, skew-symmetric, $\mathbb{Z}_2$-bilinear pairing on $T_2(J)$. The Weil pairing $e_2$ is also Galois equivariant; hence, $K_\infty$ contains the multiplicative subgroup $\mu_2$ of 2-power roots of unity in the separable closure of $K$.

We have the natural action of the absolute Galois group $G_K = \text{Gal}(\bar{K}/K)$ on each $J[2^n]$; it is well known that this action respects the Weil pairing $e_2$ up to multiplication by the cyclotomic character $\chi_2 : G_K \rightarrow \mathbb{Z}_2^\times$. Each element $\sigma \in G_K$ therefore acts as an automorphism in the group

$\text{GSp}(T_2(J)) := \{\sigma \in \text{Aut}_{\mathbb{Z}_2}(T_2(J)) \mid e_2(P^\sigma, Q^\sigma) = \chi_2(\sigma)e_2(P, Q) \forall P, Q \in T_2(J)\}$

of symplectic similitudes. We denote this natural Galois action by $\rho_2 : G_K \rightarrow \text{GSp}(T_2(J))$ and each modulo-2$^n$ action by $\bar{\rho}_2 : G_K \rightarrow \text{GSp}(J[2^n])$. For any field $F$, we write $F(\mu_2)$ for the algebraic extension of $F$ obtained by adjoining all 2-power roots of unity. Clearly the image of $\rho_2$ is contained in the symplectic group

$\text{Sp}(T_2(J)) := \{\sigma \in \text{Aut}_{\mathbb{Z}_2}(T_2(J)) \mid e_2(P^\sigma, Q^\sigma) = e_2(P, Q) \forall P, Q \in T_2(J)\}$

if and only if $K = K(\mu_2)$. For each $n \geq 0$, we write $\Gamma(2^n) \triangleleft \text{Sp}(T_2(J))$ for the level-2$^n$ principal congruence subgroup consisting of automorphisms whose images modulo 2$^n$ are trivial.

It is well known that we always have $K_1 \subseteq k(\alpha_1, ..., \alpha_d)$ and that equality holds except when $d = 4$ (see [16]). The main purpose of this paper is to provide an explicit description of the maximal...
abelian subextension of $K_{\infty}/K_1$, which we denote by $K_{\infty}^{ab}$. (Below for any integer $n \geq 1$, we write $\zeta_{2^n} \in \bar{k}$ to denote a $2^n$th root of unity.)

**Theorem 1.1.** Let $\gamma_{i,j} = \alpha_j - \alpha_i$ (resp. $\gamma_{i,j} = (\alpha_j - \alpha_i) \prod_{l \neq i,j} (\alpha_l - \alpha_i)$) if $d = 2g + 1$ (resp. if $d = 2g + 2$) for $1 \leq i, j \leq 2g + 1$.

a) If $g \geq 2$ and $\zeta_4 \in \bar{k}$, we have

$$K_2(\mu_2) = K_1(\mu_2, \{\sqrt{\gamma_{i,j}}\}_{1 \leq i < j \leq 2g+1}) \subseteq K_{\infty}^{ab} = K_2(\mu_2, \{\sqrt[4]{\gamma_{i,j}}\}_{i=1}^{2g+1}) \subseteq K_3(\mu_2)$$

and $\text{Gal}(K_{\infty}^{ab}/K_1(\mu_2)) \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2$. If $\zeta_4 \notin \bar{k}$, we instead have $K_{\infty}^{ab} = K_2(\mu_2)$.

b) If $g = 1$ and $\zeta_8 \in \bar{k}$, we have

$$K_2(\mu_2) = K_1(\mu_2, \{\sqrt{\gamma_{i,j}}\}_{1 \leq i < j \leq 3}) \subseteq K_{\infty}^{ab} = K_2(\mu_2, \sqrt[4]{\gamma_12\gamma_13\gamma_2^2}, \sqrt[8]{\gamma_23\gamma_1^2\gamma_2^2}, \sqrt[8]{\gamma_23\gamma_3^2\gamma_12}, \sqrt[16]{\gamma_13\gamma_3^2}) \subseteq K_4(\mu_2)$$

and $\text{Gal}(K_{\infty}^{ab}/K_1(\mu_2)) \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^2$. If $\zeta_4 \notin \bar{k}$ but $\zeta_8 \in \bar{k}$, we instead have $K_{\infty}^{ab} = K_2(\mu_2, \sqrt[4]{\gamma_12\gamma_13\gamma_2}, \sqrt[8]{\gamma_23\gamma_1\gamma_2}, \sqrt[16]{\gamma_23\gamma_3}, \sqrt[32]{\gamma_23\gamma_1\gamma_3})$, and if $\zeta_8 \notin \bar{k}$, we instead have $K_{\infty}^{ab} = K_2(\mu_2)$.

c) Let $\sigma \in G_K$ be any Galois automorphism such that $p_2(\sigma) = -1 \in \text{GSp}(T_2(J))$. Then $\sigma$ acts on $K_{\infty}^{ab}$ by fixing $K_2(\mu_2)$, changing the signs of all generators of the form $\sqrt{\gamma_{i,j}}$, and fixing (resp. changing the signs of) the remaining generators given in (2) and (3) if $g$ is even (resp. if $g$ is odd).

The following corollary is proven via the argument in Step 4 of the proof of [16, Lemma 3].

**Corollary 1.2.** Let $a_0, ..., a_{d-1} \in k$ be distinct elements and let $J$ be the Jacobian of the hyperelliptic curve defined by the equation $y^2 = f(x) := x^d + \sum_{i=0}^{d-1} a_i x^i$. Let $\bar{a}_1, ..., \bar{a}_d \in \bar{k}$ denote the roots of the polynomial $f(x) \in k[x]$ and let $\gamma_{i,j} \in \bar{k}$ be given by formulas in terms of the $\bar{a}_i$'s analogous to those used to define the $\gamma_{i,j}$'s in the statement of Theorem 1.1.

a) If $g \geq 2$, we have the inclusion

$$k(\bar{J}[8]) \supseteq k(\bar{J}[2])(\{\sqrt{\gamma_{i,j}}\}_{1 \leq i < j \leq 2g+1}, \{\sqrt[4]{\gamma_{i,j}}\}_{i=1}^{2g+1}).$$

b) If $g = 1$, we have the inclusion

$$k(\bar{J}[16]) \supseteq k(\bar{J}[2])(\{\sqrt[2]{\gamma_{i,j}}\}_{1 \leq i < j \leq 2g+1}, \sqrt[8]{\gamma_12\gamma_13\gamma_2^2}, \sqrt[8]{\gamma_23\gamma_1^2\gamma_2^2}, \sqrt[8]{\gamma_23\gamma_3^2\gamma_12}, \sqrt[16]{\gamma_13\gamma_3^2}).$$

c) Let $\sigma$ be any automorphism in the absolute Galois group of $k$ which acts on $k(\bar{J}[16])$ as multiplication by $-1$. Then $\sigma$ acts on the subfields described above by changing the signs of all generators of the form $\sqrt{\gamma_{i,j}}$ and by fixing (resp. changing the signs of) all remaining generators given in (2) and (3) if $g$ is even (resp. if $g$ is odd).

**Remark 1.3.** We can also verify part (b) of Theorem 1.1 for the $d = 3$ case by combined use of the formulas given in [14] and [16]. We illustrate how to see that $K_4(\mu_2)$ contains an element whose 8th power is $\gamma_12\gamma_13\gamma_2^2$, as follows (one may use a similar argument for the other generators). For $n = 1, 2, 3$ and $1 \leq i < j < 3$, we fix elements $\sqrt[8]{\gamma_{i,j}} \in K$ whose 8th powers are $\gamma_{i,j} \in \bar{k}$ and which are compatible in the obvious way, and we fix a square root of $\sqrt[16]{\gamma_{1,2}} + \sqrt[16]{\gamma_{1,3}}$. (Note that due to the equivariance of the Weil pairing, $-1$ has a 8th root in $K(J[2n+1])$ for each $n \geq 1$.) Let $L$ be the 3-regular tree defined in [14], and assume the notation used throughout this paper. Let $\{\Lambda_0, \Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4\}$ be a non-backtracking path in $L$, where $\Lambda_0$ is the root and $\Lambda_1 = \Lambda(\alpha_1)$. Then it is tedious but straightforward to verify that there exists a decoration $\Psi : L \setminus \{\Lambda_0\} \rightarrow \bar{k}$ (see [14, Definition 1.2]) such that $\Psi(\Lambda_2), \Psi(\Lambda_3) = \gamma_{1,2} + \gamma_{1,3} \pm 2\sqrt[16]{\gamma_{1,2}\gamma_{1,3}}$;

$$\Psi(\Lambda_3), \Psi(\Lambda_3) = -\Psi(\Lambda_2) - (\Psi(\Lambda_2) - \Psi(\Lambda_2) \pm 4(\sqrt[16]{\gamma_{1,2}} + \sqrt[16]{\gamma_{1,3}}) \sqrt[16]{\gamma_{1,2}} \sqrt[16]{\gamma_{1,3}}) \sqrt[16]{\gamma_{1,2}} \sqrt[16]{\gamma_{1,3}} \sqrt[16]{\gamma_{1,2}} \sqrt[16]{\gamma_{1,3}};$$

and

$$\Psi(\Lambda_4) = -\Psi(\Lambda_3) - (\Psi(\Lambda_3) - \Psi(\Lambda_3)) + 4\sqrt[16]{2}(\sqrt[16]{\gamma_{1,2}} + \sqrt[16]{\gamma_{1,3}} + 2\sqrt[16]{\gamma_{1,2}} \sqrt[16]{\gamma_{1,3}}) \sqrt[16]{\gamma_{1,2}} \sqrt[16]{\gamma_{1,3}} \sqrt[16]{\gamma_{1,2}} \sqrt[16]{\gamma_{1,3}}.$$
By [14 Proposition 2.5(b)], we have \(\Psi(\Lambda_2), \Psi(\Lambda_2'), \Psi(\Lambda_3), \Psi(\Lambda_3'), \Psi(\Lambda_4) \in K_4\). Moreover, from [16 Theorem 1, Remark 11(b)], we see that \(\sqrt{2} (\sqrt[3]{71,2} + \sqrt[3]{71,3} + 2 \sqrt[3]{71,2} \sqrt[3]{71,3}) \in K_3\). It follows that

\[
\sqrt[3]{71,2} + \sqrt[3]{71,3} \not\in K_4.
\]

