Mathematical Research Letters **8**, 125–140 (2001)

JACOBIANS OF GENUS ONE CURVES

Catherine O'Neil

1. Introduction

We introduce the notion of an "n-prepared curve," which over a field containing nth roots of unity and where n is invertible is an embedding of a smooth genus one curve C in $\mathbb{P}^{n-1}$ along with a rational n-torsion point T on its Jacobian. The action of T on C then extends to an automorphism of $\mathbb{P}^{n-1}$, i.e. an element $M_T \in \mathrm{PGL}_n$. For $n = 3$ and 5 we find the equation for the Jacobian of an n-prepared curve. In particular, there is a map from the space of n-prepared curves to $X_1(n)$, namely the Jacobian map (along with the specified level n structure); for $n = 3$ and 5, this map turns out to have a beautiful formula in terms of invariants. If F is a cubic equation giving C in $\mathbb{P}^2$, $\mathcal{T}$ is the symmetric trilinear form associated to F and $v_i, (i = 0, 1, 2)$, are distinct fixed points of M_T as above, then the Jacobian map from the set of n- prepared curves to $X_1(3)$ is given by first mapping C to the projective line given by the function $\dfrac{F(v_0)F(v_1)F(v_2)}{\mathcal{T}(v_0, v_1, v_2)^3}$, then by identifying the line with $X_1(3)$ by sending the coordinate λ to the point corresponding to $E_\lambda : X^3 + Y^3 + \lambda Z^3 + XYZ = 0$. In $\mathbb{P}^4$, C is given by the intersection of five quadrics. We may choose a quadric Q so that its orbit under the action of M_T gives five such quadrics. If B is the assocatied bilinear form to Q and if $v_i, (i = 0, \ldots, 4)$, are distinct fixed points of M_T, then map C as above to $\mathbb{P}^1$ by the function $\dfrac{Q(v_0)Q(v_1)Q(v_2)Q(v_3)Q(v_4)}{B(v_0, v_2)B(v_1, v_3)B(v_2, v_4)B(v_3, v_0)B(v_4, v_1)}$, and identify $\mathbb{P}^1$ with $X_1(5)$ by sending the coordinate λ to the point corresponding to the intersection of the following five quadrics: $S_0 = x_0^2 - x_2x_3 + x_1x_4$, $S_1 = x_1^2 - x_0x_2 + \lambda\, x_3x_4$, $S_2 = x_2^2 - x_1x_3 - \lambda\, x_0x_4$, $S_3 = x_3^2 - x_0x_1 - x_2x_4$, and $S_4 = -\lambda\, x_4^2 + x_1x_2 - x_0x_3$.

For $n = 3$ and $n = 5$ we standardize the form of M_T and create sampling spaces of n-prepared curves.

Many other people have studied the problem of finding Jacobians of genus one curves in various contexts and degrees of generality; see [5], [8], [3], [2], [10] and [11].

The author wishes to thank her thesis advisor Barry Mazur for many helpful comments and suggestions.

Received September 28, 2000.

2. General results

2.1. n-prepared genus one curves.

Definition 2.1. *For an integer $n \geq 3$[1], an "n-prepared genus one curve (over $\mathcal{S}$)" is a triple*

$$(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}, \lambda_n),$$

where $\mathcal{C} \xrightarrow{\pi} \mathcal{S}$ is a projective flat morphism whose fibers are smooth genus one curves, $\mathcal{L}$ is an invertible sheaf on $\mathcal{C}$ of degree n (in particular $\mathcal{L}_t$ is a degree n invertible sheaf for every geometric fiber $\mathcal{C}_t$), and λ_n is a fixed-point free S-automorphism of C of order n.

Claim 2.1. *Given a pair $(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \lambda_n)$ of a genus one curve and fixed-point free automorphism as above, let $\mathcal{E}$ be the Jacobian of $\mathcal{C}$. Then λ_n is induced from the natural homogeneous space map $\lambda : \mathcal{C} \times \mathcal{E} \longrightarrow \mathcal{C}$ by restriction to an n-torsion point $\mathcal{T} \in \mathcal{E}[n](\mathcal{S})$.*

Sketch of Proof. This is well-known over a field. In general, we base change to $\mathcal{S}'$ where $\mathcal{C}$ and $\mathcal{E}$ are isomorphic and compare the λ_n map to the map "translation by $\lambda_n(O_E)$;" applying Corollary 6.2 of the Rigidity Lemma (p. 116 of [7]) as in the proof of 2.9, we conclude that λ_n is translation by $\mathcal{T}'$ over $\mathcal{S}'$. We descend $\mathcal{T}'$ to $\mathcal{T}$ over $\mathcal{S}$ as in the proof of 2.9 using Theorem 6 on page 135 of [1]. We leave it to the reader to conclude that λ_n is translation by $\mathcal{T}$. □

In light of the above claim we will use the notation $\lambda_n = \lambda_{\mathcal{T}}$.

Remark A. An n-prepared genus one curve comes with a closed immersion of the curve $\mathcal{C}$ into $\mathbb{P}(\pi_*(\mathcal{L}))$ over $\mathcal{S}$, using the notation of page 162 of [4]. In the case where $\mathcal{S}$ is the spectrum of a local ring or a field, $\mathbb{P}(\pi_*(\mathcal{L}))$ is isomorphic to $\mathbb{P}^{n-1}_{\mathcal{S}}$, and the isomorphism is defined by a choice of basis of the module of global sections of the sheaf $\mathcal{L}$. Fix such an embedding $f : \mathcal{C} \longrightarrow \mathbb{P}^{n-1}_{\mathcal{S}}$, noting that any other choice differs from f by an element of $\mathrm{Aut}(\mathbb{P}^{n-1}_{\mathcal{S}}) = \mathrm{PGL}_n(S)$. Note that f only uses the data of $\mathcal{C} \xrightarrow{\pi} \mathcal{S}$ and the line bundle $\mathcal{L}$.

Definition 2.2. *We define a "morphism of two n-prepared curves" over $\mathcal{S}$*

$$(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}, \lambda_{\mathcal{T}}) \xrightarrow{(g,\alpha)} (\mathcal{C}' \xrightarrow{\pi'} \mathcal{S}, \mathcal{L}', \lambda_{\mathcal{T}'})$$

to be a pair (g, α) with :

1. *$g : \mathcal{C} \longrightarrow \mathcal{C}'$ an $\mathcal{S}$-morphism of schemes,*
2. *$\alpha : \mathcal{L} \cong g^*\mathcal{L}'$, and*
3. *the induced map of Jacobians $g^* : \mathcal{J}' \to \mathcal{J}$ sends $\mathcal{T}'$ to $\mathcal{T}$.*

Remark B. A morphism between two n-prepared genus one curves induces a map between the spaces $\mathbb{P}(\pi_*(\mathcal{L}))$ and $\mathbb{P}(\pi_*(\mathcal{L}'))$ which we also call g; in the case where $\mathcal{S}$ is the spectrum of a local ring and we have fixed closed embeddings f

[1]We can define a 2-prepared genus one curve similarly, with two (linearly inequivalent) invertible sheafs; for the sake of brevity we will assume $n \geq 3$.

and f', there is a unique map over $\mathcal{S}$ which extends g, which we also denote by g :

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{f} & \mathbb{P}^{n-1}_{\mathcal{S}} \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ \mathcal{C}' & \xrightarrow{f'} & \mathbb{P}^{n-1}_{\mathcal{S}} \end{array} \quad ;$$

in words, an $\mathcal{S}$-morphism of n-prepared curves extends to a matrix in $\mathrm{PGL}_n(\mathcal{S})$.

