A NOTE ON 8-DIVISION FIELDS OF ELLIPTIC CURVES

JEFFREY YELTON

Abstract. Let $K$ be a field of characteristic different from 2 and let $E$ be an elliptic curve over $K$, defined either by an equation of the form $y^2 = f(x)$ with degree 3 or as the Jacobian of a curve defined by an equation of the form $y^2 = f(x)$ with degree 4. We obtain generators over $K$ of the 8-division field $K(E[8])$ of $E$ given as formulas in terms of the roots of the polynomial $f$, and we explicitly describe the action of a particular automorphism in Gal($K(E[8])/K$).

Let $K$ be any field of characteristic different from 2, and let $E$ be an elliptic curve over $K$. For any integer $N \geq 1$, we write $E[N]$ for the $N$-torsion subgroup of $E$ and $K(E[N])$ for the (finite algebraic) extension of $K$ obtained by adjoining the coordinates of the points in $E[N]$ to $K$. Let $T_2(E)$ denote the 2-adic Tate module of $E$; it is a free $\mathbb{Z}_2$-module of rank 2 given by the inverse limit of the finite groups $E[2^n]$ with respect to the multiplication-by-2 map. The absolute Galois group $G_K = \text{Gal}(\bar{K}/K)$ of $K$ acts in a natural way on each free rank-2 $\mathbb{Z}/2^n\mathbb{Z}$-module $E[2^n]$; we denote this action by $\rho_{2^n} : G_K \to \text{Aut}(E[2^n])$. This induces an action of $G_K$ on $T_2(E)$, which we denote by $\rho_2 : G_K \to \text{Aut}(T_2(E))$.

The purpose of this note is to provide formulas for generators of the 8-division field $K(E[8])$ of an elliptic curve $E$ and to describe how a certain Galois element in Gal($K(E[8])/K$) acts on these generators. We will consider the case where $E$ is given by a standard Weierstrass equation of the form $y^2 = \prod_{i=1}^{3}(x - \alpha_i) \in K[x]$ (the “degree-3 case”) and the case where $E$ is the Jacobian of the genus-1 curve given by an equation of the form $y^2 = \prod_{i=1}^{4}(x - \alpha_i) \in K[x]$ (the “degree-4 case”), where in both cases the elements $\alpha_i \in K$ are distinct.

For the statement of the main theorem and the rest of this article, we fix the following algebraic elements over $K$ (for ease of notation, we will treat indices $i$ as elements of $\mathbb{Z}/3\mathbb{Z}$). In the degree-3 case, for each $i \in \mathbb{Z}/3\mathbb{Z}$, we choose an element $A_i \in \bar{K}$ whose square is $\alpha_i + 1 - \alpha_{i+2}$. In the degree-4 case, for each $i \in \mathbb{Z}/3\mathbb{Z}$, we choose an element $A_i \in \bar{K}$ whose square is $(\alpha_i - \alpha_4)(\alpha_{i+1} - \alpha_{i+2})$. One checks that in either case, we have the identity

\begin{equation}
A_1^2 + A_2^2 + A_3^2 = 0,
\end{equation}

which we will exploit below.

In the degree-3 case, it is well known that $K(E[2]) = K(\alpha_1, \alpha_2, \alpha_3)$. Meanwhile, in the degree-4 case, the extension $K(E[2])/K$ is generated by polynomials in the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ which are fixed by the group of permutations in $S_4$ that fix all partitions of the roots into 2-element subsets. This follows from a well-known description of the 2-torsion points of the Jacobian of a hyperelliptic curve (see for instance the statement and proof of [7 Corollary 2.11]) which says that the points in $E[2]$ are parametrized by partitions of the set of roots $\{\alpha_i\}_{i=1}^{4}$ into even-cardinality subsets, and that $G_K$ acts on $E[2]$ via the Galois action on these partitions determined by permutation of the $\alpha_i$’s. In fact, it is clear (from examining, for instance, the solution to the “generic” quartic equation via the resolvent cubic) that $K(E[2])$ coincides with $K(\gamma_1, \gamma_2, \gamma_3)$, where $\gamma_i = (\alpha_i + 1 + \alpha_{i+2})(\alpha_i + \alpha_4)$ for $i \in \mathbb{Z}/3\mathbb{Z}$; note that $A_i^2 = \gamma_{i+1} - \gamma_{i+2}$ for each $i$. Thus, in either case, we have $A_1^2, A_2^2, A_3^2 \in K(E[2])$.

Now for each $i \in \mathbb{Z}/3\mathbb{Z}$, fix an element $B_i \in \bar{K}$ whose square is $A_i(A_i+1 + \zeta_4A_i+2)$. Let $\zeta_8 \in \bar{K}$ be a primitive 8th root of unity, and let $\zeta_4 = \zeta_8^2$, which is a primitive 4th root of unity. Our result is as follows.

**Theorem 1.** a) We have $K(E[4]) = K(E[2], \zeta_4, A_1, A_2, A_3)$ and $K(E[8]) = K(E[4], \zeta_8, B_1, B_2, B_3)$. 


b) If the scalar automorphism $-1 \in \text{Aut}(E[8])$ lies in the image under $\bar{\rho}_8$ of some Galois element $\sigma \in G_K$, then $\sigma$ acts on $K(E[8])$ by fixing $K(E[2], \zeta_8)$ and changing the sign of each generator $A_i, B_i \in \bar{K}$.