By [16 Theorem 1], we have \(\sqrt{\pm \gamma_{i,j}}, B_1 := \sqrt{-2\gamma_{2,3}} \sqrt[3]{71,2} + \sqrt[3]{71,3} \in K_3\). Therefore, we have

\[
\sqrt{-2\gamma_{2,3}} \sqrt[3]{71,2} \sqrt[3]{71,3} = -\sqrt{-2\gamma_{2,3}} \sqrt[3]{71,2} \sqrt[3]{71,3} / B_1 \in K_4.
\]

The rest of this paper is dedicated to a proof of Theorem 1.1; our plan is as follows. We will first assume that \(k = \mathbb{C}\) and prove Theorem 1.1 in that case by viewing the situation in a topological setting similar to the author’s strategy in [15]; we will retain this assumption throughout §2 and §3. In §2 we determine generators for the 4-torsion field \(K_2\), which is contained in \(K_{\infty}^{ab}\). Then in §3 we determine generators for \(K_{\infty}^{ab}\) over \(K_2\), treating the \(g \geq 2\) case and the \(g = 1\) case separately. Finally, in §4 we generalize these results to the situation where \(k\) is any field of characteristic different from 2.

2. The 4-division field over \(\mathbb{C}\)

We assume for this section as well as in §3 that \(k = \mathbb{C}\), so that \(K\) is generated over \(\mathbb{C}\) by the symmetric functions of the transcendental elements \(\alpha_i\). We will consider \(K\) as a subfield of the function field of the ordered configuration space \(Y_d\) of \(d\)-element ordered subsets of \(\mathbb{C}\); we view \(Y_d(\mathbb{C})\) as a topological space. The fundamental group of \(Y_d\) is well known to be the pure braid group on \(d\) strands, which we denote by \(P_d\). has a well-known presentation (see [3, Lemma 1.8.2]) with generators \(A_{i,j}\) for \(1 \leq i < j \leq d\). It is known (see [3] Corollary 1.8.4 and its proof) that the center of \(P_d\) is cyclically generated by the element \(\Sigma := A_{1,2}(A_{1,3}A_{2,3})...A_{1,d}A_{2,d}...A_{d-1,d} \in P_d\).

The profinite completion \(\hat{P}_d\) of \(P_d\) is the etale fundamental group of \(Y_d\) and may be identified with the Galois group of \(K^{unr}/K(\{\alpha_i\}_{1 \leq i \leq d})\), where \(K^{unr}\) is the maximal extension of \(K\) unramified away from the primes \((\alpha_j - \alpha_i)\) for \(1 \leq i < j \leq d\). The criterion of Néron-Ogg-Shafarevich ([12 Theorem 1]) implies that the natural \(\ell\)-adic representation \(\rho_{\ell}: G_K \to \text{GSp}(T_\ell(J))\), restricted to the subgroup fixing the Galois extension \(K(\{\alpha_i\}_{1 \leq i \leq d})\), factors through the restriction map \(\text{Gal}(K/K(\{\alpha_i\}_{1 \leq i \leq d})) \to \hat{P}_d\); we denote the induced representation of \(\hat{P}_d\) also by \(\rho_2\).

There is a “universal” family of hyperelliptic curves \(C \to Y_d\) whose fiber \(C_{\overline{z}}\) over each point \(\overline{z} = (z_1, ..., z_d) \in Y_d(\mathbb{C})\) is the hyperelliptic curve given by the monic polynomial in \(\mathbb{C}[x]\) whose roots are the elements of the \(d\)-element ordered set \(\overline{z}\); this family has \(C\) as its generic fiber. We write \(\rho^{top}: P_d \to \text{Aut}(H_1(C_{\overline{z}}, \mathbb{Z}))\) for the representation induced by the monodromy representation \(P_d \cong \pi_1(Y_d, \overline{z}_0) \to \text{Aut}(\pi_1(C_{\overline{z}_0}, P_0))\) associated to the family \(C \to Y_d\), where \(\overline{z}_0 := (1, ..., d) \in Y_d(\mathbb{C})\) and \(P_0 \in C_{\overline{z}_0}\) are basepoints. The monodromy action respects the intersection pairing on \(C_{\overline{z}_0}\), and therefore, the image of \(\rho^{top}\) is contained in the group of symplectic automorphisms \(\text{Sp}(H_1(C_{\overline{z}_0}, \mathbb{Z}))\). (See [14] §2 for more details of this construction.)

As both \(P_d\) and \(\text{Sp}(H_1(C_{\overline{z}_0}, \mathbb{Z}))\) are residually finite, the representation \(\rho^{top}\) induces a representation of the profinite completion \(\hat{P}_d\) on each pro-\(\ell\) completions \(H_1(C_{\overline{z}_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell \cong H_1(C_{\overline{z}_0}, \mathbb{Z})\). For each prime \(\ell\), we denote this representation by \(\rho^{top}_\ell: \hat{B}_d \to \text{Sp}(H_1(C_{\overline{z}_0}, \mathbb{Z})) \otimes \mathbb{Z}_\ell\). Our technique is to study \(\rho_2\) by relating it to the topologically-defined representation \(\rho^{top}_2\) using a key comparison result proved by the author as [15] Proposition 2.2] in §2.

**Lemma 2.1.** For any prime \(\ell\), there is an isomorphism of \(\mathbb{Z}_\ell\)-modules \(H_1(C_{\overline{z}_0}, \mathbb{Z}) \otimes \mathbb{Z}_\ell \cong T_\ell(J)\), making the representations \(\rho^{top}_\ell\) and \(\rho_\ell\) isomorphic.

We now state and prove some properties of the representation \(\rho^{top}\) that we will need below.
Proposition 2.2. a) The image of $P_d < B_d$ under $\rho^{\text{top}}$ coincides with the principal congruence subgroup $\Gamma(2) < \text{Sp}(H_1(C_{\mathfrak{z}}, \mathbb{Z}))$.

b) If $d$ is odd, we have $\rho^{\text{top}}(\Sigma) = -1 \in \Gamma(2)$.

c) If $d$ is even, we have $\rho^{\text{top}}(\Sigma) = 1 \in \Gamma(2)$ and $\rho^{\text{top}}(\Sigma') = -1 \in \Gamma(2)$, where $\Sigma' = A_{1,2}(A_{1,3}A_{2,3})...(A_{1,d-1}A_{2,d-1}...A_{d-2,d-1}) \in P_d$.

Proof. The statement of (a) has been shown in several works; see [1] Théorème 1, [10] Lemma 8.12, or [17] Theorem 7.3(ii).

Assume that $d$ is odd, so $d = 2g+1$, where $g$ is the genus of $C_{\mathfrak{z}}$. Then one deduces directly from the presentation of $P_d$ given by [3] Lemma 1.8.2 that the abelianization of $P_d$ is a free $\mathbb{Z}$-module of rank $2g^2+g$ whose generators are the images of the elements $A_{i,j}$, $1 \leq i < j \leq 2g+1$; its maximal abelian quotient of exponent 2 is therefore a $(2g^2+g)$-dimensional $\mathbb{F}_2$-vector space generated by the images of the $A_{i,j}$'s. Meanwhile, it follows directly from [11] Corollary 2.2 that the maximal abelian exponent-2 quotient of $\Gamma(2)$ also has rank $2g^2+g$. It follows that the restriction of $\rho^{\text{top}}$ to $P_d$ induces an isomorphism between the exponent-2 abelianizations of $P_d$ and $\Gamma(2)$. Now since $\Sigma$ is a product of each of the elements $A_{i,j} \in P_d$, it has nontrivial image in the exponent-2 abelianization of $P_d$ and therefore has nontrivial image in $\Gamma(2)$. However, as $\Sigma$ lies in the center of $P_d$ and $\rho^{\text{top}}(P_d) = \Gamma(2)$ by (a), the image $\rho^{\text{top}}(\Sigma)$ lies in the center of $\Gamma(2)$. The only nontrivial central element of $\Gamma(2)$ is the scalar $-1$, proving part (b).

