Jacobians of Curves of Genus One

A thesis presented

by

Catherine Helen O'Neil

to

The Department of Mathematics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Mathematics

Harvard University
Cambridge, Massachusetts

April, 1999

Abstract

In this thesis we consider the passage from curves of genus one to their Jacobian elliptic curves. More specifically, given the equations for a curve of genus one, our goal is to produce equations for its Jacobian. To achieve this goal we endow our curve with the structure of a torsion point on its Jacobian. We study this structure in generality and then apply these considerations to the three cases where our curve is embedded in $\mathbb{P}^2, \mathbb{P}^4$, and $\mathbb{P}^1 \times \mathbb{P}^1$, and is endowed with a 3-, 5-, and 2-torsion point on its Jacobian.

Acknowledgments

I would like to thank my advisor, Barry Mazur, for giving me a really great problem and also some really great advising.

I am deeply indebted to Brian Conrad for a careful reading of my thesis and many very helpful comments.

My understanding of the mathematics in this thesis has benefited hugely through conversations with the many wonderful people surrounding me. I will list only some of them here: Adam Logan, Jordan Ellenberg, Benedict Gross, Tomas Klenke, William McCallum, Michael Roth, Ravi Vakil, and Nicholas Katz.

Finally, I would like to thank my parents, my husband, and my friend Kenneth Ribet for their unbounded support.

Contents

1 Introduction

The purpose of my thesis is to explore the passage from smooth curves of genus one defined over a field K to their Jacobian curves. Specifically I consider curves of genus one in certain multiprojective spaces and provide explicit equations for their Jacobians, provided that their Jacobians have certain level structure. I do this in the three cases of $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, and $\mathbb{P}^4$. This problem has been and is currently being worked on by a number of people. This includes Salmon, who in 1873 published a book which contains formulas that (unbenownst to him) give a more general theorem than the one below, albeit quite complicated and lengthy; also, Shepherd-Barron and Fisher are looking at the problem in $\mathbb{P}^4$; An, Hammond, Kim, Kim, Marshall, McCallum, and Perlis are curresntly writing a survey article which explains what is and what is not known about the problem. In particular, the problem has been completely solved in $\mathbb{P}^3$.

For the case of $\mathbb{P}^2$ we prove

Theorem 1.1 *Let C be a smooth curve of genus one over a field K. Assume K does not have characteristic 3 and that K contains a primitive 3rd root of unity. Let $f : C \to \mathbb{P}^2_K$ be a closed immersion over K and let $F_C(X, Y, Z)$ be the cubic defining C. Assume that the Jacobian E of C has a non-trivial rational three-torsion point $T \in E[3](K)$. After modifying f by a $K-$linear automorphism of $\mathbb{P}^2_K$ the cubic F_C is of the following form:*

$$F_C(X,Y,Z) = \alpha \cdot (b^2X^3 + bY^3 + Z^3) + \beta \cdot (bXY^2 + bX^2Z + YZ^2)$$
$$+ \gamma \cdot (bX^2Y + Z^2X + Y^2Z) + \delta \cdot (3XYZ),$$

for some elements $\alpha, \beta, \gamma, \delta, b \in K$. Then $E = Jac(C)$ is given by the cubic

$$F_E(X,Y,Z) = X^3 - Y^3 + [(\alpha b + \delta)^3 + \beta^3 b^2 + \gamma^3 b - 3(\alpha b + \delta)\beta\gamma b] \cdot Z^3$$
$$+(2\alpha b - 3\delta) \cdot XYZ,$$

with the origin of E given by $O_E = (1 : 1 : 0)$.

The general idea is as follows. We consider C as a principal homogeneous space for its Jacobian elliptic curve. Then the assumption that there is a non-trivial rational three-torsion point on E gives a fixed-point free action of order three on the curve C, namely translation by that point. We show that this action can be extended to a linear automorphism of the entire projective plane. Moreover, we determine a standard form for the matrix representing this action which fixes a standard form for the cubic giving C. Putting this action into standard form amounts to composing the original embedding of C with a K-automorphism of $\mathbb{P}^2_K$. We then abstractly embed E in $\mathbb{P}^2_K$ in such a way that, upon a choice of a special element x_0 of $C(L)$ for a suitable finite separable extension L of K, there exists a map φ (an isomorphism) from C to E over L which extends to a linear automorphism of $\mathbb{P}^2_L$. The x_0 we have chosen is the L-rational point which maps to the identity of the group law on E. In much the same way as we did with C, we standardize the embedding of E, thereby rigidifying the map φ. We may think of the above theorem as giving us two families; the first is a family of genus one curves, parameterized by the coefficients α, β, γ, and δ, which contains every curve of genus one whose Jacobian has a non-trivial rational three-torsion point and which has an embedding into $\mathbb{P}^2_K$ as a degree three curve. The second is the family of their Jacobians, and we find explicit formulas for a map between the two families over the field $L = K(x_0)$.