**Remark 2.** a) Rouse and Zureick-Brown have computed the full 2-adic Galois images of all elliptic curves over $\mathbb{Q}$ in [9]; in particular, their database can be used to find the image of $\bar{\rho}_8$ for any elliptic curve over $\mathbb{Q}$. Our result allows one to view these mod-8 Galois images somewhat more explicitly.

b) For certain elliptic curves, it is possible to determine using various methods that the image of $\rho_2$ contains $\Gamma(8)$. See [13] Example 4.3, which shows this for elliptic curves in Legendre form whose Weierstrass roots satisfy certain arithmetic conditions; e.g. $y^2 = x(x-1)(x-10)$. One can then use our result to determine the full 2-adic image in these cases.

The rest of this article is devoted to proving Theorem 1. We begin by justifying a simplifying assumption about the ground field $K$. From now on, the superscript “$S_d$” over a ring containing independent transcendental variables $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_d$ indicates the subring of elements fixed under all permutations of the variables $\tilde{\alpha}_i$.

**Lemma 3.** To prove Theorem 1 for the degree-$d$ case, it suffices to prove the statement when $K = \mathbb{C}(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_1)^{S_d}$ and the set of roots defining $E$ consists of the transcendental elements $\tilde{\alpha}_i \in \bar{K}$.

**Proof.** Assume that the statements of Theorem 1 are true in the degree-$d$ case when $K$ is $L := \mathbb{C}(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_1)^{S_d}$ and each root $\alpha_i$ is equal to $\tilde{\alpha}_i$.

**Step 1:** We show that the statements are true for $K = k((\tilde{\alpha}_1, \ldots, \tilde{\alpha}_1)^{S_d}$, where $k$ is any subfield of $\mathbb{C}$. Due to the Galois equivariance of the Weil pairing, we have $\zeta_4 \in K(E[4])$ and $\zeta_8 \in K(E[8])$. We will therefore assume that $\zeta_8 \in k$, so that the image of $\text{Gal}(\bar{K}/K)$ under $\rho_2$ modulo 4 (resp. modulo 8) is contained in the group $\text{SL}(E[4])$ (resp. $\text{SL}(E[8])$) of automorphisms of determinant 1. For any $n \geq 1$, write

$$\phi_{2^n} : \text{Gal}(K(E[2^n])/K) \hookrightarrow \text{SL}(E[2^n])$$

for the obvious injection induced by $\rho_2$, and define $\phi_{2^n, \rho} : \text{Gal}(L(E[2^n])/L) \hookrightarrow \text{SL}(E[2^n])$ analogously. From the formulas given in Theorem 1 and elementary computations of the orders of the (finite) groups above for $n \in \{2, 3\}$, we see that $\phi_{4, \rho}$ and $\phi_{8, \rho}$ are isomorphisms. Now let

$$\theta_{2^n} : \text{Gal}(L(E[2^n])/L) \rightarrow \text{Gal}(K(E[2^n])/K)$$

be the composition of the natural inclusion $\text{Gal}(L(E[2^n])/L) \hookrightarrow \text{Gal}(L(E[2^n])/K)$ with the natural restriction map $\text{Gal}(L(E[2^n])/K) \rightarrow \text{Gal}(K(E[2^n])/K)$. Note that the automorphism in $\text{Gal}(L(E[8])/L(E[2]))$ which changes the sign of each generator given in Theorem 1 is sent by $\theta_8$ to the automorphism in $\text{Gal}(K(E[8])/K)$ which changes the sign of each of these generators.

It is clear that $\phi_{2^n, \rho} = \phi_{2^n} \circ \theta_{2^n}$. It will therefore suffice to show that $\theta_8$ and $\theta_3$ are isomorphisms. Indeed, they are injections due to the fact that $L(E[2^n])$ is the compositum of the subfields $K(E[2^n])$ and $\mathbb{C}$ for each $n \geq 1$, and the fact that they are surjections in the case of $n \in \{2, 3\}$ follows immediately from the surjectivity of $\phi_{4, \rho}$ and $\phi_{8, \rho}$.

**Step 2:** We show that the statements are true for $K = \mathbb{F}_p((\tilde{\alpha}_1, \ldots, \tilde{\alpha}_1)^{S_d}$, where $p \neq 2$. Let $E_0$ be the elliptic curve defined in the obvious way over $K_0 := \mathbb{Q}((\tilde{\alpha}_1, \ldots, \tilde{\alpha}_1)^{S_d}$ in the degree-$d$ case. By what was shown in Step 1, the statement of Theorem 1 is true for $E_0$. It is easy to see that $E_0$ admits a model $\mathcal{E}$ over

$$S := \text{Spec}(\mathbb{Z}[\frac{1}{2}, (\tilde{\alpha}_i)_{i=1}^d, ((\tilde{\alpha}_i - \tilde{\alpha}_j)^{-1})_{1 \leq i < j \leq d}]^{S_d})$$

which is an abelian scheme whose fiber over the prime $(p)$ is isomorphic to $E$. For each $n \geq 1$, Proposition 20.7 of [3] implies that the kernel of the multiplication-by-2 map on $\mathcal{E} \rightarrow S$, which we denote by $\mathcal{E}[2^n] \rightarrow S$, is a finite étale group scheme over $S$. Since the morphism $\mathcal{E}[2^n] \rightarrow S$ is finite, $\mathcal{E}[2^n]$ is an affine scheme; we write $\mathcal{O}_{S,2^n} \supset \mathcal{O}_S$ for the minimal extension of scalars under which $\mathcal{E}[2^n]$ becomes constant. Note that the ring $\mathbb{Z}[\frac{1}{2}, (\tilde{\alpha}_i)_{i=1}^d, ((\tilde{\alpha}_i - \tilde{\alpha}_j)^{-1})_{1 \leq i < j \leq d}]$, along with
Lemma 4. In the degree-d case, we have an isomorphism \( G_K^\text{unr} \cong \hat{B}_d \).