Now assume that $d$ is even. Note that the family $C \rightarrow Y_d$ is an unramified degree-2 cover of the family $Y_{d+1} \rightarrow Y_d$ whose fiber over each $\mathfrak{z} = (z_1, ..., z_d) \in Y_d$ is $\mathbb{P}^1_{\mathbb{C}} \backslash \{z_1, ..., z_d\}$ $(Y_{d+1}$ is essentially the ordered configuration space of cardinality-$(d+1)$ subsets of $\mathbb{P}^1_{\mathbb{C}}$ whose first $d$ elements lie in $\mathbb{C}$). This implies that the monodromy action $\rho^{\text{top}}$ is induced by the monodromy action associated to the family $Y_{d+1} \rightarrow Y_d$ via the inclusion of and quotients by characteristic subgroups

$$\pi_1(\mathbb{P}^1_{\mathbb{C}}(\mathbb{C}) \backslash \{(z_i)_{1 \leq i \leq d}, \tilde{P}_0\}) \cong \pi_1(C_{\mathfrak{z}}(\mathbb{C}) \backslash \{(z_i, 0)\}_{1 \leq i \leq d}, P_0) \rightarrow \pi_1(C_{\mathfrak{z}}(\mathbb{C}), P_0)$$

(8) (here $\tilde{P}_0$ is the projection of the basepoint $P_0 \in C_{\mathfrak{z}}$). In fact, if we let $x_1, ..., x_d$ denote the generators of $\pi_1(\mathbb{P}^1_{\mathbb{C}}(\mathbb{C}) \backslash \{(z_i)_{1 \leq i \leq d}, \tilde{P}_0\}$ given in [7] §4, then $\pi_1(C_{\mathfrak{z}}(\mathbb{C}) \backslash \{(z_i, 0)\}_{1 \leq i \leq d}, P_0)$ is the subgroup generated by the elements $x_ix_{i+1}$ for $1 \leq i \leq d-1$ and $x_i^2$ for $1 \leq j \leq d$, and $\pi_1(C_{\mathfrak{z}}(\mathbb{C}), P_0)$ is the quotient of this by the elements $x_i^2$. Using the fact that the images of the elements $x_ix_{i+1}$ for $1 \leq i \leq d-2$ form a $\mathbb{Z}$-basis of the abelianization $H_1(C_{\mathfrak{z}}, \mathbb{Z})$, one may then explicitly compute the automorphisms of $H_1(C_{\mathfrak{z}}, \mathbb{Z})$ induced by $\Sigma$ and $\Sigma'$ using the statement and proof of [7] Lemma 4.1, thus verifying part (c). (One can also prove that $\rho^{\text{top}}(\Sigma) = 1$ using [7] Lemma 4.2 and the well-known fact that the kernel of Birman’s surjection onto the mapping class group coincides with the center of $P_d$.)

Below, for each integer $N \geq 1$, we fix $\zeta_N \in \mathbb{C}$ to be the $N$th root of unity given by $e^{2\pi i/N}$.

Lemma 2.3. For any integer $N \geq 1$, the maximal abelian exponent-$N$ subextension of $K^{\text{unr}}/K_1$ coincides with $K_1(\sqrt[1]{\zeta_j} - \zeta_i)_{1 \leq i < j \leq d}$. Each standard generator $A_{i,j}$ of $P_d \subset P_d = \text{Gal}(K^{\text{unr}}/K_1)$ acts on this subextension by sending $\sqrt[1]{\zeta_j} - \zeta_i$ to $\zeta_N \sqrt[1]{\zeta_j} - \zeta_i$ and fixing all of the other generators.

Proof. The first statement results from a standard application of Kummer theory. To prove the second statement, we fix some $N \geq 1$ and assume without loss of generality that $(i,j) = (d-1,d)$. Let $Y_d \rightarrow Y_d$ be the covering corresponding to the maximal abelian exponent-$N$ subextension of $K^{\text{unr}}/K_1$. We choose as a topological representative of $A_{i,j}$ the loop given by $t \mapsto (1, ..., d-1, d-1 + e^{2\pi i/N}t \epsilon/2) \in Y_d(\mathbb{C})$ for $t \in [0,1]$, where $\epsilon$ is a real number satisfying $\min_{1 \leq i \leq d-2} |z_{i+1} - z_i| > \epsilon > 0$ (we are allowed to move the basepoint to $(1, ..., d-1, d-1 + \epsilon/2) \in Y_d(\mathbb{C})$ because the monodromy action we are considering factors through the abelianization of the fundamental group). We have a closed embedding of the punctured disk $B^* := \{z \in \mathbb{C} \mid 0 < |z| < 1\}$
into $Y_d(\mathbb{C})$ given by $z \mapsto (1,\ldots,d-1,d-1+\varepsilon z)$ which takes a loop representing the standard generator of $\pi_1(B^*,1/2)$ to the loop representing $A_{d-1,d}$ defined above. The pullback of the cover $Y_d^{(N)}(\mathbb{C}) \to Y_d(\mathbb{C})$ via $B^* \to Y_d(\mathbb{C})$ is clearly homeomorphic to the cover $B^* \to B^*$ given by $z \mapsto z^N$. Locally, the standard generator of $\pi_1(B^*,1/2)$ acts on the ring of holomorphic functions defined on the covering space as $\zeta \cdot \zeta_N \zeta$, and the claim follows.

$$\Box$$

We are now ready to state and prove the main result of this section which explicitly describes the extension $K_2/K$ and in particular that it is abelian over $K_1$ and therefore contained in $K_\text{ab}$.

**Theorem 2.4.** For $1 \leq i, j \leq 2g + 1$, let $\gamma_{i,j}$ be defined as in the statement of Theorem 1.4. Then we have $K_2 = K_1(\{\sqrt{\gamma_{i,j}}\}_{1 \leq i < j \leq 2g+1})$. Moreover, any Galois automorphism in $G_K$ which acts as multiplication by $-1$ on the subgroup $J[4]$ acts on $K_2$ by fixing $K_1$ and changing the signs of all generators $\sqrt{\gamma_{i,j}}$.

**Proof.** For $g = 1$, this was already shown by the author as [16] Proposition 6(a),(b)], so we assume that $g \geq 2$. In particular, this means that $K_1 = \mathbb{C}(\{\alpha_i\}_{1 \leq i \leq d})$. The first statement of the theorem was proved for odd $d$ as [15], Proposition 3.1, but the following argument proves the full theorem for general $d$.

By [15] Corollary 1.2(c)], we have that $\rho_2$ induc3es an isomorphism $\rho_2 : \text{Gal}(K_2/K_1) \cong \Gamma(2)/\Gamma(4)$. We note from the proof of [11] Corollary 2.2] that the largest abelian quotient of $\Gamma(2)$ of exponent 2 is in fact $\Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^{2g+2}$; therefore, $K_2$ is the unique abelian subextension of $K_\infty/K_1$ of exponent 2. Since the extension $K_\infty/K_1$ is unramified over all primes of the form $(\alpha_j - \alpha_i)$, such a subextension must be a subgroup of $\bar{K}_2 := K_1(\{\sqrt{\alpha_j - \alpha_i}\}_{1 \leq i < j \leq 2d})$. If $d = 2g + 1$, then $\text{Gal}(\bar{K}_2/K_1)$ already has rank $2g^2 + g$ and therefore $K_2 = K_2$; moreover, Proposition 2.2(b) combined with Lemma 2.3 implies that any Galois element whose image under $\bar{\rho}_2$ is $-1 \in \Gamma(2)/\Gamma(4)$ changes the sign of each $\sqrt{\alpha_j - \alpha_i} = \sqrt{\gamma_{i,j}}$. This proves the statement in the $d = 2g + 1$ case.

Now suppose that $d = 2g + 2$. Then $\text{Gal}(\bar{K}_2/K_1)$ has rank $d(d - 1)/2 > 2g^2 + g$, which implies that $K_2 \subsetneq \bar{K}_2$. Kummer theory then tells us that $\text{Gal}(K_2/K_1)$ is canonically identified with the dual of some subgroup $H \subset K_1^\times/(K_1^\times)^2$, where both are considered as vector spaces over $\mathbb{F}_2$ of dimension $2g^2 + g$. Clearly $H$ is a subspace of the space $\bar{H} \subset K_1^\times/(K_1^\times)^2$ (which itself is the dual of $\text{Gal}(K_2/K_1)$) generated by images of the elements $\alpha_j - \alpha_i$ for $1 \leq i < j \leq d$; we write $[\alpha_j - \alpha_i] = [\alpha_i - \alpha_j] \in \bar{H}$ for each such image and use additive notation for elements of $\bar{H}$.

We now identify $H$ with its dual $\text{Gal}(K_2/K_1)$ via the basis $\{[\alpha_j - \alpha_i]\}_{1 \leq i < j \leq d}$ of $\bar{H}$. Lemma 2.3 implies that the image of each $A_{i,j} \in P_d \subset \bar{P}_d = \text{Gal}(K_{\text{unr}}/K_1)$ under $\rho_2$ composed with reduction modulo 4 is $[\alpha_j - \alpha_i] \in H = \text{Gal}(K_2/K_1)$. It follows from Proposition 2.2(c) that each element of $H$ must be the sum of an even number of generators of $\bar{H}$.