Remark C. The map $\lambda_{\mathcal{T}}$ can be extended to a morphism of Γ to itself, since the degree of $\mathcal{L}$ and the order of $\mathcal{T}$ are both n. When $\mathcal{S}$ is the spectrum of a local ring we have

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{f} & \mathbb{P}^{n-1}_{\mathcal{S}} \\ {\scriptstyle \lambda_{\mathcal{T}}}\downarrow & & \downarrow{\scriptstyle \lambda_{\mathcal{T}}} \\ \mathcal{C} & \xrightarrow{f} & \mathbb{P}^{n-1}_{\mathcal{S}} \end{array} \quad .$$

For a scheme $\mathcal{S}' \to \mathcal{S}$, an n-prepared genus one curve Γ over $\mathcal{S}$ naturally corresponds to one over $\mathcal{S}'$, namely by base change. We will denote this $\Gamma_{\mathcal{S}'} = \Gamma \times_{\mathcal{S}} \mathcal{S}'$. A "$\mathcal{S}'$-morphism" of Γ over $\mathcal{S}$ is defined as above by base changing the curves and replacing $\mathcal{S}$ by $\mathcal{S}'$.

Definition 2.3. *Let $\Gamma = (\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}, \lambda_{\mathcal{T}})$ be an n-prepared curve. Define its associated Jacobian n-prepared curve $\Gamma_{\mathcal{E}} = (\mathcal{E} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}_E, \lambda_{\mathcal{T},\mathcal{E}})$ where $\mathcal{E}$ is the Jacobian of $\mathcal{C}$, $\lambda_{\mathcal{T},\mathcal{E}}$ is "translation by $\mathcal{T}$ on $\mathcal{E}$" for the same $\mathcal{T}$ as in Γ (see Claim 2.1), and $\mathcal{L}_{\mathcal{E}} = \mathcal{O}(\mathcal{T} + 2 \cdot \mathcal{T} + \cdots + n \cdot \mathcal{T})$. Here $i \cdot \mathcal{T}$ is the image of $\mathcal{T}$ under the multiplication-by-i map.*

Our goal is to fine an appropriate base change $\mathcal{S}' \to \mathcal{S}$ so that there exists an $\mathcal{S}'$-morphism between $\Gamma_{\mathcal{S}'}$ and $\Gamma_{\mathcal{E},\mathcal{S}'}$. The existence of such a morphism will give us a matrix (see Remark B) bringing $\mathcal{C}$ to its Jacobian $\mathcal{E}$, at least when the base scheme is nice enough. This is an extremely simple map and arises from the choice of an appropriate basepoint on C. We will geometrically define this basepoint for all n and work out the computations only for $n = 3$ and 5.

2.2. The form of λ_T over a field. Let $n \geq 2$ be an integer and let K be a field whose characteristic does not divide n.

Definition 2.4. *Let $\mathcal{C}_n(K)$ denote the set of n-prepared curves over K. Define the function*

$$b : \mathcal{C}_n(K) \longrightarrow K^*/K^{*n}$$

to send $(C, \mathcal{L}, \lambda_T)$ to $[b] \in K^*/K^{*n}$ if the characteristic polynomial of any lift of λ_T to $GL_n(K)$ (see Remark C) is $x^n - b$.

In order to justify the above definition, we need to show a lift M_T of λ_T has characteristic polynomial $x^n - b$. Before we do that, note the following: let $M'_T \in \mathrm{GL}_n(K)$ be another lift of λ_T; Then $M'_T = u\, M_T$ and the characteristic polynomial of M'_T is $x^n - u^n b$. Also, let f' be another choice of a closed immersion

of C into $\mathbb{P}^{n-1}_K$. Then f' can be written $f\,G$ where $G \in \mathrm{PGL}_n(K)$ is some automorphism of $\mathbb{P}^{n-1}_K$. Then λ_T as an element of $\mathrm{PGL}_n(K)$ will be conjugated by G, but the characteristic polynomial is fixed by conjugation.

Now for the characteristic polynomial of M_T : Clearly $M_T^n = b\,I$ for some $b \in K^*$, since λ_T has order n in $\mathrm{PGL}_n(K)$. Next, the polynomial $x^n - b \in K[x]$ is separable since the characteristic of (K) doesn't divide n. Thus M_T is semisimple and diagonalizable. Finally, we show the eigenvalues of M_T are distinct. The eigenvectors of M_T correspond to fixed points of λ_T in $\mathbb{P}^{n-1}(K^{sep})$. Fix n points $\{p_0, p_1, \ldots p_{n-1}\} \in \mathbb{P}^{n-1}(K^{sep})$ in general position and fixed by M_T. Define $\mathcal{H}_i$ to be the hyperplane in $\mathbb{P}^{n-1}(K^{sep})$ containing all the p_j's except p_i. The $\mathcal{H}_i$ are M_T-invariant. Indeed to show the eigenvalues associated to the fixed points p_i are distinct it is enough to show that the $\mathcal{H}_i$ are the only hyperplanes in $\mathbb{P}^{n-1}(K^{sep})$ which are M_T-invariant. We will use the following lemma:

Lemma 2.1. *Let $\mathcal{H}$ be a hyperplane in $\mathbb{P}^{n-1}_K$ which is M_T-invariant. Then $\mathcal{H}$ intersects C in n distinct $\overline{K}$-rational points. If $\mathcal{H}$ and $\mathcal{H}'$ are two distinct M_T-invariant hyperplanes, then $\mathcal{H} \cap C$ and $\mathcal{H}' \cap C$ are disjoint. Finally, let $x \in \mathcal{H} \cap C(\overline{K})$. Then x has the following property:*

$$\mathcal{L}_{\overline{K}} = \mathcal{O}(\, n \cdot x + T' \,) \in Pic^n_{C/K}(\overline{K}),$$

where $T' = \frac{n(n-1)}{2} \cdot T$.

Proof. The geometric points on $\mathcal{H} \cap C$ form an orbit of the action of λ_T. This implies that $\mathcal{H}_i$ intersects C in n distinct points. Assume there is a geometric point x in both $\mathcal{H} \cap C$ and $\mathcal{H}' \cap C$. Then $\mathcal{H} \cap C$ and $\mathcal{H}' \cap C$ consist of the same orbit, so $\mathcal{H} = \mathcal{H}'$. Then $\mathcal{H} \cap C = \sum_{i=0}^{n-1}(x + i \cdot T)$, and since $\mathcal{H}$ is a hyperplane $\mathcal{O}(\mathcal{H} \cap C) \sim \mathcal{L}$. □

Note that we can rewrite the property $\mathcal{L}_{\overline{K}} = \mathcal{O}(\, n \cdot x + T' \,) \in Pic^n_{C/K}(\overline{K})$, over $\overline{K}$ as $L_{\overline{K}} \otimes \mathcal{O}(-T') = \mathcal{O}(\, n \cdot x \,)$. Since the map $[n\,]$ is finite étale with degree n^2, there are clearly only n^2 such geometric points x. We have accounted for all n^2 points by the n distinct hyperplanes $\mathcal{H}_i$ defined above. If $\mathcal{H}$ is any hyperplane fixed by λ_T, from above we see that $\mathcal{H} \cap C = \mathcal{H}_i \cap C$ for some i, which implies that $\mathcal{H} = \mathcal{H}_i$.