b) The map \( \rho_2 : G_K \to \text{SL}(T_2(E)) \) is surjective and factors through the obvious restriction map
\[
G_K \to G_K^\text{unr} \cong \hat{B}_d, \text{ inducing a surjection } \rho_2^\text{unr} : \hat{B}_d \to \text{SL}(T_2(E)).
\]
c) For each $n \geq 0$, the algebraic extension $K(E[2^n])/K$ is a subextension of $K^\text{unr}/K$ and corresponds to the normal subgroup $(\rho_2^\text{unr})^{-1}(\Gamma(2^n)) \triangleleft \hat{B}_d$.

d) The normal subgroup $(\rho_2^\text{unr})^{-1}(\Gamma(2)) \triangleleft \hat{B}_d$ coincides with $\hat{P}_3 \triangleleft \hat{B}_3$ in the degree-3 case, and it coincides with a subgroup $H \triangleleft \hat{B}_4$ which strictly contains $\hat{P}_4 \triangleleft \hat{B}_3$ and which is isomorphic to $\hat{P}_3$ in the degree-4 case.

Proof. Let $X_d$ denote the affine scheme $\text{Spec}(\mathbb{C}[\{\alpha_i\}_{i=1}^d]/\Delta)$, where $\Delta$ is the discriminant locus. It is clear from definitions that $G_K^\text{unr}$ can be identified with the étale fundamental group of $X_d$. Since $X_d$ is a complex scheme, it may also be viewed as a complex manifold, and so we may use Riemann’s Existence Theorem ([4], Exposé XII, Corollaire 5.2) to identify its étale fundamental group with the profinite completion of the fundamental group of the topological space $X_d$. Now $X_d$ is the configuration space of (unordered) $d$-element subsets of $\mathbb{C}$, and it is well known that the fundamental group of $X_d$ is isomorphic to the braid group $B_d$. Hence, $G_K^\text{unr} \cong \hat{B}_d$, and part (a) is proved. It is also well known that the cover of $X_d$ corresponding to the normal subgroup $P_d \triangleleft B_d$ is given by the ordered configuration space $Y_d := \text{Spec}(\mathbb{C}[\{\alpha_i\}_{i=1}^d, \{(\alpha_i - \alpha_j)^{-1}\}_{1 \leq i < j \leq d}])$ with its obvious map onto $X_d$.

To prove (b), we first note that $\rho_2$ is surjective because it is known that there exist elliptic curves with “largest possible” 2-adic Galois images; see also [12 Corollary 1.2(b)]. Now choose any prime $\mathfrak{p}$ of the coordinate ring of $X_d$ and note that $E$ has good reduction with respect to this prime. It follows from the criterion of Néron-Ogg-Shafarevich ([11 Theorem 1]) that the action $\rho_2$ is unramified with respect to $\mathfrak{p}$ and therefore factors through an algebraic extension of $K((\alpha_i)_{i=1}^d)$ which is unramified over $\mathfrak{p}$. The second claim of (b) follows.

Part (c) is immediate from the observation that the action $\bar{\rho}_2^n : G_K \to \text{Aut}(E[2^n])$ is clearly the composition of $\rho_2$ with the quotient-by-$\Gamma(2^n)$ map.

Finally, we investigate the subgroup $(\rho_2^\text{unr})^{-1}(\Gamma(2)) \triangleleft \hat{B}_d$. In the degree-3 case, we get $(\rho_2^\text{unr})^{-1}(\Gamma(2)) = \hat{P}_3 \triangleleft \hat{B}_3$ from the fact that $K(E[2]) = K(\alpha_1, \alpha_2, \alpha_3)$, which is the function field of the ordered configuration space $Y_3$ as defined above. In the degree-4 case, we have seen that $K(E[2]) = K(\gamma_1, \gamma_2, \gamma_3) \subseteq K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, which is the function field of $Y_4$. Therefore, we have $H := (\rho_2^\text{unr})^{-1}(\Gamma(2)) \triangleleft \hat{P}_4 \triangleleft \hat{B}_4$. It is easy to check that the $\gamma_i$’s are independent and transcendental over $\mathbb{C}$, so that $K(E[2])$ and the function field of $Y_3$ are isomorphic as abstract $\mathbb{C}$-algebras. Thus, $H \cong \hat{P}_3$, and (d) is proved.

We now present several well-known group-theoretic facts which will be needed later.

**Lemma 5.**

a) The centers of $B_d$ and $P_d$ are both generated by $\Sigma := (\beta_1 \beta_2 \ldots \beta_{d-1})^d \in P_d \triangleleft B_d$; this element can be written as an ordered product of 1st powers of all the generators $A_{i,j}$ in the presentation for $P_d$ given in [2, Lemma 1.8.2].

b) The abelianization of $P_d$ is isomorphic to $\mathbb{Z}^{d(d-1)/2}$. More explicitly, it is freely generated by the images of the above generators $A_{i,j}$.

c) For each $n \geq 1$, the quotient $\Gamma(2^n)/\Gamma(2^{n+1})$ is an elementary abelian group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$.