We note that the degree-$(d-1)$ curve $C' : y^2 = \prod_{i=1}^{d-1} (x_i - 1/(\alpha_{2g+2} - \alpha_i))$ is isomorphic to the degree-$d$ curve $C : y^2 = \prod_{i=1}^{2g+2} (x - \alpha_i)$ over the quadratic extension $K(\beta)/K$ given by

$$(x', y') \mapsto (1/(\alpha_{2g+2} - x), y/(\beta(\alpha_{2g+2} - x)^{g+1})), $$

where $\beta \in K$ is a square root of the element $\prod_{i=1}^{2g+1} (\alpha_{2g+2} - \alpha_i)$. (This is just the isomorphism of hyperelliptic curves induced from an automorphism of the projective line which moves $\alpha_{2g+2}$ to $\infty$.)

From what was shown above for the odd-degree case, we have

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

Thus, $K_2(\beta)$ is generated over $K_1(\{\sqrt{\gamma_{i,j}}\}_{1 \leq i < j \leq 2g+1})$ by the element $\beta$. Since each $\gamma_{i,j}$ corresponds to the element $[\alpha_j - \alpha_i] + \sum_{i \neq j} [\alpha_{2g+2} - \alpha_i] \in H$, which is the sum of an even number of generators while $\beta^2$ corresponds to $\sum_{i \neq 2g+2} [\alpha_{2g+2} - \alpha_i] \in H$, which is not, the extension
$K_1(\{\sqrt{3_{i,j}}\}_{1\leq i<j\leq 2g+1})/K_1$ must be the fixed field corresponding to $H \subset \bar{H}$ and therefore coincides with $K_2$. Moreover, the braid $\Sigma' \in P_{2g+2}$ defined in the statement of Proposition 2.3(c) corresponds to a Galois automorphism whose restriction to $K_\infty$ is $-1 \in \Gamma(2) \cong \text{Gal}(K_\infty/K_1)$ by that proposition, and Lemma 2.3 implies that $\Sigma'$ changes the sign of each $\sqrt{3_{i,j}}$, thus implying that any Galois element whose image under $\rho_1$ is $-1 \in \Gamma(2)/\Gamma(4)$ acts in this way, hence the statement in the $d = 2g + 2$ case.

3. The maximal abelian subfield over $\mathbb{C}$

3.1. The abelianization of the Galois group. We retain our assumption from the last section that $k = \mathbb{C}$. Having found a particular abelian subextension of $K_\infty/K_1$, namely $K_2/K_1$, we shall now determine the maximal abelian subextension. In order to do this, we first need to know what its Galois group over $K_1$ looks like.

Lemma 3.1. The abelianization $\Gamma(2)^{ab}$ of the principal congruence subgroup $\Gamma(2) \triangleleft \text{Sp}_{2g}(\mathbb{Z}_2)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g-2} \times (\mathbb{Z}/4\mathbb{Z})^{2g}$ (resp. $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^2$), and the abelianization map $\pi : \Gamma(2) \to \Gamma(2)^{ab}$ factors through $\Gamma(2)/\Gamma(8)$ (resp. $\Gamma(2)/\Gamma(16)$) if $g \geq 2$ (resp. if $g = 1$).

Proof. The description of $\Gamma(2)^{ab}$ for the $g \geq 2$ case is given by [11] Corollary 2.2. We therefore assume that $g = 1$ and proceed to compute the commutator subgroup $[\Gamma(2), \Gamma(2)] < \Gamma(2)$.

We first claim that $[\Gamma(2), \Gamma(2)]$ contains $\Gamma(16)$. Write $\sigma = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$ and $\tau = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. We verify by straightforward computation that for any integers $m, n \geq 1$, we have the formula

$$\sigma^m \tau^n \sigma^{-m} \tau^{-n} = \begin{bmatrix} 1 - 2^{m+n} & 2^{2m+n} \\ -2^{m+n} & 1 + 2^{m+n} + 2^{2m+n} \end{bmatrix} \in [\Gamma(2), \Gamma(2)].$$

Using this formula, we compute $(\sigma^2 \tau^{-2} \tau^{-1})(\sigma \tau \sigma^{-1} \tau^{-1})^2 \equiv \tau^8$, $(\sigma^2 \tau^{-2} \tau^{-1})(\sigma \tau \sigma^{-1} \tau^{-1})^2 \equiv \sigma^8$, and $(\sigma \tau \sigma^{-1} \tau^{-1})^4 \equiv 17$ modulo 32. It is easy to show that for $n \geq 1$, the images modulo $2^{n+1}$ of $\sigma^{2n-1}$, $\tau^{2n-1}$, and the scalar matrix $1 + 2^n$ generate $\Gamma(2^n)/\Gamma(2^{n+1}) \cong (\mathbb{Z}/2\mathbb{Z})^3$; thus, in particular, $[\Gamma(2), \Gamma(2)]$ contains $\Gamma(16)$ modulo 32. Now we show by induction that for each $n \geq 5$, $[\Gamma(2), \Gamma(2)]$ contains $\Gamma(2^n)$ modulo $2^{n+1}$, which suffices to prove that $[\Gamma(2), \Gamma(2)] \supset \Gamma(16)$. Assume this is the case for $n - 1$; then in particular, $[\Gamma(2), \Gamma(2)]$ contains elements which are equivalent modulo 2 to $\sigma^{2n-2}$, $\tau^{2n-2}$, and $1 + 2^{n-1}$. On computing that the squares of such elements must be equivalent modulo $2^{n+1}$ to $\sigma^{2n-1}$, $\tau^{2n-1}$, and $1 + 2^n$ respectively, the claim is proven.

We next claim that the image of $[\Gamma(2), \Gamma(2)]$ modulo 16 is cyclically generated by the image modulo 16 of $\sigma \tau \sigma^{-1} \tau^{-1}$. To see this, we recall the well-known fact that $\Gamma(2)$ decomposes as the direct product of $\{\pm 1\}$ and the subgroup generated by $\sigma$ and $\tau$ and therefore, $[\Gamma(2), \Gamma(2)]$ coincides with the commutator subgroup of $\langle \sigma, \tau \rangle < \Gamma(2)$. On checking that $\sigma \tau \sigma^{-1} \tau^{-1}$ commutes with both $\sigma$ and $\tau$ modulo 16, we deduce as an easy exercise in group theory that the commutator of any two elements in $\Gamma(2)/\Gamma(16)$ is a power of the image of $\sigma \tau \sigma^{-1} \tau^{-1}$. Since the smallest normal subgroup of $\Gamma(2)/\Gamma(16)$ containing these powers is simply the cyclic subgroup generated by the image of $\sigma \tau \sigma^{-1} \tau^{-1}$, we have proven the claim.

Now it follows from the fact that $\Gamma(2^n)/\Gamma(2^{n+1}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ for $n \geq 1$ that $\Gamma(2)/\Gamma(16)$ has order $2^9 = 512$; meanwhile, we see from what we have computed above that the image of $\sigma \tau \sigma^{-1} \tau^{-1}$ modulo 16, which generates the image of $[\Gamma(2), \Gamma(2)]$, has order 4. Therefore, the $\Gamma(2)^{ab}$ has order 128. Since $\Gamma(2)^{ab}$ is generated by the images of $-1$, $\sigma$, and $\tau$ modulo $[\Gamma(2), \Gamma(2)]$, the first statement of the lemma follows from the easy verification (by considering the image of $[\Gamma(2), \Gamma(2)]$ modulo 16) that the images of $\sigma$ and $\tau$ each have order 8 in $\Gamma(2)^{ab}$. \hfill \qed
In order to find the extension of $K_1$ corresponding to the Galois quotient described by the lemma, we consider the $g \geq 2$ and $g = 1$ cases separately.

3.2. The $g \geq 2$ case. Lemma 3.1 together with the results of [2] and the fact that $K_\infty \subset K^\text{unr}$, implies that $K_{ab}^\infty$ is an extension of $K_2 = K_1/(\sqrt{\alpha_j - \alpha_i})$ obtained by adjoining $2g$ independent 4th roots of products of the elements $(\alpha_j - \alpha_i)$. Similarly to what we saw in the proof of Theorem 2.4, Kummer theory tells us that $\text{Gal}(K_{ab}^\infty/K_2)$ is canonically identified with some subgroup $V \subset K_2^\times/(K_2^\times)^2$, where both are considered as vector spaces over $\mathbb{F}_2$ of dimension $2g$. In fact, since $K_\infty \subset K^\text{unr}$, the first statement of Lemma 2.3 implies that $V$ is also a subspace of the space $\overline{V}$ generated by the images in $K_2^\times/(K_2^\times)^2$ of elements of the form $\sqrt{\alpha_j - \alpha_i}$, where $\overline{K}_2 = K_2(\sqrt{\alpha_j - \alpha_i})$. In our situation, this turns out to be the case.