Corollary 2.2. *Let $\Gamma = (C, \mathcal{L}, \lambda_T)$ be an n-prepared curve over a field K of characteristic prime to n. Let $b(\Gamma) = b$, and fix an embedding of C in $\mathbb{P}^{n-1}_K$ and a lift M_T of λ_T to $GL_n(K)$. Then there exist n distinct eigenvectors of M_T defined over $K(\sqrt[n]{b})$ with eigenvalues $\sqrt[n]{b}\,\zeta_n^i, i = 1, \ldots, n$.*

Theorem 2.3. *Assume K is infinite. Let $\Gamma = (C, \mathcal{L}, \lambda_T)$ be an n-prepared curve over K. There is a (non-unique) choice of the closed immersion f so that λ_T*

lifts to the matrix

$$M_{n,b} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ b & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Proof. Various choices of f differ by automorphisms of $\mathbb{P}^{n-1}(K)$, which result in conjugation of λ_T. Let $M_T \in \mathrm{GL}_n(K)$ be a lift of λ_T. We wish to find $G \in \mathrm{GL}_n(K)$ such that GM_TG^{-1} is the above matrix. Say we have a vector v in $\mathbb{A}^n_K$ such that the set of vectors

$$\{\omega_1 = v, \omega_2 = M_T v, \omega_3 = M_T^2 v, \dots, \omega_n = M_T^{n-1} v\}$$

is a basis for $\mathbb{A}^n_K$. Then let G be any lift of the corresponding change of basis matrix (note that M_T sends $\omega_n = M_T^{n-1}v$ to $M_T \cdot M_T^{n-1}v = b \cdot v$). It remains to prove such a v exists. A vector whose orbit under M_T does not span all of $\mathbb{A}^n_K$ correspond to a point of $\mathbb{P}^{n-1}_K$ which lies on one of the n hyperplanes $\mathcal{H}_i$ (see page 128), fixed by λ_T. Take v to be a vector corresponding to a K-point away from these hyperplanes. Such a v exists since K is infinite. □

2.3. Jacobian n-prepared curves. Let $n \geq 3$ be an integer and let K be a field whose characteristic does not divide n. Let $\Gamma = (C, \mathcal{L}, \lambda_T)/K$ be an n-prepared curve and let

$$\Gamma_E = (E, \mathcal{L}_E = \mathcal{O}(n \cdot O_E + T'), \lambda_{T,E})/K,$$

where $T' = \frac{n(n-1)}{2} \cdot T$, be the associated n-prepared Jacobian (see Definition 2.3). Fix an closed immersion f_E of E in $\mathbb{P}^{n-1}_K$ (Remark A). By Remark C the automorphism $\lambda_{T,E}$ extends to an automorphism $\lambda_{T,E} \in \mathrm{PGL}_n(K)$. Choose a lift $M_{T,E} \in \mathrm{GL}_n(K)$ of $\lambda_{T,E}$.

Claim 2.2. *Assume K is infinite and that $\zeta_n \in K$ is a fixed primitive nth root of unity. We may choose the closed immersion f_E so that $\lambda_{T,E}$ lifts to the matrix $D = diag(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1})$. Moreover we may choose O_E to be any K-rational point which is not fixed by $\lambda_{T,E}$ but is lying on $\lambda_{T,E}$-invariant hyperplane.*

Proof. By Theorem 2.3 we can lift $\lambda_{T,E}$ to the matrix M_b (page 128). By Corollary 2.8 which will be proved on page 132, $b(\Gamma_E) = 1$. We need to find a matrix W defined over K which conjugates $M_{b=1}$ to D. Such a W is given by $(w_{i\,j})_{i,\,j}$ where $w_{i\,j} = \zeta_n^{i\,j}$. By construction the line bundle which gives f_E is associated to the divisor $n \cdot O_E + T'$ where $T' = \frac{n(n-1)}{2} \cdot T$. In other words O_E plays the part of x_0 from Lemma 2.1. Then by Lemma 2.1, O_E is on a $\lambda_{T,E}$-invariant hyperplane of D but is not fixed by D since $\lambda_{T,E}$ acts fixed-point free on E. Moreover, note that any invertible diagonal matrix commutes with D. Then we may move O_E to any K-rational point lying on a fixed hyperplane of $[D]$. Since the matrix is invertible, the image point will not be fixed by D. □

Theorem 2.4. *Let $x_0 \in C(\overline{K})$ satisfy the condition of Claim* 2.1*, namely that $\mathcal{L}_{\overline{K}} \sim \mathcal{O}(\, n \cdot x + T'\,)$. Then there is a $K(x_0)$-morphism (φ_{x_0}, α) from $\Gamma_{K(x_0)}$ to $\Gamma_{E,K(x_0)}$ sending x_0 to O_E. In particular once we identify C with $\underline{Pic}^1(C)$, φ_{x_0} sends a point $x \in C$ to the point of E corresponding to the degree zero divisor $(x - x_0)$.*

Remark. The above theorem is the realization of the goal; we have found the choice of basepoint x_0 giving rise to the Jacobian morphism of n-prepared curves.

Proof. Start with the map φ_{x_0} with $\varphi_{x_0}(x) \mapsto (x - x_0)$. For φ_{x_0} to extend to a $K(x_0)$-morphism there must exist a map $\alpha : \mathcal{L} \cong \varphi_{x_0}^* \mathcal{L}_E$. On the level of divisors this translates as $n \cdot x_0 + T' \sim (n \cdot O_E + T') + n \cdot x_0$. The induced map of Jacobians sends T to T once we identify E with its own Jacobian. □

Claim 2.3. $\varphi_{x_0} \lambda_T = \lambda_{T,E}\, \varphi_{x_0}$.

Proof. On the level of divisors this is saying $(x + T) - x_0 \sim (x - x_0) + T$. □

2.4. The Weil Pairing. Let $n \geq 2$ be an integer. Let K be a field whose characteristic does not divide n. From Remark A, given a pair $(C, \mathcal{L})/K$ where $\mathcal{L}$ is a degree n line bundle over the smooth genus one curve C we get an embedding f of C in $\mathbb{P}^{n-1}_K$, defined up to automorphism of $\mathbb{P}^{n-1}_K$. Let E/K be the Jacobian of C; by Remark C, for any $T \in E[n](K)$ we can uniquely extend λ_T, translation by T on C, to $[M_T] \in \mathrm{PGL}_n(K)$, an automorphism of $\mathbb{P}^{n-1}_K$. By extending the base field K if necessary we may assume that all points of $E[n]$ are rational over K. Then we get a homomorphism

$$\chi : E[n](K) \longrightarrow PGL_n(K).$$

$$\chi : T \longmapsto [M_T].$$

Remarks. χ is injective because $E[n]$ acts faithfully on C; χ is a homomorphism by uniqueness of $[M_T]$; finally, χ is Galois-invariant because the maps λ_T and f are defined over K, so $\lambda_T^\sigma = \lambda_{T^\sigma}$.

A natural question to ask is: how close is χ to being a representation? If for each T we could lift M_T to $\mathrm{GL}_n(K)$ such that their combined image commutes, we would have a representation. The obstruction to the lifting is the commutator $[M_T, M'_T]$. Note that the determinant of this element is one and its image in $\mathrm{PGL}_n(K)$ is trivial since $E[n]$ is abelian. Therefore

$$[M_T, M'_T] = \epsilon \cdot I, \qquad \epsilon^n = 1.$$

We thus have a pairing $e(L) : E[n](L) \times E[n](L) \longrightarrow \mu_n(L)$. The pairing $e(L)$ is bilinear, alternating, and induced by a bilinear alternating pairing of group schemes

$$e : E[n] \times E[n] \longrightarrow \mu_n.$$

Theorem 2.5. *e is the Weil pairing.*

Sketch of Proof. In [6], Mumford defines the concept of a theta group associated to a line bundle over an abelian variety (pages 221-229). In exactly the same way it is possible to define the theta group associated to a line bundle over a homogeneous space of an abelian variety. On page 222 of [6], Mumford defines a skew-symmetric bihomomorphism for any theta group, which he denotes by $e^{\mathcal{L}}$ in the case of the theta-group associated to a line bundle $\mathcal{L}$. In our situation the pairing e above is the skew-symmetric bihomomorphism for the theta group associated to $\mathcal{L}$ over the curve C. Finally, on page 228 [6], Mumford proves crucial properties of $e^{\mathcal{L}}$ and in particular how it relates to the Weil pairing. Using properties 4 and 5 we deduce that e above is the Weil pairing on E. □

2.5. A cohomological invariant. Let K be a field whose characteristic does not divide the integer $n \geq 2$. Let $\Gamma = (C, \mathcal{L}, \lambda_T)$ be an n-prepared curve over the field K, and let $\mathcal{C}_n(K)$ be the set of n-prepared curves over K. Let G_K be the absolute Galois group of K. We defined map (page 127) $b : \mathcal{C}_n(K) \longrightarrow K^*/K^{*n}$. Using our knowledge of the Weil pairing we will identify b as a cohomological invariant attached to Γ.