In analogous ways we find families of genus one curves over K containing every curve of genus one whose Jacobian has a non-trivial rational two (resp. five) -torsion point and which has an embedding into $\mathbb{P}^1_K \times \mathbb{P}^1_K$ (resp. $\mathbb{P}^4_K$) as a homogeneous $(2,2)$-form (resp. degree 5 curve), and we explicitly write down a map to the corresponding families of Jacobian curves after a suitable base extension.

2 Conventions

We will work over a fixed field K unless otherwise stated, with K_s a fixed separable closure of K and with $G_K = Gal(K_s/K)$. A *curve* defined over K is an smooth, proper K-scheme of dimension 1, which is geometrically connected over K. All curves are projective over K.

Let L be a field extension of K. The automorphism group of $\mathbb{P}^n_L$ defined over L is $PGL_{n+1}(L)$, and a matrix class represented by $M = (a_{i\,j})_{\,0 \le i,j \le n}$

acts on the point $(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(L)$ by sending it to

$$\left(\sum_{j=0}^{n} a_{0\,j} x_j \;:\sum_{j=0}^{n} a_{1\,j} x_j \;:\ldots:\sum_{j=0}^{n} a_{n\,j} x_j\right) \in \mathbb{P}^n(L).$$

In other words, we represent points as column vectors and multiply by matrices on the left. The column vector whose topmost non-zero entry is 1 associated to a point $x \in \mathbb{P}^n(L)$ will be denoted $vec(x)$: for example,

$$vec\,(2 : -2) = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Similarly, the point in projective space x corresponding to a vector v is denoted $x = proj(v)$.

All fiber products are assumed to take place over $Spec(K)$ when not otherwise indicated. If L is a field extension of K and X a $K-$ scheme, we will write $X \times_K L$ or $X \times L$ instead of $X \times_{Spec(K)} Spec(L)$.

For integers n_i and closed points P_i of C, a divisor $D = \sum n_i P_i$ has degree $\sum n_i\,[K(P_i) : K]$. $\mathrm{Div}^n_K(C)$ is the set of all divisors on C of degree n.

We will use the description of the Jacobian of a curve C as the abelian variety which coarsely represents the functor P^0_C which associates to a scheme $T \xrightarrow{q} Spec(K)$ the set

$$P^0_C(T) = \{L \in Pic\,(C \times T) \mid deg(L_t) = 0\,\forall\, t \in T\}/q^* Pic\,(T).$$

Theorem 1.1 on page 168 of [6] states:

Theorem *There is an abelian variety J over K and a morphism of functors $\iota : P^0_C \longrightarrow J$ such that $\iota : P^0_C(T) \longrightarrow J(T)$ is an isomorphism whenever $C(T)$ is nonempty.*

Indeed the Jacobian represents the functor $T \mapsto P^0_C(T_L)^{G_K}$, where L is any finite Galois extension of K such that $C(L)$ is nonempty. In the case of $T = Spec(K)$, we have an injective map $\iota : P^0_C(K) \longrightarrow J(K)$. We will sometimes write $J = \underline{Pic}^0_{C/K}$.

For n prime to the characteristic of K, ζ_n is understood to be a primitive nth root of unity in K_s. $\mathcal{O}$ is the origin of an elliptic curve, and $O(D)$ is the sheaf associated to the Cartier divisor D (see page 144 of [4]).

3 General Results

3.1 n-prepared genus one curves

For an integer $n > 2$, we define an "n-prepared genus one curve (over $\mathcal{S}$)" to be a triple

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

where $\mathcal{C} \xrightarrow{\pi} \mathcal{S}$ is a projective flat morphism whose fibers are smooth genus one curves, $\mathcal{L}$ is a degree n line bundle on $\mathcal{C}$ (in particular $\mathcal{L}_t$ is a degree n line bundle for every geometric fiber $\mathcal{C}_t$), and $\mathcal{T}$ is an S-section of exact order n of the Jacobian group scheme $\mathcal{J} \to \mathcal{S}$. Such a $\mathcal{J}$ exists by Theorem 8.1 of [6].

We define a "2-prepared genus one curve (over $\mathcal{S}$)" to be a triple

$$(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, (\mathcal{L}_1, \mathcal{L}_2), \mathcal{T}),$$

where $\mathcal{C} \xrightarrow{\pi} \mathcal{S}$ is a projective flat morphism whose fibers are smooth genus one curves, $\mathcal{L}_1$ and $\mathcal{L}_2$ are line bundles of degree two on $\mathcal{C}$ which are linearly inequivalent on all fibers, and $\mathcal{T} \in \mathcal{J}(S)$ has exact order 2.

Remark A. For n at least 3, 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 immersion is defined by a choice of basis of the module of global sections of the line bundle $\mathcal{L}$. Hence this embedding is only defined up the action of $\mathrm{Aut}(\mathbb{P}^{n-1}_{\mathcal{S}}) = \mathrm{PGL}_n(S)$. Similarly, a 2-prepared genus one curve over the spectrum of a local ring or a field $\mathcal{S}$ comes with an embedding of the curve $\mathcal{C}$ into $\mathbb{P}^1_{\mathcal{S}} \times \mathbb{P}^1_{\mathcal{S}}$ defined up the action of $\mathrm{Aut}(\mathbb{P}^1_{\mathcal{S}}) \times \mathrm{Aut}(\mathbb{P}^1_{\mathcal{S}})$. Note that this map only uses the data of $\mathcal{C} \xrightarrow{\pi} \mathcal{S}$ and the line bundle $\mathcal{L}$ (resp. $(\mathcal{L}_1, \mathcal{L}_2)$).