When $g = 2$, we claim that the representation $(\psi)$ is isomorphic to the standard representation of $S_d$ over $\mathbb{F}_2$ (see [13] §2 for the construction of the standard representations over characteristic 2 of dimension $d - 1$ if $d$ is odd and of dimension $d - 2$ if $d$ is even).

As $V$ is a vector space over $\mathbb{F}_2$ of dimension $2g$, one candidate for the action $\psi$ is the well-known standard representation of $S_d$ over $\mathbb{F}_2$ (see [13] §2.2 for the construction of the standard representations over characteristic 2 of dimension $d - 1$ if $d$ is odd and of dimension $d - 2$ if $d$ is even).

In our situation, this turns out to be the case.

Proof. We fix a symplectic ordered basis $\{a_1, ..., a_g, b_1, ..., b_g\}$ of $T_2(J)$, i.e. a basis satisfying $e_2(a_i, b_j) = -1 \in \mathbb{Z}_2$ for $1 \leq i \leq g$ and $e_2(a_i, b_j) = 0$ for $1 \leq i < j \leq g$ and such that the image of each $a_i$ (resp. each $b_i$) in $J[2]$ is represented by the even-cardinality subset of roots given by $\{\alpha_{2i - 1}, \alpha_{2i}\}$ (resp. $\{\alpha_{2i}, ..., \alpha_{2g+1}\}$); see the statement and proof of [10, Corollary 2.11] for a description of the elements in $J[2]$ in terms of the roots $\alpha_i$. In the following argument, we use the description of $[\Gamma(2), \Gamma(2)]$ given by [11, Proposition 2.1] as the subgroup of matrices (with respect to our symplectic basis) in $\text{Sp}(T_2(J))$ which lie in $\Gamma(4)$ and whose $(i, i + g)$th and $(i + g, i)$th entries are divisible by 8 for $1 \leq i \leq g$. Note in particular that the automorphisms given by $v \mapsto v + 4e_2(v, a_i)a_i$ and $v \mapsto v + 4e_2(v, b_i)b_i$ each have $\pm 4$ as their $(i, i + g)$th or $(i + g, i)$th entries respectively, so their images in $\Gamma(4)/[\Gamma(2), \Gamma(2)]$ are nontrivial and distinct and in fact form a basis for the $\mathbb{F}_2$-space $\Gamma(4)/[\Gamma(2), \Gamma(2)]$.

We claim that the representation $(\psi)$ is faithful. Indeed, suppose that $\psi$ has nontrivial kernel. Since $d \geq 5$, this implies that the kernel of $\psi$ contains $A_d < S_d$. Consider any element of $V$, written as a linear combination $\sum_{1 \leq i < j \leq 2g+1} c_{i,j}[i, j] \in V$ with $c_{i,j} \in \mathbb{F}_2$; by our assumptions this element must be fixed by $A_d$. But then the 2-transitivity of $A_d$ implies that the $c_{i,j}$’s are all equal, so that $V$ is spanned by the element $\sum_{1 \leq i < j \leq 2d}[i, j]$, which contradicts the fact that $V$ is 2$g$-dimensional.

If $g \geq 3$, then [13, Theorem 1.1] implies that $(\psi)$ is isomorphic to the standard representation of $S_d$, and we are done. We therefore assume that $g = 2$. It follows from the statement and proof of [13, Lemma 3.2][iii],[iv] that $(\psi)$ is isomorphic to the standard representation if and only if the transpositions in $S_d$ map to transvections in $\text{Aut}(V)$ (in this context a transvection is defined to be any operator $A \in \text{Aut}(V)$ such that $A - 1$ has rank 1). It therefore suffices to show that the transposition $(12) \in S_d$ acts on $V$ as a transvection. This is equivalent to the claim that...
any element of $G_2$ whose image modulo 2 is $(12) \in S_d = \text{Gal}(K_1/K)$ acts by conjugation on $\Gamma(4)/[\Gamma(2),\Gamma(2)] \cong \text{Gal}(K_{ab}/K_2)$ (which is the dual of $V$) as a transvection. For any $a \in T_2(J)$, let $T_a \in \text{Aut}(V)$ denote the automorphism given by $v \mapsto v + c_2(v,a)a$. Then we see from the description of elements of $J[2]$ in terms of subsets of the set of $\alpha_i$'s which was mentioned above that the image of $T_{a_1} \in \text{Sp}(T_2(J))$ modulo 2 is $(12)$; since (as noted above) $\{T_{a_1},T_{a_2},T_{b_1},T_{b_2}\}$ is an $F_2$-basis of $\Gamma(4)/[\Gamma(2),\Gamma(2)]$, we only need to calculate the conjugates of each of these basis elements by $T_{a_1}$. We compute that $T_{a_1}$ commutes with each of them except for $T_{b_1}^4$, and that

$$T_{a_1}T_{b_1}T_{a_1}^{-1} = T_{b_1}T_{a_1}^{-1} \mod ([\Gamma(2),\Gamma(2)])$$

Thus, we have seen that $T_{a_1}$ minus the identity operator acts on the $F_2$-space $\Gamma(4)/[\Gamma(2),\Gamma(2)]$ by sending all basis elements to 0 except for $T_{b_1}^4$, which it sends to $T_{a_1}^4$. Therefore, $T_{a_1}$ acts as a transvection, as desired.

Now the following proposition suffices to prove Theorem 3.1(a) when $k = C$.

**Proposition 3.3.** The subspace $V$ defined above is generated by the images in $\bar{\Gamma}$ of the elements $\prod_{j \neq i} \sqrt{\gamma_{i,j}} \in K_2^\times$ for $1 \leq i \leq 2g + 1$.

**Proof.** For $1 \leq i < j \leq 2g + 1$, we write $[i,j]' = [j,i]'$ for the elements of $K_2^\times/(K_2^\times)^2$ represented by $\sqrt{\gamma_{i,j}}$ (note that $[i,j]' = [i,j]$ in the $d = 2g + 1$ case); we need to show that $V$ is spanned as an $F_2$-space by the set $\{\prod_{j \neq i}[i,j]'_1 \leq i \leq 2g+1\}$.

We know from Lemma 3.2 that the action $\psi : S_d \to \text{Aut}(V)$ defines the standard representation of $S_d$ of dimension $d - 1$ (resp. $d - 2$) if $d$ is odd (resp. even). We first assume that $d = 2g + 1$. By the construction of the standard representation, there exist elements $v_i \in V$ for $1 \leq i \leq 2g + 1$ which span $V$ and satisfy the unique linear relation $\sum_{1 \leq i \leq 2g+1} v_i = 0$, and such that $S_{2g+1}$ acts on the set of $v_i$'s by $v_i'^\sigma = v_{\sigma(i)}$ for each permutation $\sigma$. We claim that $v_i = \sum_{j \neq i}[1,j]'$, from which it follows by acting on $v_i$ by any transposition $(1i)$ that $v_i = \sum_{j \neq i}[i,j]'_2 \leq i \leq 2g + 1$, and we get the desired spanning set for $V$.

As $v_i$ is obviously nontrivial, some $[s,t]$ appears in its expansion as a linear combination of basis elements of $\bar{\Gamma}$. Suppose that $1 \in \{s,t\}$. Then the elements $[1,j]$ appear in the expansion of $v_i$ for all $2 \leq j \leq 2g + 1$, due to the fact that $v_i$ is fixed by every permutation in $S_{2g+1}$ which fixes 1. If, on the other hand, $1 \notin \{s,t\}$, then by a similar argument, all elements $[s,t]$ with $1 \notin \{s,t\}$ appear in the expansion of $v_i$. It follows that either (i) $v_i = \sum_{j \neq 1}[1,j]'$, (ii) $v_i = \sum_{s,t \neq 1}[s,t]'$, or (iii) $v_i = \sum_{1 \leq s < t \leq 2g+1}[s,t]'$. In case (ii), we see that $\sum_{1 \leq i \leq 2g+1} v_i = \sum_{1 \leq i < 2g+1}[s,t]' \neq 0$, a contradiction. In case (iii), we see that $v_i$ is fixed by all elements of $S_{2g+1}$ and therefore, all the elements $v_i$ are equal, which contradicts the fact that $V$ has dimension $2g$. Therefore, (i) is the case, and we are done.

Now assume that $d = 2g + 2$. By the construction of the standard representation, there exist elements $v_{i,j} = v_{j,i} \in V$ for $1 \leq i < j \leq 2g + 2$ such that for any $i$, $\{v_{i,j}\}_{j \neq i}$ spans $V$ and satisfies the unique linear relation $\sum_{j \neq i} v_{i,j} = 0$; such that $v_{s,t} + v_{s,j} = v_{i,j}$ for distinct $s,t,j$; and such that $S_{2g+2}$ acts on the set of $v_{i,j}$'s by $v_{i,j}' = v_{\sigma(i),\sigma(j)}$ for each permutation $\sigma$. We claim that $v_{1,2g+2} = \sum_{2 \leq j \leq 2g+1}[1,j]'$, from which we can again see by acting on $v_{1,2g+2}$ by any transposition $(1i)$ that $v_{i,2g+2} = \sum_{j \neq i}[i,j]'_2 \leq i \leq 2g + 1$, and we again get the desired spanning set for $V$.