Let E be (isomorphic to) the Jacobian of C. Then we may identify C in the cohomology group $H^1(G_K, E(\overline{K}))$. Indeed since $\mathcal{L}$ is a degree n line bundle on C we actually know that C corresponds to an element $\xi_C \in H^1(G_K, E(\overline{K}))[n]$. Thus we have a map $\overline{\ell} : \mathcal{C}_n(K) \to H^1(G_K, E(\overline{K}))[n]$. We make use of the short exact sequence (page 197 of [9]):

$$0 \longrightarrow E(K)/n\,E(K) \xrightarrow{\delta} H^1(G, E[n](\overline{K})) \longrightarrow H^1(G, E(\overline{K}))[n] \longrightarrow 0.$$

Claim 2.4. *There exists a lift $\ell : \mathcal{C}_n(K) \to H^1(G, E[n](\overline{K}))$ of $\overline{\ell}$ which sends ξ_C to the cocycle class of $x_0 - x_0^\sigma$ for $x_0 \in C(\overline{K})$ as in Theorem 2.4.*

Proof. Write $\mathcal{L} = \mathcal{O}(D)$ for some K-rational degree n divisor D. Then by construction $n \cdot x_0 + T' \sim D$, so $n \cdot (x_0 - x_0^\sigma) \sim (D - T') - (D - T')^\sigma \sim O_E$, since D and T are K-rational. □

Remarks. (1) A different choice x_0' will differ (with respect to the action of E) from x_0 by an n-torsion point, since $n \cdot x_0 + T' \sim n \cdot x_0' + T' \Rightarrow n(x_0 - x_0') \sim 0$. Therefore the cocycles $x_0 - x_0^\sigma$ and $x_0' - x_0'^\sigma$ differ by a coboundary and ℓ is well-defined. (2) We have used all of the information of Γ, not just C, to define ℓ.

Since $T \in E[n](K)$ we get a group scheme map $\mathbb{Z}/n\mathbb{Z} \longrightarrow E[n]$; using the identification $E[n] \cong E[n]^\wedge$ by sending $S \mapsto e(-, S)$ we dualizes the above map to get $E[n] \longrightarrow \mu_n$, giving the cohomological map

$$e^*(-, T) : H^1(G, E[n](\overline{K})) \longrightarrow H^1(G, \mu_n(\overline{K})) \cong K^*/K^{*n}.$$

The last isomorphism uses Hilbert's Theorem 90. Composing we produce a map

$$\ell \circ e^*(-, T) : \mathcal{C}_n(K) \longrightarrow K^*/K^{*n}.$$

Theorem 2.6. $\ell \circ e^*(-, T) = b$.

Proof. The map $H^1(G, \mu_n) \cong K^*/K^{*n}$ is given by

$$\left[\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\right] \longleftrightarrow a.$$

Let S_σ be the n-torsion point $x_0 - x_0^\sigma \in E[n](\overline{K})$ and let $M_{S_\sigma} \in \mathrm{GL}_n(\overline{K})$ denote a lift of the extension of λ_{S_σ} to $\mathbb{P}^{n-1}_{\overline{K}}$. By definition, $(e^* \circ l\,)(\Gamma)$ is the class of the cocycle

$$\sigma \mapsto e(x_0 - x_0^\sigma, T)$$

Using the version of the Weil pairing defined on page 130, we have

$$e(x_0 - x_0^\sigma, T) \cdot I = [M_{S_\sigma},\, M_T].$$

We find $e(x_0 - x_0^\sigma, T)$ by seeing where one nonzero vector v in $\mathbb{A}^n_{\overline{K}}$ is mapped by $M_{S_\sigma}\, M_T\, M_{S_\sigma}^{-1}\, M_T^{-1}$. Recall that $x_0 \in C(\overline{K})$ is on a hyperplane $\mathcal{H} \subset \mathbb{P}^{n-1}_{\overline{K}}$ containing all but one fixed point p under M_T. Let v be a vector corresponding to that p. The eigenvalue of v is $\sqrt{n}[b]\zeta_n^i$ for some i. An alternate definition of $\mathcal{H}$ is that it contains x_0's orbit under λ_T.

Lemma 2.7. *For any $\sigma \in G_K$, $M_{S_\sigma}^{-1}(v) = \varepsilon \cdot v^\sigma$ for some $\varepsilon \in \overline{K}^*$.*

Proof. $M_{S_\sigma}^{-1}(x_0 + j \cdot T) = x_0^\sigma + j \cdot T = (x_0 + j \cdot T)^\sigma$ since S_σ corresponds to the degree zero divisor $x_0 - x_0^\sigma$. Since the $x_0 + j \cdot T$ generate $\mathcal{H}$, we conclude that $M_{S_\sigma}^{-1}(\mathcal{H}) = \mathcal{H}^\sigma$. The fixed points of M_T, $n-1$ of which are on $\mathcal{H}$, are permuted by M_{S^σ} so we must have $M_{S_\sigma}^{-1}(p) = p^\sigma$; in other words $M_{S_\sigma}^{-1}(v) = \varepsilon \cdot v^\sigma$ for some $\varepsilon \in \overline{K}^*$. □

To finish, we have

$$\begin{aligned} M_{S_\sigma}\, M_T\, M_{S_\sigma}^{-1}\, M_T^{-1}(v) \;&=\; M_{S_\sigma}\, M_T\, M_{S_\sigma}^{-1}(v) \cdot \frac{1}{\sqrt[n]{b}\,\zeta^i} \\ = M_{S_\sigma}\, M_T(v^\sigma) \cdot \frac{\varepsilon}{\sqrt[n]{b}\,\zeta^i} \;&=\; M_{S_\sigma}\, (M_T(v))^\sigma \cdot \frac{\varepsilon}{\sqrt[n]{b}\,\zeta^i} \\ = M_{S_\sigma}(v^\sigma) \cdot \frac{\varepsilon(\sqrt[n]{b}\,\zeta^i)^\sigma}{\sqrt[n]{b}\,\zeta^i} \;&=\; v \cdot \frac{\varepsilon(\sqrt[n]{b}\,\zeta^i)^\sigma}{\varepsilon\,\sqrt[n]{b}\,\zeta^i} \;=\; v \cdot \frac{(\sqrt[n]{b}\,\zeta^i)^\sigma}{\sqrt[n]{b}\,\zeta^i}. \end{aligned}$$

□

Corollary 2.8. *Let Γ_E be the n-prepared Jacobian associated to Γ. Then*

$$b\,(\Gamma_E) = 1 \in K^*/K^{*n}.$$

Proof. By Definition 2.3, $\Gamma_E = (E, \mathcal{O}(T + 2 \cdot T + \cdots + n \cdot T), \lambda_{T,\mathcal{E}}\,)$. Clearly E corresponds to the trivial class in $H^1(G_K, E(\overline{K}))$. Moreover, the lift in Claim 2.4 is also trivial, since we may take $x_{0,E}$ to be O_E (see Theorem 2.4). Thus its image in K^*/K^{*n} is 1. □

2.6. Jacobians of Families of Curves. We have included this section in order to assert that we have found the Jacobian map for an entire family of curves rather than for individual fibers of the family. It may be skipped and referenced as needed.

Let $\mathcal{C}$ be a genus one curve over a base $\mathcal{S}$, let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$, and let $\mathcal{E}$ be an elliptic curve over $\mathcal{S}$. Let $\kappa : \mathcal{S}' \to \mathcal{S}$ be a surjective étale morphism. Assume there exist morphisms $r : \mathcal{J}_{\mathcal{S}'} \to \mathcal{C}_{\mathcal{S}'}$ and $\varphi : \mathcal{C}_{\mathcal{S}'} \to \mathcal{E}_{\mathcal{S}'}$ defined over $\mathcal{S}'$ such that

1. $\mathcal{J}_{\mathcal{S}'} \overset{r}{\cong} \mathcal{C}_{\mathcal{S}'} \overset{\varphi}{\cong} \mathcal{E}_{\mathcal{S}'}$ sends the origin $O_{\mathcal{J}}$ to $O_{\mathcal{E}}$,
2. $\forall$ fields F such that $t : \mathrm{Spec}(F) \to \mathcal{S}$ is a $\mathrm{Spec}(F)$-valued point of $\mathcal{S}$, there exists $\alpha_t : \mathcal{J}_t \cong \mathcal{E}_t$, and
3. $\forall$ fields F and points $t' : \mathrm{Spec}(F) \to \mathcal{S}'$ of $\mathcal{S}'$ we define $t = \kappa \circ t'$; then we have $\alpha_t = \varphi_{t'} \circ r_{t'}$.