**Proof.** The statement of (a) can be found in [2, Corollary 1.8.4] and its proof. Part (b) can be deduced directly from the presentation of $P_d$ mentioned above. Part (c) can be seen easily from direct computations and is a special case of what is shown in the proof of [10 Corollary 2.2].

It is now easy to determine the 4-division field of $E$ in both cases and to describe how $G_K$ acts on it. We note that in the degree-3 case, parts (a) and (b) are well known and can be deduced by straightforward calculations of order-4 points (for instance, in [1 Example 2.2]; see also [12 Proposition 3.1]).
Proposition 6. a) We have $K(E[4]) = K(E[2], A_1, A_2, A_3)$.

b) Any Galois element $\sigma \in G_K$ with $\rho_2(\sigma) = -1 \in \text{SL}(T_2(E))$ acts on $K(E[4])$ by fixing $K(E[2])$ and changing the signs of each generator $A_i$ in $K$.

c) In the degree-3 case, the scalar automorphism $-1 \in \text{SL}(T_2(E))$ is the image of the braid $\Sigma \in \hat{P}_3$ under $\rho_2^{\text{unr}}$. In the degree-4 case, the scalar $-1 \in \text{SL}(T_2(E))$ is the image of the braid $\Sigma \in \hat{P}_3 \cong H$, where $H \triangleleft \hat{B}_4$ is the subgroup from the statement of Lemma 4(c).

Proof. Consider the composition of the restriction $\rho_2^{\text{unr}} : (\rho_2^{\text{unr}})^{-1}(\Gamma(2)) \to \Gamma(2)$ with the quotient map $\Gamma(2) \to \Gamma(2)/\Gamma(4)$. Since $\Gamma(2)/\Gamma(4)$ is an abelian group of exponent 2 by Lemma 3(c), this composition must factor through the maximal exponent-2 abelian quotient $K$ with $\text{Gal}(\Gamma(2)/\Gamma(4) \cong \hat{P}_3)$. We denote this induced surjection by $R : P_3^{\text{ab}}/2P_3^{\text{ab}} \to \Gamma(2)/\Gamma(4)$. It follows from parts (b) and (c) of Lemma 3 that both $P_3^{\text{ab}}/2P_3^{\text{ab}}$ and $\Gamma(2)/\Gamma(4)$ are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, and so $R$ is an isomorphism. Thus, $K(E[4])$ is the unique subextension of $K^{\text{unr}}/K(E[2])$ with $\text{Gal}(K(E[4])/(K(E[2]))) \cong (\mathbb{Z}/2\mathbb{Z})^3$. It is easy to check that in both cases, $K(E[2], A_1, A_2, A_3)$ is such a subextension, and so $K(E[4]) = K(E[2], A_1, A_2, A_3)$, proving (a).

Part (b) follows from checking that the automorphism of $K(E[4])$ defined by changing the signs of all the $A_i$’s is the only nontrivial automorphism lying in the center of $\text{Gal}(K(E[2], A_1, A_2, A_3)/K)$.

Now it follows from (a) and (b) of Lemma 3 that $\Sigma$ has nontrivial image in $P_3^{\text{ab}}/2P_3^{\text{ab}}$. It therefore has nontrivial image in $\Gamma(2)/\Gamma(4)$, so $\rho_2^{\text{unr}}(\Sigma)$ is a nontrivial element of $\text{SL}(T_2(E))$. We know from Lemma 3(a) that $\Sigma$ lies in the center of $\hat{P}_3$. It follows from Lemma 4(d) that $\rho_2^{\text{unr}}$ restricted to $(\rho_2^{\text{unr}})^{-1}(\Gamma(2)) \cong \hat{P}_3$ is surjective onto $\Gamma(2) \triangleleft \text{SL}(T_2(E))$, so it takes the center of $\hat{P}_3$ to the center of $\Gamma(2)$, which is $\{\pm 1\}$. We therefore get $\rho_2(\sigma) = -1 \in \Gamma(2)$, which is the statement of (c).

We now want to find generators for the extension $K(E[8])/K(E[2])$. In order to do so, we will first prove that $\hat{P}_3$ has a unique quotient isomorphic to $\Gamma(2)/\Gamma(8)$ (Lemma 5 below), and then we will show that the extension of $K(E[2])$ given in the statement of Theorem 4 has Galois group isomorphic to $\Gamma(2)/\Gamma(8)$ (Lemma 6 below). For the following, we note that after fixing a basis of the free rank-2 $\mathbb{Z}_2$-module $T_2(E)$, we may consider $\text{SL}(T_2(E))$ as the matrix group $\text{SL}_2(\mathbb{Z}_2)$. Moreover, by applying a suitable form of the Strong Approximation Theorem (see for instance Theorem 7.12 of [8]), we have $\Gamma(2)/\Gamma(8) \cong (\Gamma(2) \cap \text{SL}_2(\mathbb{Z}))/\Gamma(8) \cap \text{SL}_2(\mathbb{Z}))$. In light of this, in the proofs of the next two lemmas, we use the symbols $\Gamma(2)$ and $\Gamma(8)$ to denote principal congruence subgroups of $\text{SL}_2(\mathbb{Z})$ rather than of $\text{SL}_2(\mathbb{Z}_2) \cong \text{SL}(T_2(E))$.