By a similar analysis to what was done for the $d = 2g + 1$ case, we deduce that $v_{1,2g+2}$ is some linear combination of the elements $[i,2g+2], \sum_{2 \leq j \leq 2g+1}[1,j] + [2g+2,j]$, and $\sum_{2 \leq s < t \leq 2g+1}[s,t]$. We first note that $v_{1,2g+2}$ cannot be the sum of an odd number of terms $[s,t]$, because then that would be the case for each other $v_{i,2g+2}$, and then the $2g+1$ terms $v_{i,2g+2}$ could not sum to 0. We also note that, as in the $d = 2g + 1$ case, the element $v_{1,2g+2}$ cannot be trivial nor equal to the sum $\sum_{1 \leq s < t \leq 2g+2}[s,t]$. Finally, it is straightforward to check that if $\sum_{2 \leq s < t \leq 2g+1}[s,t]$ appears
in the expansion of $v_{1,2g+2}$, then the $v_{s,t} + v_{s,j} = v_{t,j}$ property does not hold. Our only remaining choice is that $v_{1,2g+2} = \sum_{2 \leq j \leq 2g+1} (\lfloor 1, j \rfloor + [2g+2, j]) = \sum_{2 \leq j \leq 2g+1} \lfloor 1, j \rfloor'$, and we are done.

3.3. The $g = 1$ case. Lemma 3.1 together with the results of [2] and the fact that $K_\infty \subseteq K_{\text{unr}}$, imply that $K_{ab}^\infty$ is an extension of $K_2 = K_1(\sqrt{7_1,2}, \sqrt{7_1,3}, \sqrt{7_2,3})$ obtained by adjoining 2 independent 4th roots of products of the elements $\gamma_{i,j} \in K_1$ (recall from [16] that $K_1$ is generated over $K$ by the $\gamma_{i,j}$'s both for $d = 3$ and $d = 4$). Therefore, in this case, we get via Kummer theory a canonical identification of $\text{Gal}(K_{ab}^\infty/K_2)$ with some subgroup $V \subseteq K_2^\times/(K_2^\times)^4$; the submodule $V$ of the $\mathbb{Z}/4\mathbb{Z}$-module $K_2^\times/(K_2^\times)^4$ is free of rank 2. In fact, $V$ is contained in the rank-3 free submodule $\tilde{V} \subseteq K_2^\times/(K_2^\times)^4$ generated by images of the elements $\sqrt{\gamma_{i,j}} \in K_2^\times$. We denote each of these images by $[i,j]' = [j,i]' \in \tilde{V}$. We now proceed to explicitly determine the rank-$2$ submodule $V \subset \tilde{V}$.

As with the $g \geq 2$ case, we have an action of $G_2$ on $V$ which factors through the quotient $\text{Gal}(K_1/K)$; this quotient is isomorphic to $S_3$ both when $d = 3$ and when $d = 4$. This action sends a permutation $\sigma \in S_3$ to the automorphism of $V$ determined by $[i,j]' = [\sigma(i), \sigma(j)]'$ for $1 \leq i < j \leq 3$. We again write $\psi : S_3 \to \text{Aut}(V)$ for this action. The following proposition suffices to prove Theorem 1.1(b) when $k = \mathbb{C}$.

**Proposition 3.4.** The submodule $V \subset \tilde{V}$ is generated by

$$\{[1,2]' + [1,3]', [2,3]', [2,1]' + [2,3]', 2[3,1]', 2[3,2]' + 2[1,2]'\} \subset \tilde{V}.$$  

**Proof.** We first note that the action $\psi$ has trivial kernel, by the same argument as was used in the proof of Proposition 3.3. Since $\text{Aut}(V/2V) \cong \text{SL}_2(\mathbb{F}_2) \cong S_3$, this implies that the induced action of $\psi$ modulo $2V$ is isomorphic to the standard representation of $S_3$. By essentially the same argument that was used in the proof of Proposition 3.3 for the odd-degree case, this shows that $V/2V$ is spanned by the images modulo 2 of the elements $\sigma_{j\neq i}[i,j]'$ for $i = 1, 2, 3$, implying that

$$2[1,2]' + 2[1,3]', 2[2,3]', [2,1]' + 2[2,3]', 2[3,1]', 2[3,2]' + 2[1,2]' \in V.$$  

Therefore, the element $2[1,2]' + 2[1,3]' + 2[2,3]' \in \tilde{V}$ cannot lie in $V$, because otherwise $V$ would contain the subgroup generated by $2[1,2]', 2[1,3]', 2[2,3]'$ which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, contradicting the fact that $V$ has rank 2.

Let $\Phi : \tilde{V} \to \mathbb{Z}/4\mathbb{Z}$ be the functional sending $c_1[2,3]' + c_2[3,1]' + c_3[1,2]'$ to $c_1 + c_2 + c_3 \in \mathbb{Z}/4\mathbb{Z}$. We claim that $V$ coincides with the kernel of $\Phi$. Suppose that for some $v \in V$, we have $\Phi(v) \neq 0$. Since $\Phi(\psi(\sigma)(v)) = \Phi(v)$ for all $\sigma \in S_3$, we have $\Phi(\sum_{\sigma \in A_3} \psi(\sigma)(v)) = 3\Phi(v) \neq 0$. But $\sum_{\sigma \in A_3} \psi(\sigma)(v) \in V$ is fixed by $A_3 \triangleleft S_3$ and is therefore some nontrivial multiple of $[1,2]' + [1,3]' + [2,3]' \in \tilde{V}$, which contradicts the fact that $2[1,2]' + 2[1,3]' + 2[2,3]' \notin V$, hence the claim. Since the image of $\Phi$ has order 4, its kernel $V$ has order $64/4 = 16$. Meanwhile, the generators given in the statement of the proposition lie in $V$, and the statement now follows from the elementary verification that the group they generate also has order 16.

3.4. The action of $-1$. We have shown that parts (a) and (b) of Theorem 1.1 hold when $k = \mathbb{C}$; we will now prove that the element $-1 \in \Gamma(2) \cong \text{Gal}(K_\infty/K_1)$ acts as stated in Theorem 1.1(c), and then the full theorem will be proved over the complex numbers. In the odd-degree case, it follows immediately from the fact that $\rho^{\text{top}}(\Sigma) = -1$ by Proposition 2.2(b) combined with Lemma 2.3 that since $\gamma_{i,j} = \alpha_j - \alpha_i$, the element $-1$ acts trivially (resp. by sign change) on the generators of $K_{ab}^\infty/K_2$ listed in the statement of the theorem if $g$ is even (resp. if $g$ is odd). Similarly in the even-degree case, it follows immediately from the fact that $\rho^{\text{top}}(\Sigma') = -1$ by Proposition 2.2(c) combined with Lemma 2.3 that since $\gamma_{i,j} = (\alpha_j - \alpha_i)\prod_{l \neq i,j}(\alpha_{2l+2} - \alpha_l)$, the element $-1$ acts trivially (resp. by sign change) on the generators of $K_{ab}^\infty/K_2$ listed in the statement of the theorem if $g$ is even (resp. if $g$ is odd).
4. Proof of the Theorem in the General Case

We have now shown that Theorem 1.1 holds when $k = \mathbb{C}$; we will now prove that this suffices to show that Theorem 1.1 holds in general. In this section, whenever the ground field $k$ is specified (e.g. $k = \mathbb{Q}$), we will write $K_k$ (e.g. $K_\mathbb{Q}$) for the extension of $k$ obtained by adjoining the symmetric functions of the independent transcendental elements $\alpha_1, \ldots, \alpha_d$; our goal is to show that the particular generators of $(K_C)_{\infty}^{ab}/K_C$ that we found in [2], [3] can also be used to generate $K_{\infty}^{ab}/K$ (and that any Galois element mapping to $-1 \in \text{GSp}(T_2(J))$ acts in the same way on them), where $K = K_k$ for any field $k$ of characteristic different from $2$. The rest of this section will be devoted to proving the following proposition.

**Proposition 4.1.** To prove Theorem 1.1 it suffices to prove the statement when $k = \mathbb{C}$.

We assume that $g \geq 2$ and only prove part (a) of the theorem as well as part (c) for the $g \geq 2$ case, noting that the claims for the $g = 1$ case result from very similar arguments. In what follows, we will freely use the obvious fact that given an abelian variety $A$ over a field $F$ and an extension $F'/F$, the finite algebraic extension $F'(A[2^n])$ coincides with the compositum $F'_2/F(A[2^n])$ for any $n \geq 1$. We first need the following lemmas.

**Lemma 4.2.** Let $k$ be any field of characteristic different from $2$ with separable closure $\bar{k}$. Then we have

a) $\text{Gal}(K_n(\mu_2)/K_1(\mu_2)) \cong \Gamma(2)/\Gamma(2^n)$ for $n \geq 1$ and thus $\text{Gal}(K_{\infty}(\mu_2)/K_1(\mu_2)) \cong \Gamma(2)$; and

b) $K_n \cap \bar{k} = k(\zeta_{2^n})$ for $n \geq 1$ and thus $K_{\infty} \cap \bar{k} = k(\mu_2)$.