Let $\gamma = \varphi \circ r$.

Theorem 2.9. *We can descend γ to an isomorphism $\mathcal{J} \overset{\gamma}{\cong} \mathcal{E}$.*

Proof. By Theorem 6 on page 135 of [1], since $\mathcal{S}' \to \mathcal{S}$ is surjective étale, we can descend γ if and only if $p_1^*(\gamma) = p_2^*(\gamma)$, where

$$\begin{array}{ccc} \mathcal{S}' \times_{\mathcal{S}} \mathcal{S}' & \xrightarrow{p_2} & \mathcal{S}' \\ {\scriptstyle p_1}\downarrow & & \downarrow \\ \mathcal{S}' & \longrightarrow & \mathcal{S} \end{array} .$$

We will apply Corollary 6.2 of the Rigidity Lemma (p. 116 of [7]) to each connected component of $\mathcal{S}' \times_{\mathcal{S}} \mathcal{S}'$. The corollary states that given two elliptic curve families $\mathcal{E}_1$ and $\mathcal{E}_2$ over the base $\mathcal{T}$ and two maps φ_1 and φ_2 from $\mathcal{E}_1$ to $\mathcal{E}_2$, if $\varphi_1 = \varphi_2$ at a $\mathrm{Spec}(F)$-point of $\mathcal{T}$ then φ_1 and φ_2 differ by a section. For any $\mathrm{Spec}(F) \overset{t''}{\to} \mathcal{S}' \times_{\mathcal{S}} \mathcal{S}'$, define $t'_1 = p_1 \circ t''$ and $t'_2 = p_2 \circ t''$. By the third condition above, we have $\alpha_t = \varphi_{t'_1} \circ r_{t'_1} = \gamma_{t'_1} = p_1^*(\gamma)_{t''}$. By symmetry we also have $\alpha_t = p_2^*(\gamma)_{t''}$. Thus $p_1^*(\gamma)$ and $p_2^*(\gamma)$ differ by a section; since they both bring the origin to the origin, the section is trivial. □

3. The case of 3-prepared curves

3.1. When $\zeta_3 \in K$. Let K be a field of characteristic prime to 3. Assume $\zeta_3 \in K$. Let (C, L, λ) be a 3-prepared curve over the field K, where $[M_T] \in \mathrm{PGL}_3(K)$ represents λ and $b \in K^*/K^{*3}$ is the associated cohomological invariant (see Theorem 2.6). Let $(E, L_E, [D])$ be its associated 3-prepared Jacobian, where D is the diagonal matrix $diag(1, \zeta_3, \zeta_3^2) \in \mathrm{PGL}_3(K)$ and $O_E = (1 : -1 : 0)$ (Claim 2.2). Fix a cubic F which defines C in $\mathbb{P}^2_K$. Let x_0 be a K^{sep}-point of C satisfying the conditions of Theorem 2.4, so that the map φ_{x_0} from $C_{K^{sep}}$ to $E_{K^{sep}}$ extends to $\mathrm{PGL}_3(K^{sep})$. Finally, let φ_{x_0} be represented in $\mathrm{PGL}_3(K^{sep})$ by the matrix Φ^{-1}. Fix eigenvectors v_1, v_2, v_3 of M_T defined over the field $K(\sqrt[3]{b})$ such that

each v_i has eigenvalue $\sqrt[3]{b}\zeta^i$ and so the set $\{v_i\}$ is fixed under the action of Gal $(K(\sqrt[3]{b}/K)$ (see Corollary 2.2).

Theorem 3.1. *E is given by:*

$$F_E = X^3 + Y^3 + F(v_1)F(v_2)F(v_3) \cdot Z^3 + \mathcal{T}(v_1, v_2, v_3) \cdot XYZ,$$

for v_i as above and where $\mathcal{T}$ is the symmetric trilinear form associated to F.[2]

Remark. By scaling Z above we see that the Jacobian map is given by the composition of the morphism $\dfrac{F(v_1)F(v_2)F(v_3)}{\mathcal{T}(v_1, v_2, v_3)^3}$ from the space of 3-prepared curves to $\mathbb{P}^1$ with the identification of $\mathbb{P}^1$ with $X_1(3)$ which sends the coordinate λ to the curve $E_\lambda : X^3 + Y^3 + \lambda Z^3 + XYZ = 0$.

Proof. The proof is given by the following claim. □

Claim 3.1. *With the above notation, and with a possible permutation of the names of the v_i, $x_0 = v_1 - \theta \cdot v_2$ and the map $\varphi_{x_0} = [\Phi^{-1}]$ is given by*

$$\Phi = (v_1 \;\; \theta\, v_2 \;\; \theta^2 F(v_2)\, v_3),$$

where $\theta^3 = \dfrac{F(v_1)}{F(v_2)}$.

Proof. By Claim 2.3 we have $\lambda_{T,E}\, \varphi_{x_0} = \varphi_{x_0} \lambda_{T,C}$; in terms of matrices this implies $[\Phi\, D] = [M_T\, \Phi]$. Write $\Phi = (w_1\, w_2\, w_3)$ for some vectors w_i. Then

$$[\Phi\, D] = \left[(w_1\, w_2\zeta\, w_3\zeta^2)\right] = [(M_T w_1\, M_T w_2\, M_T w_3)] = [M_T\, \Phi]\,;$$

we conclude that the $w_i's$ are eigenvectors of M_T with distinct eigenvalues. With possible rescaling of Φ and relabeling of the v_i we may assume $w_1 = v_1$, w_2 is some multiple θ of v_2, and w_3 is some multiple $\theta^2\, l$ of v_3.

D acts linearly on the space of cubics; since $\lambda_{T,E}$ lifts to D, the cubic F_E giving E is in an eigenspace of D. There are three eigenspaces, and two of the three have the property that any element has zeroes at the fixed points of D. Since $\lambda_{T,E}$ has no fixed points on E, F_E is in the third eigenspace, and we conclude that there exist $r_i \in K$ such that $F_E = r_1\, X^3 + r_2\, Y^3 + r_3\, Z^3 + r_4\, XYZ$. On the other hand we have $F_E(X, Y, Z) = F(\Phi(X, Y, Z)) = F(v_1\, X + \theta v_2\, Y + l\theta^2 v_3\, Z)$. Expanding we get $r_1 = F(v_1), r_2 = \theta^3 F(v_2).r_3 = l^3\theta^6 F(v_3)$ and $r_4 = l\theta^3 \mathcal{T}(v_1, v_2, v_3)$. Plugging in $O_E = (1 : -1 : 0)$ we conclude that $\theta^3 = \frac{F(v_1)}{F(v_2)}$.[3] Note that $F(v_i) \neq 0$ since there are no fixed points of M on C. It remains to find l. Substituting $\theta^3 = \frac{F(v_1)}{F(v_2)}$ and scaling F_E by $\frac{1}{F(v_1)}$ we obtain

$$F_E = X^3 + Y^3 + l^3\, \frac{F(v_1)F(v_3)}{F(v_2)^2}\, Z^3 + \frac{l}{F(v_2)} \mathcal{T}(v_1, v_2, v_3)\, XYZ,$$

[2]Define the trilinear form $\mathcal{T}$ associated to the cubic form F by $\mathcal{T}(u, v, w) = F(u+v+w) - F(u+v) - F(u+w) - F(v+w) + F(u) + F(v) + F(w)$.