Lemma 7. The group $\Gamma(2)$ decomposes into a direct product of the scalar subgroup $\{\pm 1\}$ with another subgroup $\Gamma(2)'$. The quotient $\Gamma(2)/\Gamma(8)$ can be presented as

(3) \[ \langle \sigma, \tau | \sigma^4 = \tau^4 = [\sigma^2, \tau] = [\sigma, \tau^2] = [\sigma, \tau]^2 = [[\sigma, \tau], \sigma] = [[\sigma, \tau], \tau] = 1 \rangle. \]

Proof. Let $\Gamma(2)'$ be the subgroup consisting of matrices in $\Gamma(2)$ whose diagonal entries are equivalent to 1 modulo 4. Then it is straightforward to check that $\Gamma(2) = \{\pm 1\} \times \Gamma(2)'$. We note that by Lemma 5(c), the order of $\Gamma(2)/\Gamma(8)$ is 64, and so since $-1 \notin \Gamma(8)$, the order of $\Gamma(2)/\Gamma(8)$ is 32.

Let $\sigma$ (resp. $\tau$) be the image of $\tilde{\sigma} := \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$ (resp. $\tilde{\tau} := \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$) in $\Gamma(2)/\Gamma(8)$. It is well known that $\tilde{\sigma}$ and $\tilde{\tau}$ generate $\Gamma(2)' \cap \text{SL}_2(\mathbb{Z})$ (see, for instance, Proposition A.1 of [9]), so $\sigma$ and $\tau$ generate $\Gamma(2)/\Gamma(8)$. It is then straightforward to check that the relations given in (3) hold. To show that these relations determine the group $\Gamma(2)/\Gamma(8)$, one checks that the only nontrivial element of the commutator subgroup of the group given by (3) has order 2 and that the quotient by the commutator subgroup is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; therefore, the group has order 32. Since $\Gamma(2)/\Gamma(8)$ also has order 32, it must be fully determined by the relations in (3).
Lemma 8. The only normal subgroup of $\tilde{P}_3$ which induces a quotient isomorphic to $\Gamma(2)/\Gamma(8)$ is $(\rho_2^{\text{unr}})^{-1}(\Gamma(8)) < (\rho_2^{\text{unr}})^{-1}(\Gamma(2)) \cong \tilde{P}_3$.

Proof. Since $\tilde{P}_3$ and $P_3$ have the same finite quotients, it suffices to show that the only normal subgroup of $P_3$ inducing a quotient isomorphic to $\Gamma(2)/\Gamma(8)$ coincides with $(\rho_2^{\text{unr}})^{-1}(\Gamma(8)) \cap P_3$. Let $N < P_3$ be a normal subgroup whose corresponding quotient is isomorphic to $\Gamma(2)/\Gamma(8)$. By Lemma 5(a), the braid $\Sigma$ generates the center of $P_3$; therefore, its image modulo $N$ must lie in the center of $P_3/N \cong \Gamma(2)/\Gamma(8)$. It can easily be deduced from Lemma 7 that the center of $\Gamma(2)/\Gamma(8)$ is an elementary abelian 2-group, so the image of $\Sigma$ modulo $N$ must have order dividing 2. We claim that $\Sigma \notin N$. Indeed, if $\Sigma \in N$, then $P_3/N$ could be generated by the images of only 2 of the generators of $P_3$ given above. But it is clear from Lemma 7 that $\Gamma(2)/\Gamma(8) = \{ \pm 1 \} \times \Gamma(2)/\Gamma(8)$ cannot be generated by only 2 elements, a contradiction. Therefore, the image of $\Sigma$ modulo $N$ has order 2, so $\Sigma^2 \in N$ and the quotient map factors through $P_3/\langle \Sigma^2 \rangle$. But the discussion in §3.6.4 shows that $P_3/\langle \Sigma^2 \rangle \cong \Gamma(2)<\text{SL}_2(\mathbb{Z})$. We claim that in fact, the kernel of $\rho_2^{\text{unr}}$ coincides with $\langle \Sigma^2 \rangle$, so that the quotient-by-$N$ map factors through $\rho_2^{\text{unr}} : P_3 \to \Gamma(2)$. Since $\rho_2^{\text{unr}}(\Sigma) = -1 \in \text{SL}_2(\mathbb{Z}_2)$ by (b) and (c) of Proposition 6, we know that the kernel of $\rho_2^{\text{unr}}$ contains $\langle \Sigma^2 \rangle$, and to prove the claim we need to show that $\Gamma(2)$ has no proper quotient isomorphic to itself. But this follows from the fact that $\Gamma(2)$ is finitely generated and is residually finite, so the claim holds. Therefore, to prove the statement of the lemma, it suffices to show that $\Gamma(8)$ is the only normal subgroup of $\Gamma(2)$ which induces a quotient isomorphic to $\Gamma(2)/\Gamma(8)$.

Any surjection $\Gamma(2) \to \Gamma(2)/\Gamma(8)$ takes $-1 \in \Gamma(2)$ to a nontrivial element $\mu \in \Gamma(2)/\Gamma(8)$ and takes $\Gamma(2)'$ to some proper subgroup of $\Gamma(2)/\Gamma(8)$ not containing $\mu$, since $\Gamma(2)'$ can be generated by only 2 elements while $\Gamma(2)/\Gamma(8)$ cannot. Therefore, such a surjection takes $\Gamma(2)'$ to a subgroup of $\Gamma(2)/\Gamma(8)$ isomorphic to $\Gamma(2)'/\Gamma(8)$. So in fact it suffices to show that $\Gamma(8)$ is the only normal subgroup of $\Gamma(2)'$ which induces a quotient isomorphic to $\Gamma(2)'/\Gamma(8)$.