**Proof.** The author has shown (a) for $k$ of characteristic $0$ (as [15, Proposition 4.1]) but the following argument proves (a) in the case of positive characteristic also. We first claim that the image of $\rho_2$ in $\text{GSp}(T_2(J))$ contains a transvection given by $v \mapsto v + e_2(v, a) a$ for some $a \in T_2(J) \setminus \mathcal{T}_2(J)$. This follows from the discussion in [2], §2.3 (see also [5], §3.1 and [6], §9-10 and note that the argument holds in positive characteristic as well). Meanwhile, since the polynomial defining the hyperelliptic curve $C$ has full Galois group, the image of $\rho_2$ is isomorphic to $S_{2g+1}$ or $S_{2g+2}$. It now follows from [3], Theorem 2.1.1, §2.2 that the image $G_2$ of $\rho_2$ in $\text{GSp}(T_2(J))$ contains $\Gamma(2) \wr \text{Sp}(T_2(J))$. After restricting to the absolute Galois group of $K_1(\mu_2)$, this image coincides with $\Gamma(2)$, and (a) immediately follows.

The linear disjointness of $K_n(\mu_2)$ and $\bar{k}K_1$ over $K_1(\mu_2)$ follows immediately from the fact that $\text{Gal}(kK_n/kK_1) \cong \text{Gal}(K_n(\mu_2)/K_1(\mu_2)) \cong \Gamma(2)/\Gamma(2^n)$ by part (a). Moreover, it is well known from our description of 2-torsion fields discussed above that $K_1(\mu_2) \cap \bar{k} = k(\mu_2)$, so we get $K_n(\mu_2) \cap \bar{k} = (K_n(\mu_2) \cap \bar{k}K_1) \cap \bar{k} = k(\mu_2)$. It follows that we have $K_{\infty} \cap \bar{k} = k(\mu_2)$, so to prove part (b) it suffices to show that $K_n \cap k(\mu_2) = k(\zeta_{2^n})$ for $n \geq 1$.

Let $\bar{\Gamma}(2^n) \triangleleft \text{GSp}(T_2(J))$ denote the kernel of reduction modulo $2^n$ for each $n \geq 1$, and write $G_2 \subset \text{GSp}(T_2(J))$ for the image of $\rho_2$. It is clear that $G_2 \cap \bar{\Gamma}(2^n)$ is isomorphic to the subgroup of $\text{Gal}(K_\infty/K)$ fixing $K_n$; meanwhile, part (a) says that $G_2 \cap \Gamma(2) = \Gamma(2)$ is isomorphic to the Galois subgroup fixing $k(\mu_2)$. Therefore, $K_n \cap k(\mu_2)$ is the fixed field of the subgroup of $\text{Gal}(K_\infty/K)$ generated by $G_2 \cap \bar{\Gamma}(2^n)$ and $\Gamma(2)$, which is easily seen to coincide with the kernel of the mod-$2^n$ determinant map $G_2 \to (\mathbb{Z}/2^n\mathbb{Z})^\times$. But by equivariance of the Weil pairing, the fixed field of this subgroup coincides with $k(\zeta_{2^n})$, and we are done.

Let $J_0$ denote the Jacobian of the hyperelliptic curve $C_0$ defined over $K_\mathbb{Q}$ given by the equation in (1). Note that $C_0$ admits a smooth model $\mathcal{C}$ over $S := \text{Spec}(\mathbb{Z}[1/2, \{\alpha_i\}_{1 \leq i \leq d}, \{(\alpha_i - \alpha_j)^{-1}\}_{1 \leq i < j \leq 2g+1}]^{S_2})$, where the superscript "$S_d$" indicates taking the subring of invariants under the obvious permutation action on the $\alpha_i$'s. Define $J \to S$ to be the abelian scheme representing the Picard functor of the
scheme \( \mathcal{C} \to S \) (see \cite[Theorem 8.1]{9}). Note that the ring \( \mathbb{Z} \left[ \frac{1}{2}, \{ \alpha_i \}_{1 \leq i \leq d}, \{ (\alpha_i - \alpha_j)^{-1} \}_{1 \leq i < j \leq 2g+1} \right] \), along with all subrings of invariants under finite groups of automorphisms, is integrally closed; in particular, \( \mathcal{O}_S := \mathbb{Z} \left[ \frac{1}{2}, \{ \alpha_i \}_{1 \leq i \leq d}, \{ (\alpha_i - \alpha_j)^{-1} \}_{1 \leq i < j \leq 2g+1} \right] \) is integrally closed.

For each \( n \geq 1 \), \cite[Proposition 20.7]{8} implies that the kernel of the multiplication-by-\( 2^n \) map on \( \mathfrak{f} \to S \), which we denote by \( \mathfrak{f}[2^n] \to S \), is a finite étale group scheme over \( S \). Since the morphism \( \mathfrak{f}[2^n] \to S \) is finite, \( \mathfrak{f}[2^n] \) is an affine scheme; we write \( \mathcal{O}_{S,n} \supset \mathcal{O}_S \) for the minimal extension of scalars under which \( \mathfrak{f}[2^n] \) becomes constant. It follows from the fact that \( \mathcal{O}_S \) is integrally closed and from the finite étaleness of \( \mathfrak{f}[2^n] \) that \( \mathcal{O}_{S,n} \) is also integrally closed; its fraction field coincides with \( K_0(J_0[2^n]) \).

Let \( \mathcal{O}_{S,\infty} \supset \mathcal{O}_S \) denote the integrally closed extension whose fraction field coincides with the maximal abelian subextension \((K\mathcal{Q}(\mu_2))^{\mathrm{ab}}\) of \((K\mathcal{Q})_{\infty}/(K\mathcal{Q})_1(\mu_2)\). Lemmas \ref{lem:gen} and \ref{lem:finite} together imply that \((K\mathcal{Q})_2(\mu_2) \subsetneq (K\mathcal{Q}(\mu_2))^{\mathrm{ab}} \subsetneq (K\mathcal{Q})_3(\mu_2)\); that the extension \((K\mathcal{Q}(\mu_2))^{\mathrm{ab}}/(K\mathcal{Q})_1(\mu_2)\) has Galois group isomorphic to \((\mathbb{Z}/2\mathbb{Z})^{2g^2-g} \times (\mathbb{Z}/4\mathbb{Z})^{2g}\); and that the analogous statements hold over each \( \mathbb{F}_p \). Thus it is clear that for each prime \( p \neq 2 \), the fraction field of \( \mathcal{O}_{S,\infty}^{\mathrm{ab}}/(p) \) coincides with the subfield of \((K\mathcal{F}_p)_3(\mu_2)\) fixed by the kernel of the map \( \pi : \Gamma(2)/\Gamma(8) \to (\mathbb{Z}/2\mathbb{Z})^{2g^2-g} \times (\mathbb{Z}/4\mathbb{Z})^{2g} \) induced by the abelianization map \( \pi \) and is therefore the maximal abelian subextension of \((K\mathcal{F}_p)_\infty/(K\mathcal{F}_p)_1(\mu_2)\). Moreover, if \( k \) is any field of characteristic \( p \neq 2 \), then it similarly follows from Lemmas \ref{lem:gen} and \ref{lem:finite} that \((K_k(\mu_2))^{\mathrm{ab}}\) coincides with the subfield of \((K\mathcal{F}_p)_3(\mu_2)\) fixed by the kernel of \( \pi \).

Note that \( k(\mu_2) \) contains \( \mathcal{F}_p \), where the prime subfield \( \mathcal{F}_p \) is \( K \) (resp. \( \mathbb{F}_p \)) if the characteristic of \( k \) is 0 (resp. \( p \geq 3 \)). It then follows from the linear disjointness of \( K_3(\mu_2) \) and \( \mathcal{F}_p \) over \( \mathbb{F}_p(\mu_2) \) given by Lemma \ref{lem:finite} (b) that the subfield of \( K_3(\mu_2) \) fixed by the kernel of \( \pi \) coincides with the compositum of \( K_1(\mu_2) \) with the subfield of \((K\mathcal{F}_p)_3(\mu_2)\) fixed by the kernel of \( \pi \). The extension \((K_k(\mu_2))^{\mathrm{ab}}\) is therefore generated over \( K_1(\mu_2) \) by the generators of \( \mathcal{O}_{S,\infty}^{\mathrm{ab}} \) over \( \mathcal{O}_{S,1}[\mu_2] \) (resp. by the images of these generators modulo \( (p) \) if \( k \) has characteristic 0 (resp. if \( k \) has characteristic \( p \geq 3 \)).

It remains to show that these generators are the same ones appearing in Theorem \ref{thm:main} for which we need another lemma.

**Lemma 4.3.** The fields \((K\mathcal{C})_n \) for \( n \geq 1 \), \((K\mathcal{C})_{\infty} \), and \((K\mathcal{C})^{\mathrm{ab}}_{\infty} \) coincide with the compositums of \( \mathcal{C} \) with \((K\mathcal{Q}(\mu_2))_n \), \((K\mathcal{Q}(\mu_2))_{\infty} \), and \((K\mathcal{Q}(\mu_2))^{\mathrm{ab}}_{\infty} \) respectively.