[3]Note that this defines θ only up to a choice of a cube root. Indeed a different choice of θ corresponds to a different choice of x_0, a translate of the original choice by T. Recall that there are 9 choices for x_0, differing from each other by the 3-torsion points on E.

a K-rational equation. Since $\mathcal{T}(v_1, v_2, v_3)$ is defined over $K(\sqrt[3]{b})$ and is clearly fixed by any automorphism of that field, it is K-rational. Then $\frac{l}{F(V_2)} \in K$. Write $l = F(V_2)\,\epsilon$ for some $\epsilon \in K$. Then we have

$$F_E = X^3 + Y^3 + \epsilon^3 F(v_1)F(v_2)F(v_3)\,Z^3 + \epsilon\,\mathcal{T}(v_1, v_2, v_3)\,XYZ,$$

and we can modify this model over K by scaling Z by ϵ^{-1}. In other words we may assume $\epsilon = 1$. □

We now specialize the above formula to a situation with fixed F, M_T, and v_i.

For $b \in K$, define the matrix $M = M_{3,b}$ (see Theorem 2.3). For variables $\alpha, \beta, \gamma, \delta$, and b, define

$$F_{\mathcal{C}} = \alpha\,(b^2X^3 + bY^3 + Z^3) + \beta\,(bXY^2 + bX^2Z + YZ^2) + \gamma\,(bX^2Y + Z^2X + Y^2Z) + \delta\,(3XYZ).$$

Then M acts on $F_{\mathcal{C}}$ and thus on the underlying space. Define $\mathcal{S}$ to be the largest (open) subscheme of $\mathrm{Spec}(\mathbb{Z}[1/3, \zeta_3, b, \alpha, \beta, \gamma, \delta])$ such that $F_{\mathcal{C}}$ defines a smooth flat genus one curve $\mathcal{C}/\mathcal{S}$ embedded by $f_{\mathcal{C}}$ in $\mathbb{P}^2_{\mathcal{S}}$ and so that M acts fixed-point free on every geometric fiber. Let $\mathcal{L} = f_{\mathcal{C}}^*(\mathcal{O}(1))$.

Theorem 3.2. *$(\mathcal{C}, \mathcal{L}, [M])$ is a 3-prepared curve over $\mathcal{S}$. Moreover, any 3-prepared curve over K is the pullback of $\mathcal{C}$ to a K-point of $\mathcal{S}$.*

Proof. Given a 3-prepared curve (C, L, λ) over K, we may assume by Theorem 2.3 that $\lambda \in \mathrm{PGL}_3(K)$ lifts to M. By a similar argument as in the proof of Claim 3.1 above, the cubic giving C must be in an M-eigenspace of cubics whose elements have no M-fixed points. The only such eigenspace is four dimensional and generators are given above. □

Theorem 3.3. *The Jacobian $\mathcal{E}$ of $\mathcal{C}$ is given by*

$$F_{\mathcal{E}} = X^3 + Y^3 + [(\alpha b + \delta)^3 + \beta^3 b^2 + \gamma^3 b - 3(\alpha b + \delta)\beta\gamma b]\,Z^3 + (2\alpha b - 3\delta)\,XYZ,$$

with $O_{\mathcal{E}} = (\,1 : -1 : 0\,)$.

Proof. We will use Theorem 2.9. Let $\mathcal{S}$ be as above, and define $\mathcal{J}$ to be the Jacobian of $\mathcal{C}$ and $\mathcal{E}$ to be the elliptic curve given by the equation $F_{\mathcal{E}}$ above. Let $\mathcal{S}' = \mathcal{S}[\sqrt[3]{b}]$. There exists a natural étale surjective map $\kappa : \mathcal{S}' \to \mathcal{S}$. There exists a map $r : \mathcal{J}_{\mathcal{S}'} \to \mathcal{C}_{\mathcal{S}'}$ defined over $\mathcal{S}'$ because there is a $\mathcal{S}'$-section of $\mathcal{C}$, namely x_0 as in the proof of Claim 3.1, when we set $M_T = M$ and $v_i = (1 \;\; \zeta_3^i \sqrt[3]{b} \;\; \zeta_3^{2i} \sqrt[3]{b^2})^\tau$. Also there exists $\varphi : \mathcal{C}_{\mathcal{S}'} \to \mathcal{E}_{\mathcal{S}'}$ defined over $\mathcal{S}'$ given by the matrix Φ as in the proof of Claim 3.1. By construction the composite map sends the origin of $\mathcal{J}$ to the origin of $\mathcal{E}$. Next, Theorem 3.1 generalizes to any field F so conditions 2 and 3 on page 133 are satisfied given the above choice for M_T and v_i. We conclude by Theorem 2.9 that $\mathcal{E} \cong \mathcal{J}$. □

3.2. When $\zeta_3 \notin K$. Let the notation be as in Section 3.1 with the exception of having $\zeta_3 \in K$.

Theorem 3.4. *The Jacobian $\mathcal{E}$ of $\mathcal{C}$ is given by*

$$F_{\mathcal{E}} = (2+\mathcal{N}+\tau)(X^3+Y^3+Z^3) + (3\mathcal{N}-3)(X^2Y+Y^2Z+Z^2X+XY^2+YZ^2+ZX^2) + (6\mathcal{N}+12-3\tau)(XYZ),$$

where

$$\mathcal{N} = [(\alpha b+\delta)^3+\beta^3b^2+\gamma^3b-3(\alpha b+\delta)\beta\gamma b], \tau = (2\alpha b-3\delta),$$

and with $O_{\mathcal{E}} = (1:-1:0)$.

Proof. Again we will work over the field K and the general result will follow as above. Let (C, L, λ) be a 3-prepared curve over the field K. Let J be the Jacobian of C. Note that the curve E in Theorem 3.1 is defined over K even when $\zeta_3 \notin K$. In fact E is a twist of J and they become isomorphic over the field $K(\zeta_3)$. We exhibit this isomorphism. The only assumptions we made on the model for E were that $\lambda_{T,E}$ lifted to the matrix D and that $O_E = (1:-1:0)$. When $\zeta \notin K$ we may assume (Theorem 2.3) that $\lambda_{T,J}$ lifts to $M_E = M_{3,1}$ (see Theorem 2.3) and again that $O_E = (1:-1:0)$ (as in Claim 2.2). Then an isomorphism of J with E is given by the element

$$W = \left[\begin{pmatrix} \zeta_3^2 & \zeta_3 & 1 \\ \zeta_3 & \zeta_3^2 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right] \in \mathrm{PGL}_n(K(\zeta_3));$$

note that W has the properties that $W(1:-1:0) = (1:-1:0)$ and $W\lambda_{T,J}W^{-1} = \lambda_{T,E}$. To recover the equation for J we need only act on the equation for E by W^{-1} :

$$F_J(X,Y,Z) = F_E(W^{-1}(X,Y,Z)).$$

A computation leads to the result. □

4. The case of 5-prepared curves

Let K be a field of characteristic prime to 5. Assume $\zeta_5 \in K$, with the accompanying remark that if $\zeta_5 \notin K$, we may modify our final equations by a map W analogous to that in Section 3.2. For $b \in K$, define the matrix $M = M_{5,b}$ (see Theorem 2.3). Let $[M]$ denote the class of M in $\mathrm{PGL}_5(K)$. For variables $a_{i,j}, 0 \le i,j \le 4$, define the K-vector space $V_{\mathcal{C}}$ to be generated by the orbit of the quadric

$$Q_{\mathcal{C}} = \sum_{0 \le i,j \le 4} a_{i,j}x_ix_j$$

under the action of the matrix M. Since M acts on $V_{\mathcal{C}}$ it acts on the underlying zero locus of $V_{\mathcal{C}}$. Define $\mathcal{S}$ to be the largest subscheme of $\mathrm{Spec}(K[a_{i,j}])$ such that $V_{\mathcal{C}}$ defines a smooth flat genus one curve $\mathcal{C}/\mathcal{S}$ embedded by $f_{\mathcal{C}}$ in $\mathbb{P}^4_{\mathcal{S}}$ and so that

M acts fixed-point free on every geometric fiber. Then $\mathcal{S}$ is an open part of a closed subscheme of $\mathrm{Spec}(K[a_{i,j}])$. Let $\mathcal{L} = f_{\mathcal{C}}^*(\mathcal{O}(1))$.