Let $N < \Gamma(2)'$ be a normal subgroup such that $\Gamma(2)'/N \cong \Gamma(2)/\Gamma(8)$. Let $\tilde{\sigma}$ and $\tilde{\tau}$ be the matrices given in the proof of Lemma 7 and let $\phi_{N'} : \Gamma(2)' \to \Gamma(2)'/N'$ be the obvious quotient map. One checks from the presentation given in the statement of Lemma 7 that each element of $\Gamma(2)'/N'$ has order dividing 4; that each square element lies in the center; and that each commutator has order dividing 2 and lies in the center. It follows that $\phi_{N'}(\tilde{\sigma}^4) = \phi_{N'}(\tilde{\tau}^4) = \phi_{N'}((\tilde{\sigma}^2, \tilde{\tau})) = \phi_{N'}(\tilde{\sigma}, \tilde{\tau})^2 = \phi_{N'}((\tilde{\sigma}, \tilde{\tau})) = \phi_{N'}([\tilde{\sigma}, [\tilde{\sigma}, \tilde{\tau}]], [\tilde{\sigma}, \tilde{\tau}]) = 1$. Thus, $N'$ contains the subgroup normally generated by $\{ \tilde{\sigma}^2, \tilde{\tau}, [\tilde{\sigma}, \tilde{\tau}], [\tilde{\sigma}, \tilde{\tau}]^2, [[\tilde{\sigma}, \tilde{\tau}], \tilde{\sigma}], [[\tilde{\sigma}, \tilde{\tau}], \tilde{\tau}] \}$. But Lemma 7 implies that $\Gamma(8) < \Gamma(2)'$ is normally generated by this subset, so $\Gamma(8) \trianglelefteq N'$. Since $\Gamma(2)'/N'$ and $\Gamma(2)'/\Gamma(8)$ have the same (finite) order, we have $N' = \Gamma(8)$, as desired.

Lemma 9. The Galois group $\text{Gal}(K(E[2], A_1, A_2, A_3, B_1, B_2, B_3)/K(E[2]))$ is isomorphic to $\Gamma(2)/\Gamma(8)$.

Proof. Let $K' = K(E[2], A_1, A_2, A_3, B_1, B_2, B_3)$. Clearly $K'$ is generated over $K(E[4])$ by square roots of three elements which are independent in $K(E[4])^\times/(K(E[4])^\times)^2$, and thus, $[K' : K(E[4])] = 8$. Therefore, since $[K(E[4]) : K(E[2])] = 8$, we have $[K' : K(E[2])] = 64$.

Using the relation (1), for each $i$, we compute

$$A_i(A_i+1 + \zeta_4A_{i+2}))(A_i(A_i+1 - \zeta_4A_{i+2})) = -A_i^4.$$

In light of this, for $i \in \mathbb{Z}/3\mathbb{Z}$, we define $B_i'$ to be the element of $K'$ such that $B_i'^2 = A_i(A_i+1 - \zeta_4A_{i+2})$ and $B_iB_i' = \zeta_4A_i^2 \in K(E[2])$. Define $\sigma \in \text{Gal}(K'/K(E[2]))$ as the automorphism which acts by

$$\sigma : (A_1, A_2, A_3, B_1, B_2, B_3) \mapsto (A_1, A_2, -A_3, B_1', \zeta_4B_2', \zeta_4B_3),$$

and let $\tau \in \text{Gal}(K'/K(E[2]))$ be the automorphism which acts by

$$\tau : (A_1, A_2, A_3, B_1, B_2, B_3) \mapsto (-A_1, A_2, A_3, \zeta_4B_1, B_2', \zeta_4B_3).$$
Note that $\sigma^2$ and $\tau^2$ both act trivially on $K(E[4])$ while sending $(B_1, B_2, B_3)$ to $(B_1, B_2, -B_3)$ and to $(-B_1, B_2, B_3)$ respectively; it is now easy to check that $\sigma^2$ (resp. $\tau^2$) has order 2 and commutes with $\tau$ (resp. $\sigma$). One also verifies that $[\sigma, \tau]$ acts trivially on $K(E[4])$ and sends $(B_1, B_2, B_3)$ to $(-B_1, -B_2, -B_3)$, and that this automorphism also commutes with both $\sigma$ and $\tau$. Thus, $\sigma$ and $\tau$ satisfy all of the relations given in (3). Moreover, $\sigma$ and $\tau$ each have order 4, while $[\sigma, \tau]$ has order 2. It is elementary to verify that this implies that $(\sigma, \tau)$ has order 32, which is the order of $\Gamma(2)/\Gamma(8)$; therefore $(\sigma, \tau) \cong \Gamma(2)/\Gamma(8)$. Note also that $(\sigma, \tau)$ fixes $A_2$, whose orbit under $\text{Gal}(K/K(E[2]))$ has cardinality 2, so if $\mu$ is any automorphism in $\text{Gal}(K'/K(E[2]))$ which does not fix $A_2$, then $(\sigma, \tau, \mu)$ has order 64 and must be all of $\text{Gal}(K'/K(E[2]))$. Let $\mu$ be the automorphism that acts by changing the sign of all $A_i$'s and all $B_i$'s. Then $\mu$ commutes with $\sigma$ and $\tau$, and

$$ (5) \quad \text{Gal}(K'/K(E[2])) = \langle \sigma, \tau \rangle \times \langle \mu \rangle \cong \Gamma(2)/\Gamma(8) \times \{\pm 1\} \cong \Gamma(2)/\Gamma(8). $$

The next two propositions (Propositions 10 and 12 below) imply Theorem 1.