**Proof.** For \( n \geq 1 \), let \( \theta_n : \mathrm{Gal}((K\mathcal{C})_{\infty}/(K\mathcal{C})_n) \to \mathrm{Gal}((K\mathcal{Q})_{\infty}/(K\mathcal{Q})_n(\mu_2)) \) be the map given by the composition of the obvious inclusion map with the obvious restriction map. It is shown in the proof of \cite[Proposition 4.1]{15} that each \( \theta_n \) is an isomorphism (this can also be deduced from Lemma \ref{lem:finite} (a)). Since \( \theta_1 \) and \( \theta_3 \) are isomorphisms, they induce an isomorphism \( \Gamma(2)/\Gamma(8) \cong \mathrm{Gal}((K\mathcal{C})_3/(K\mathcal{C}))_1 \cong \mathrm{Gal}((K\mathcal{Q})_3(\mu_2)/(K\mathcal{Q})_1(\mu_2)) \), the image of whose restriction to \( \mathrm{Gal}((K\mathcal{Q}_3)/(K\mathcal{Q}))^{\mathrm{ab}}_\infty \) fixes the subfield \((K\mathcal{Q}_3)^{\mathrm{ab}}_\infty \). It follows from the definition of \( \theta_3 \) that \( K_\infty^{\mathrm{ab}} = \mathbb{C}(K\mathcal{Q}(\mu_2))^{\mathrm{ab}}_\infty \).

We now claim that \( \{ \gamma_{i,j} \}_{1 \leq i < j \leq 2g+1} \) is a set of generators for \( \mathcal{O}_{S,2}[\varsigma_8] \) over \( \mathcal{O}_{S,1}[\varsigma_8] \). Indeed, we see that \( (K\mathcal{C})_1(\{ \gamma_{i,j} \}_{1 \leq i < j \leq 2g+1}) = (K\mathcal{C})_2 = \mathbb{C}(K\mathcal{Q})_2 \) and

\[
\mathrm{Gal}((K\mathcal{Q})_2/(K\mathcal{Q})_1) \cong \tilde{\Gamma}(2)/\tilde{\Gamma}(4) = \Gamma(2)/\Gamma(4) \times \langle \iota \rangle \cong (\mathbb{Z}/2\mathbb{Z})^{2g^2+g}, \times \langle \iota \rangle
\]

using Lemma \ref{lem:finite} (a) and \( \iota \) and Lemma \ref{lem:gen}. It follows that \( \mathcal{O}_{S,2} \) is generated over \( \mathcal{O}_{S,1} \) by \( \varsigma_4 \) and the square roots of integral elements \( a_{i,j} \gamma_{i,j} \) for some \( a_{i,j} \in \mathbb{Z} \) for \( 1 \leq i < j \leq 2g + 1 \). Since the extension \( \mathcal{O}_{S,2} \) is unramified over \( \mathcal{O}_{S,1} \), we have \( a_{i,j} \in \{ \pm 1, \pm 2 \} \). But \( \pm 1, \pm 2 \in \mathbb{Z}[\varsigma_8] \subset \mathcal{O}_{S,1}[\varsigma_8] \), so we have \( \mathcal{O}_{S,2}[\varsigma_8] = \mathcal{O}_{S,1}[\varsigma_8, \{ \sqrt{\gamma_{i,j}} \}_{1 \leq i < j \leq 2g+1}] \), as claimed.

Next we find formulas for generators of \( \mathcal{O}_{S,\infty}^{\mathrm{ab}} \) over \( \mathcal{O}_{S,1}(\mu_2) \) using the ones we have shown for \( k = \mathcal{C} \). We know that \( \mathcal{O}_{S,\infty}^{\mathrm{ab}} \supset \mathcal{O}_{S,2}(\mu_2) = \mathcal{O}_{S,1}[\mu_2, \{ \sqrt{\gamma_{i,j}} \}_{1 \leq i < j \leq 2g+1}] \), and so, by Lemma \ref{lem:gen}, \( \mathcal{O}_{S,\infty}^{\mathrm{ab}} \) is generated over \( \mathcal{O}_{S,1}(\mu_2) \) by square roots of \( 2g \) independent integral elements. Then it is
clear from Lemma 1.3 that we may choose these $2g$ elements to be of the form $a_i \sqrt[\prod_{j \neq i} \gamma_{i,j}}$ for some $a_i \in \mathbb{Z}[[\mu_2]]$ for $1 \leq i \leq 2g$ and that the extension also contains a square root of $a_{2g+1} \sqrt[\prod_{j \neq 1} \gamma_{i,j} + 1}$ for some $a_{2g+1} \in \mathbb{Z}[[\mu_2]]$. Using the fact that $O_{S,\infty}^{ab}$ is Galois over $O_S[\mu_2]$, from conjugating by Galois automorphisms that fix $Q(\mu_2)$ but permute the $\alpha_i$’s, we see that we may choose the elements $a_1, ..., a_{2g+1}$ to be the same element $a \in \mathbb{Z}[[\mu_2]]$. Note that the product of these $2g+1$ elements $a \sqrt[\prod_{j \neq i} \gamma_{i,j}}$ can be written as $\pm a^{2g+1} \prod_{1 \leq i \leq j \leq 2g+1} \gamma_{i,j}$, and so this element must have a square root in $O_{S,\infty}^{ab}$. But we already know that $\pm \prod_{1 \leq i \leq j \leq 2g+1} \gamma_{i,j}$ has a square root in $O_{S,2}[\mu_2]$, so we have $\sqrt{a} \in O_{S,\infty}^{ab}$. Since $\sqrt{a}$ is algebraic over $Q(\mu_2)$, we get $\sqrt{a} \in Q(\mu_2)$ by Lemma 1.2(b).

It follows that $O_{S,\infty}^{ab}$ is generated over $O_{S,2}[\mu_2]$ by the elements $\sqrt[\prod_{j \neq i} \gamma_{i,j}}$. Therefore, the fraction field $(K(\mathbb{Q}(\mu_2)))_{ab}^{\infty}$ of $O_{S,\infty}^{ab}$ (resp. the fraction field $(K_{\mathbb{F}_p(\mu_2)})_{ab}^{\infty}$ of $O_{S,\infty}^{ab}/(p)$ for each prime $p \neq 2$) is generated over $(K(\mathbb{Q}(\mu_2)))_{2}$ (resp. $K_{\mathbb{F}_p(\mu_2))_{2}$) by the elements given in Theorem 1.1.

What we have shown above is that if any given field $k$, the statement of Theorem 1.1 holds over $k(\mu_2)$. It is now clear that $K(\mathbb{Q}(\mu_2)), \{\sqrt[\prod_{j \neq i} \gamma_{i,j}}\}_{1 \leq i \leq j \leq 2g+1}, \{\sqrt[\prod_{j \neq i} \gamma_{i,j}}\}_{1 \leq i \leq 2g+1} + 1\}$ is a subextension of $K(k(\mu_2)))_{\infty} = K(\mu_2) = K_{\infty}/K_1$. If $\zeta_k \in k$, then this subextension is clearly Kummer and therefore abelian, and it must be maximal abelian since there is no larger subextension which is abelian over $K(\mu_2)$. If $\zeta_k \notin k$, then $K_{\infty}^{ab}$ must be the largest subextension of $K(k(\mu_2)), \{\sqrt[\prod_{j \neq i} \gamma_{i,j}}\}_{1 \leq i \leq j \leq 2g+1}, \{\sqrt[\prod_{j \neq i} \gamma_{i,j}}\}_{1 \leq i \leq 2g+1} + 1\}$. Thus, the statement of Theorem 1.1(a) is proved over $k$.

Finally, let $\sigma \in G_K$ be an element such that $p_2(\sigma) = -1 \in GSp(T_2(J))$. Then it is clear from tracing through the above arguments that $\sigma$ acts on $O_{S,\infty}^{ab}$ by changing the signs of the generators $\sqrt[\prod_{j \neq i} \gamma_{i,j}}$ and by fixing (resp. changing the signs of) the remaining generators $\sqrt[\prod_{j \neq i} \gamma_{i,j}}$ if $g$ is even (resp. if $g$ is odd), and that therefore, it acts this way on $K_{\infty}^{ab}$, proving part (c) over $k$.

**References**

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

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

[3] Joan S. Birman. *Braids, links, and mapping class groups*. *Annals of Mathematical Studies*, (82), 1974.

[4] Armand Brumer and Kenneth Kramer. Large 2-adic galois image and non-existence of certain abelian surfaces over $Q$. *arXiv preprint arXiv:1701.01890*, 2017.

[5] Tim Dokchitser and Vladimir Dokchitser. Regulator constants and the parity conjecture. *Inventiones mathematicae*, 178(1):23, 2009.

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

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

[8] James S. Milne. Abelian varieties. In *Arithmetic geometry*, pages 103–150. Springer, 1986.

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

[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 and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, pages 492–517, 1968.

[13] Ascher Wagner. The faithful linear representation of least degree of $S_n$ and $A_n$ over a field of characteristic 2. *Mathematische Zeitschrift*, 151(2):127–137, 1976.

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

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

[16] Jeffrey Yelton. A note on 8-division fields of elliptic curves. *European Journal of Mathematics*, 3: 603, 2017.

[17] Jiu-Kang Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case. *Université Bordeaux I-A2X*, 351, 1996.