Theorem 4.1. *$(\mathcal{C}, \mathcal{L}, [M])$ is a 5-prepared curve over $\mathcal{S}$. Moreover, any 5-prepared curve over K is the pullback of a K-point of $\mathcal{S}$ to $\mathcal{C}$.*

Proof. $(\mathcal{C}, \mathcal{L}, [M])$ is a 5-prepared curve by construction. Let (C, L, λ) be a 5-prepared curve over K. By Theorem 2.3 we may assume λ lifts to M. By Remark A we get an embedding of C in $\mathbb{P}^4_K$ as a degree 5 curve. Then C will be the intersection of five quadrics, or equivalently will be the zero locus of a 5 dimensional vector space generated by quadrics in $\mathbb{P}^4_K$. That we can choose this basis to be an orbit of one quadric under the action of λ follows from the same argument as in the proof of Theorem 2.3. □

Theorem 4.2. *The Jacobian $\mathcal{E} = \mathcal{E}_A$ of $\mathcal{C}$ is given by the quadrics*

$$S_0 = x_0^2 - x_2x_3 + x_1x_4,\ S_1 = x_1^2 - x_0x_2 + A\,x_3x_4,\ S_2 = x_2^2 - x_1x_3 - A\,x_0x_4,$$
$$S_3 = x_3^2 - x_0x_1 - x_2x_4,\ S_4 = -A\,x_4^2 + x_1x_2 - x_0x_3,$$

where $A = \dfrac{\prod_{i=0}^4 Q(v_i)}{\prod_{i=0}^4 B(v_i, v_i+2)}$ *and with* $O_{\mathcal{E}} = (\,1 : 1 : 1 : 1 : 0\,)$.

Remark. The Jacobian map is given by sending a 5-prepared curve C to the point on $X_1(5)$ corresponding to the elliptic curve E_A as above. In other words, A is a parameter on $X_1(5)$ identifying it with $\mathbb{P}^1$.

We will first give an abstract algorithm to find the Jacobian of any 5-prepared curve over K. We will then concretely apply this algorithm to any K'-fiber of $\mathcal{C}$. The proof of Theorem 4.2 follows from this by the same argument as in Theorem 3.3.

We fix notation. Let (C, L, λ) be a 5-prepared curve over the field K, where $[M_T] \in \mathrm{PGL}_5(K)$ represents λ and $b \in K^*/K^{*5}$ is the associated cohomological invariant (see Theorem 2.6). Let $(E, L_E, [D])$ be its associated 5-prepared Jacobian, where $D = diag(1, \zeta_5, \zeta_5^2, \ldots, \zeta_5^4)$ and $O_E = (1 : 1 : 1 : 1 : 0)$ (Claim 2.2). Let x_0 be a K^{sep}-point of C satisfying the conditions of Theorem 2.4, so that the map φ_{x_0} from $C_{K^{sep}}$ to $E_{K^{sep}}$ extends to $\mathrm{PGL}_5(K^{sep})$. Finally, let φ_{x_0} be represented in $\mathrm{PGL}_5(K^{sep})$ by the matrix Φ^{-1}.

Choose eigenvectors $v_0, \ldots, v_4$ of M_T defined over the field $K(\sqrt[5]{b})$ such that each v_i has eigenvalue $\sqrt[5]{b}\zeta_5^i$ and so the set $\{v_i\}$ is fixed under the action of $\mathrm{Gal}(K(\sqrt[5]{b}/K))$ (see Corollary 2.2).

Claim 4.1. *With the above notation, and with a possible permutation of the names of the v_i, $x_0 =$ and the map $\varphi_{x_0} = [\Phi^{-1}]$ is given by*

$$\Phi = (v_0\ \ \theta\, v_1\ \ \theta^2\alpha_2\, v_2\ \ \theta^3\alpha_3\, v_3\ \ \theta^4\alpha_4\, v_4),$$

where $\alpha_2 = -\dfrac{Q(v_1)}{B(v_0, v_2)}$, $\alpha_3 = -\dfrac{B(v_1, v_2)\alpha_2}{B(v_0, v_3)}$, $\theta^5 = -\dfrac{Q(v_0)}{\alpha_2\alpha_3 B(v_2, v_3)}$,

and $\alpha_4 = \dfrac{Q(v_0)\epsilon}{\theta^5 B(v_1, v_4)}$.

Proof. By Theorem 2.4 there are 25 choices of the base point x_0 which each give rise to a matrix Φ. Let us fix a choice of x_0. By Claim 2.3 we have $\lambda_{T,E}\,\varphi_{x_0} = \varphi_{x_0}\lambda_{T,C}$; in terms of matrices this means

$$\left[D\,\Phi^{-1}\right] = \left[\Phi^{-1}\,M_T\right] \Rightarrow [\Phi\,D] = [M_T\,\Phi]\,.$$

Write $\Phi = (w_0\,w_1\,w_2\,w_3\,w_4)$ for some vectors w_i. Then

$$\left[(w_0\,w_1\zeta_5\,w_2\zeta_5^2\,w_3\zeta^3\,w_4\zeta_5^4)\right] = [(M_Tw_0\,M_Tw_1\,M_Tw_2\,M_Tw_3\,M_Tw_4)]\,;$$

we conclude that the $w_i's$ are eigenvectors of M_T with distinct eigenvalues. In other words, they are multiples of the v_i from above, and once we have know for which j we have $w_0 = \mu v_j$, the other v_i's are fixed by checking eigenvalues.

Remark. We will see that once we fix j we have fixed x_0 up to translation by some multiple of T, since $\varphi_{x_0+T} = \lambda_{-T,E}\,\varphi_{x_0} = \lambda_{T,E}^{-1}\,\varphi_{x_0}$, and by the theorem multiplying Φ by D amounts to changing our choice of a fifth root of θ. Similarly changing j amounts to translating x_0 by some 5-torsion point independent of T.

With possible rescaling of Φ and relabeling of the v_i we may assume $w_0 = v_0$, w_1 is some multiple θ of v_1, w_2 is some multiple $\theta^2\alpha_2$ of v_2, w_3 is some multiple $\theta^3\,\alpha_3$ of v_3, and w_4 is some multiple $\theta^4\,\alpha_4$ of v_4. We may now compute the quadrics that define E, expanding in terms of the bilinear form B associated to Q[4] and defining $\alpha_0 = \alpha_1 = 1$:

$$\begin{aligned} Q_E(x) = Q(\Phi x) &= Q(v_0x_0 + \theta\,v_1x_1 + \theta^2\alpha_2\,v_2x_2 + \theta^3\alpha_3\,v_3x_3 + \theta^4\alpha_4\,v_4x_4) \\ &= \sum_{i=0}^{4} \theta^{2i}\,\alpha_i^2\,Q(v_i)\,x_i^2 + \sum_{0\le i\ne j\le 4} \theta^{i+j}\,\alpha_i\alpha_j\,B(v_i,v_j)\,x_ix_j. \end{aligned}$$

The quadrics in the orbit of Q_E under D also define E; define $Q_{E,k}(x)$ to be the quadric $Q_E(D^kx)$. We introduce new quadrics R_i to define E determined by the equations $\sum_{k=0}^{4}\zeta_5^{ik}Q_{E,k} = 5R_i$. Then we have

$$\begin{aligned} R_0 &= Q(v_0)x_0^2 + \theta^5\alpha_4B(v_1,v_4)x_1x_4 + \theta^5\alpha_2\alpha_3B(v_2,v_3)x_2x_3, \\ R_1 &= (Q(v_1)x_1^2 + \alpha_2B(v_0,v_2)x_0x_2 + \theta^5\alpha_3\alpha_4B(v_3,v_4)x_3x_4)\theta^2, \\ R_2 &= (\alpha_2^2Q(v_2)x_2^2 + \alpha_4B(v_0,v_4)x_0x_4 + \alpha_3B(v_1,v_3)x_1x_3)\theta^4, \\ R_3 &= (\theta^5\alpha_3^2Q(v_3)x_3^2 + B(v_0,v_1)x_0x_1 + \theta^5\alpha_2\alpha_4B(v_2,v_4)x_2x_4)\theta, \\ R_4 &= (\theta^5\alpha_4^2Q(v_4)x_4^2 + \alpha_3B(v_0,v_3)x_0x_3 + \alpha_2B(v_1,v_2)x_1x_2)\theta^3. \end{aligned}$$