**Proposition 10.** We have $K(E[8]) = K(E[2], A_1, A_2, A_3, B_1, B_2, B_3)$.

**Proof.** As before, write $K'$ for $K(E[2], A_1, A_2, A_3, B_1, B_2, B_3)$. It is straightforward to check by computing norms that the field extension $K'/K(E[2])$ obtained by adjoining the $A_i$'s and $B_i$'s is unramified away from the discriminant locus (the union of the primes $(\alpha_i - \alpha_j)$) and thus, $K'$ is a subextension of $K^{\text{unr}}/K$. Lemma 4(d) tells us that $\text{Gal}(K^{\text{unr}}/K(E[2])) \cong \hat{P}_3$, so the subextension $K'$ corresponds to some normal subgroup of $\hat{P}_3$ inducing a quotient isomorphic to $\text{Gal}(K'/K(E[2])) \cong \Gamma(2)/\Gamma(8)$. Lemma 5 then implies that this normal subgroup of $\hat{P}_3$ is the one corresponding to $(\rho_2^{\text{unr}})^{-1}(\Gamma(8)) \lhd \hat{P}_3$. But Lemma 4(c) says that the subextension corresponding to $(\rho_2^{\text{unr}})^{-1}(\Gamma(8))$ is $K(E[8])$. Therefore, $K' = K(E[8])$, as desired.

**Remark 11.** We may now use Proposition 10 to compute several elements that lie in $K(E[8])$.

a) We first compute, for $i \in \mathbb{Z}/3\mathbb{Z}$ (and with $B_i'$ defined as in the proof of Lemma 9), that

$$ (6) \quad (B_i \pm B_i')^2 = 2A_iA_{i+1} \pm 2\zeta_8A_i^2; \quad (B_i \pm \zeta_4B_i')^2 = 2\zeta_4A_iA_{i+2} \mp 2A_i^2. $$

Therefore, for each $i$, we have (up to sign changes)

$$ \sqrt{-A_i^2 \pm \zeta_4A_iA_{i+1}} = (1 \mp \zeta_4)^{-1}(B_i \pm B_i'), \quad \sqrt{\zeta_4A_iA_{i+2} \pm A_i^2} = (\zeta_8 + \zeta_8^{-1})^{-1}(B_i \mp \zeta_4B_i') \in K(E[8]). $$

b) We similarly compute, for $i \in \mathbb{Z}/3\mathbb{Z}$, that

$$ 2^{-1}\zeta_4(B_i - B_i')^2B_{i+2}^2/(A_i \pm \zeta_4A_{i+1})^2 = (A_i(A_i + \zeta_4A_{i+1}))(A_{i+2}(A_i + \zeta_4A_{i+1}))/((A_i + \zeta_4A_{i+1})^2

$$

$$ = A_iA_{i+2}(A_i + \zeta_4A_{i+1})^2/((A_i + \zeta_4A_{i+1})^2 = A_iA_{i+2}. $$

Therefore, for each $i$, we have $\pm\sqrt{A_iA_{i+2}} = \pm(1 - \zeta_4)^{-1}(B_i - B_i')B_{i+2}/(A_i + \zeta_4A_{i+1}) \in K(E[8]).$

**Proposition 12.** Any Galois element $\sigma \in G_K$ with $p_2(\sigma) = -1 \in \text{SL}(T_2(E))$ acts on $K(E[8])$ by changing the sign of each of the generators $A_i, B_i \in K$.

**Proof.** Let $\sigma \in G_K$ be an automorphism which acts on $K(E[8])$ by changing the sign of each generator $A_i, B_i \in K$. Then it follows from Proposition 6(b) that $\hat{\sigma}(\sigma)$ is the scalar $-1 \in \text{SL}(E[4])$. Moreover, we observe that the restriction of $\sigma$ to $K(E[8])$ lies in the center of $\text{Gal}(K(E[8])/K)$, so $\hat{\sigma}(\sigma)$ is a scalar automorphism in $\text{SL}(E[8])$, either $-1$ or $3$. In order to determine which scalar it is, we first treat the degree-3 case and compute a point of order 8 in $E(\hat{K})$. To simplify computations, we instead work with the elliptic curve $E'$ defined by $y^2 = x(x - (\alpha_2 - \alpha_1))(x - (\alpha_3 - \alpha_1))$, which is isomorphic to $E$ over $K(E[2])$ via the morphism $(x, y) \mapsto (x - \alpha_1, y)$. (We note that replacing...
the roots \(\alpha_i\) with the new roots \(\alpha'_i := \alpha_i - \alpha_1\) in the formulas for \(A_i, B_i \in \bar{K}\) does not change the elements \(A_i, B_i \in \bar{K}\).