Since the point $O_E = (1:1:1:1:0)$ is on E, are able to deduce the following:

From the equation $R_1(O_E) = 0$ we deduce the value $\alpha_2 = -\dfrac{Q(v_1)}{B(v_0,v_2)}$, from the equation $R_4(O_E) = 0$ the value $\alpha_3 = -\dfrac{B(v_1,v_2)\alpha_2}{B(v_0,v_3)}$, and from the equation $R_0(O_E) = 0$ the value $\theta^5 = -\dfrac{Q(v_0)}{\alpha_2\alpha_3B(v_2,v_3)}$. Scaling, the equation R_0 becomes

[4]Define $B(w,v) = Q(w+v) - Q(w) - Q(v)$.

$S_0 = x_0^2 - x_2x_3 + \dfrac{\theta^5\alpha_4 B(v_1,v_4)}{Q(v_0)}x_1x_4$. The R_i's generate a K-rational vector space; by their shapes we see each R_i is conjugated to a multiple of itself by any Galois element. In particular $\dfrac{\theta^5\alpha_4 B(v_1,v_4)}{Q(v_0)} \in K$, so for some $\epsilon \in K$ we can write $\alpha_4 = \dfrac{Q(v_0)\epsilon}{\theta^5 B(v_1,v_4)}$. Moreover by scaling x_4 by $\frac{1}{\epsilon}$ we can assume $\epsilon = 1$. □

Remarks. 1) We may freely divide by the values of Q and B on the vectors v_i : first, if for any i we had $Q(v_i) = 0$, then v_i would correspond to a fixed point on the curve C under M. Second, since $Q(v_i) \neq 0$,all the values of B in the equations $R_i(O_E) = 0$ for $i = 0, 1, 2$, and 3 are nonzero - moreover if both values of B in the equation $R_4(O_E) = 0$ were zero, then R_4 would be a reducible quadric. 2) We have two extra equations $R_2(O_E) = 0$ and $R_3(O_E) = 0$ from which we may infer identities on the Q and B values:

$$Q(v_1)Q(v_2)B(v_0,v_3) = -B(v_1,v_3)B(v_0,v_2)B(v_1,v_2) \text{ and}$$
$$Q(v_0)Q(v_3)B(v_1,v_2) = -B(v_0,v_1)B(v_2,v_3)B(v_0,v_3).$$

More generally,

Lemma 4.3. *For all i we have the following identities:*

$$\frac{Q(v_{i+1})Q(v_{i+2})B(v_i,v_{i+3})}{B(v_{i+1},v_{i+3})B(v_i,v_{i+2})B(v_{i+1},v_{i+2})} = \frac{Q(v_i)Q(v_{i+3})B(v_{i+1},v_{i+2})}{B(v_i,v_{i+1})B(v_{i+2},v_{i+3})B(v_i,v_{i+3})}$$

$$= -1.$$

Proof of Lemma. By the Remark on page 138, choosing a different x_0 is tantamount to cyclically permuting the indices of the v_i, and the columns of the associated matrix Φ would be similarly permuted and scaled by elements in $\overline{K}$. Note that identities such as those above are unaffected by scaling each v_i. □

By construction the first quadric S_0 defining E is given by $S_0 = x_0^2 - x_2x_3 + x_1x_4$. After scaling R_1 (using the definition of α_2) and defining $A = \dfrac{\theta^5\alpha_3\alpha_4 B(v_3,v_4)}{Q(v_1)} = \dfrac{B(v_1,v_2)B(v_3,v_4)Q(v_0)}{B(v_0,v_3)B(v_0,v_2)B(v_1,v_4)} = \dfrac{\prod_{i=0}^4 Q(v_i)}{\prod_{i=0}^4 B(v_i,v_i+2)}$ (by the above lemma multiplying by both terms when $i = 1$) we obtain $S_1 = x_1^2 - x_0x_2 + A\,x_3x_4$. After scaling R_2 we have the two coefficients $\dfrac{\alpha_4 B(v_0,v_4)}{\alpha_2^2 Q(v_2)}$ and $\dfrac{\alpha_3 B(v_1,v_3)}{\alpha_2^2 Q(v_2)}$; after expanding we see the latter is -1 by the above lemma; dividing A by the former simplifies $\dfrac{Q(v_0)Q(v_2)B(v_3,v_4)}{B(v_0,v_2)B(v_0,v_4)B(v_2,v_3)} = -1$ again by the lemma. We conclude that $S_2 = x_2^2 - x_1x_3 - A\,x_0x_4$. Scaling R_3 (and using the definition of the α_i and the above lemma when $i = 0$) we need only identify

the coefficient $\dfrac{alpha_2\alpha_4 B(v_2,v_4)}{\alpha_3^2 Q(v_3)} = \dfrac{Q(v_0)Q(v_1)B(v_2,v_4)}{B(v_0,v_2)B(v_0,v_1)B(v_1,v_4)} = -1$ by the lemma. We get $S_3 = x_3^2 - x_0x_1 - x_2x_4$. Finally, scaling R_4 and using the definition of α_3 we need only identify the coefficient $\dfrac{\theta^5\alpha_4^2 Q(v_4)}{\alpha_2 B(v_1,v_2)}$. Dividing this by A simplifies to $\dfrac{Q(v_1)Q(v_4)B(v_2,v_3)}{B(v_1,v_2)B(v_3,v_4)B(v_1,v_4)} = -1$ by the lemma, and we conclude $S_4 = -A\,x_4^2 + x_1x_2 - x_0x_3$. □

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models,*, Ergeb. Math. Grenzgeb. **21**, Springer-Verlag, Berlin, 1990.

[2] J. W. S. Cassels, *Lectures on Elliptic Curves,* London Mathematical Society Student Texts **24**, Cambridge University Press, Cambridge, 1991.

[3] T. Fisher, *On 5 and 7 Descents for Elliptic Curves*, Ph. D. thesis, Cambridge University, 2000.

[4] R. Hartshorne, *Algebraic Geometry,*, Graduate Texts in Mathematics **52**, Springer-Verlag, New York, 1977.

[5] S. An, S. Kim, D. Marshall, S. Marshall, W. McCallum, and A. Perlis, *Jacobians of Genus One Curves*, Journal of Number Theory, to appear.

[6] D. Mumford, *Abelian Varieties,* published for the Tata Institute of Fundamental Research, Oxford University Press, Oxford, 1970.

[7] ———, *Geometric Invariant Theory,* Ergeb. Math. Grenzgeb. **34**, Academic Press Inc., Berlin, 1965.

[8] Rodriguez-Villega, F., and Tate, J., *Jacobian of $y^2 = f(x)$ with f of degree 4*, `http://www.ma.utexas.edu/users/villegas/cnt/jac_ quart.gp` and *Jacobian of plane cubics*, `http://www.ma.utexas.edu/users/villegas/cnt/jac_cubic.gp`.

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Grad. Texts in Math. **106** Springer-Verlag, New York, 1986.

[10] A. Weil, *Remarques sur un mémoire d'Hermite*, Arch. Math. **5** (1954), 197–202.

[11] ———, *Euler and the jacobians of elliptic curves*, Arithmetic and geometry vol. I, Progr. Math. **35** (1983), 353–359.

Dept. of Mathematics, MIT, 77 Massachusetts Avenue, Cambridge, MA 02139.
E-mail address: `coneil@math.mit.edu`