Given a point \((x_0, y_0) \in E(\bar{K})\), in [1, \S2], Bekker and Zarhin describe an algorithm to find a point \(P \in E(\bar{K})\) with \(2P = (x_0, y_0)\). In order to find such a point, one chooses elements \(r_1, r_2, r_3 \in \bar{K}\) with \(r_i^2 = x_0 - \alpha_i\) for \(i = 1, 2, 3\) and with \(r_1^2 r_2 r_3 = -y_0\). Then

\[
P := (x_0 + (r_1 r_2 + r_2 r_3 + r_3 r_1), -y_0 + (r_1 + r_2 + r_3)(r_1 r_2 + r_2 r_3 + r_3 r_1))
\]
satisfies \(2P = (x_0, y_0)\). Following this algorithm, we get a point \(P\) of order 4 with \(2P = (0, 0)\) given by

\[
P := (\zeta_4 A_2 A_3, \zeta_4 A_2 A_3 (A_2 + \zeta_4 A_3)).
\]

Similarly, we get a point \(Q\) of order 8 with \(2Q = P\) given by

\[
Q = (\zeta_4 A_2 A_3 + (r_1 r_2 + r_2 r_3 + r_3 r_1), -\zeta_4 A_2 A_3 (A_2 + \zeta_4 A_3) + (r_1 + r_2 + r_3)(r_1 r_2 + r_2 r_3 + r_3 r_1)),
\]

where \(r_1, r_2, r_3 \in \bar{K}\) are elements satisfying

\[
r_1^2 = \zeta_4 A_2 A_3 - \alpha'_1 = \zeta_4 A_2 A_3; \quad r_2^2 = \zeta_4 A_2 A_3 - \alpha'_2 = \zeta_4 A_2 A_3 + A_3^2; \quad r_3^2 = \zeta_4 A_2 A_3 - \alpha'_3 = \zeta_4 A_2 A_3 - A_3^2.
\]

and \(r_1 r_2 r_3 = -\zeta_4 A_2 A_3 (A_2 + \zeta_4 A_3)\). Using the formulas computed in Remark [11] we see that one may choose

\[
r_1 \in \{\pm(\zeta_8 - \zeta_8^{-1})^{-1}(B_3 - B_3')B_2/(A_3 + \zeta_4 A_1)\}, \quad r_2 \in \{\pm(\zeta_8 + \zeta_8^{-1})^{-1}(B_3 - \zeta_4 B_3')\}, \quad r_3 \in \{\pm(1 - \zeta_4)^{-1}(B_2 + B_2')\}
\]

with \(r_1^2 r_2 r_3\) as specified above. It follows that the \(x\)-coordinate (resp. the \(y\)-coordinate) of \(Q\) can be written as a quotient of homogeneous polynomial functions in the \(A_i'\)'s, \(B_i'\)'s, and \(B_i''\)'s with coefficients in \(K\) whose degree (the degree of the numerator minus the degree of the denominator) is 2 (resp. 3). Therefore, since \(\sigma\) changes the sign of each \(B_i'\) as well as each of the \(A_i'\)'s and \(B_i''\)'s, we see that \(\sigma\) fixes the \(x\)-coordinate of \(Q\) while changing the sign of the \(y\)-coordinate, so \(\sigma(Q) = -Q\). Thus, \(\rho_2(\sigma) = -1 \in \text{SL}(T_2(E))\), and we have proven the statement of the proposition for the degree-3 case. In particular, we see from Proposition [6, c] that if we choose \(\sigma \in G_K\) to be an automorphism whose image under the restriction map to \(G^K_{\text{unr}} \cong \hat{P}_3\) is the central element \(\Sigma \in \hat{P}_3\), then \(\sigma\) acts on \(K(E[8])\) by changing the sign of each of the \(A_i'\)'s and \(B_i''\)'s.

In the degree-4 case, similarly let \(\sigma \in \text{Gal}(\bar{K}/K(E[2]))\) be an automorphism whose image under the restriction map to \(\text{Gal}(K^{\text{unr}}/K(E[2])) \cong \hat{P}_3\) is the central element \(\Sigma \in \hat{P}_3\) as defined in the statement of Lemma [5, a]. Then it follows from what was remarked at the end of the last paragraph that \(\sigma\) again acts on \(K(E[8])\) by changing the sign of each of the \(A_i'\)'s and \(B_i''\)'s, so to prove the theorem for this case it suffices to show that \(\rho_2(\sigma) = -1 \in \text{SL}(T_2(E))\). But this is given by Proposition [6, c].

\[\square\]

The author is grateful to Yuri Zarhin for his guidance in supervising the author’s investigation of 8-torsion of elliptic curves during his time at The Pennsylvania State University. The author would also like to thank the referee for pointing out a gap in an earlier version of this work.

**References**

[1] Boris M. Bekker and Yuri G. Zarhin. The divisibility by 2 of rational points on elliptic curves. arXiv preprint arXiv:1702.02255, 2017.

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

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

[4] Alexander Grothendieck. Revêtements étalés et géométrie algébrique (SGA 1). Lecture Notes in Math, 224, 1971.

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

[6] David Mumford. Tata lectures on theta I. Progress in Mathematics, 28, 1983.

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

[8] Vladimir Platonov, Andrei Rapinchuk, and Rachel Rowen. Algebraic Groups and Number Theory. Pure and Applied Mathematics, 139, 1993.
[9] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. Research in Number Theory, 1(1):12, 2015.

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

[11] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. Annals of Mathematics, pages 492–517, 1968.

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

[13] Jeffrey Yelton. Boundedness results for 2-adic Galois images associated to hyperelliptic Jacobians. arXiv preprint arXiv:1703.10917, 2017.