For $n \geq 3$ (resp. $n = 2$) we define a morphism of two n-prepared curves over $\mathcal{S}$

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

$$(\text{resp. } (\mathcal{C} \xrightarrow{\pi} \mathcal{S}, (\mathcal{L}_1, \mathcal{L}_2), \mathcal{T}) \xrightarrow{(f,(\alpha_1,\alpha_2))} (\mathcal{C}' \xrightarrow{\pi'} \mathcal{S}, (\mathcal{L}'_1, \mathcal{L}'_2), \mathcal{T}'))$$

to be a pair (f, α) (resp. $(f, (\alpha_1, \alpha_2))$) with:

1. $f : \mathcal{C} \longrightarrow \mathcal{C}'$ a morphism of schemes,
2. $\pi = \pi' \cdot f$,
3. $\alpha : \mathcal{L} \cong f^*\mathcal{L}'$ (resp. $\alpha_i : \mathcal{L}_i \cong f^*\mathcal{L}_i'$), and
4. the induced map of Jacobians $f^* : \mathcal{J}' \to \mathcal{J}$ sends T' to T.

Remark B. A morphism between two n-prepared genus one curves with $n \geq 3$ (resp. $n = 2$) induces a map between the spaces $\mathbb{P}(\pi_*(\mathcal{L}))$ and $\mathbb{P}(\pi_*(\mathcal{L}'))$ (resp. $\mathbb{P}(\pi_*(\mathcal{L}_i))$ and $\mathbb{P}(\pi_*(\mathcal{L}_i')))$ which we also call f; in the case where $\mathcal{S}$ is the spectrum of a local ring and we have fixed choices of bases of global sections of $\mathcal{L}$ and $\mathcal{L}'$, there is a unique map over $\mathcal{S}$ which extends f, which we also denote by f :

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\pi} & \mathbb{P}^{n-1}_{\mathcal{S}} \\ f\downarrow & & \downarrow f \\ \mathcal{C}' & \xrightarrow{\pi'} & \mathbb{P}^{n-1}_{\mathcal{S}} \end{array} \quad \left(\begin{array}{cccc} & \mathcal{C} & \xrightarrow{\pi} & \mathbb{P}^1_{\mathcal{S}} \times \mathbb{P}^1_{\mathcal{S}} \\ resp. & f\downarrow & & \downarrow f \\ & \mathcal{C}' & \xrightarrow{\pi'} & \mathbb{P}^1_{\mathcal{S}} \times \mathbb{P}^1_{\mathcal{S}} \end{array} \right).$$

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

For $n \geq 3$ (resp. $n = 2$), fix $\Lambda = (\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}, \mathcal{T})$ (resp.$(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, (\mathcal{L}_1, \mathcal{L}_2), \mathcal{T})$) an n-prepared curve of genus one. Let $\mathcal{J}$ be an elliptic curve over $\mathcal{S}$. Fix a principal homogeneous space action of $\mathcal{J}$ on Λ, i.e. a morphism

$$\lambda : \mathcal{C} \times_{\mathcal{S}} \mathcal{J} \to \mathcal{C}$$

which induces an isomorphism of $\mathcal{J}$ with the Jacobian of $\mathcal{C}$. Any $\mathcal{S}'$-valued point P of $\mathcal{J}$ gives us an $\mathcal{S}'$-morphism

$$\lambda_P = \lambda(-, P) : \mathcal{C}_{\mathcal{S}'} \times_{\mathcal{S}} \mathcal{S}' \to \mathcal{C}_{\mathcal{S}'}.$$

We say that $\tau \in$Aut$(\Lambda)(\mathcal{S}')$ "covers λ_P" (or τ is a "λ_P-morphism") if $\tau = (\lambda_P, \alpha)$. Let Aut$(\Lambda)(\mathcal{S}')$ be the set of $\mathcal{S}'$-morphisms of Λ to itself covering λ_P for some $P \in \mathcal{J}(\mathcal{S}')$. Aut$(\Lambda)$ is a contravariant functor. There is a natural map of functors

$$F : \mathrm{Aut}(\Lambda) \longrightarrow \mathcal{J}.$$

Claim 3.1 *For any n-prepared genus one curve Λ, the image of*

$$F : \mathrm{Aut}(\Lambda) \longrightarrow \mathcal{J}$$

is the functor associated to the finite group scheme $\mathcal{J}[n]$.

Proof. Given $(\lambda_P, \alpha) \in \mathrm{Aut}(\Lambda)(\mathcal{S}')$, we have $\alpha : \mathcal{L}_{\mathcal{S}'} \cong \lambda_P^* \mathcal{L}_{\mathcal{S}'} \cong P^{\otimes n} \otimes \mathcal{L}_{\mathcal{S}'}$, so $P \in \mathcal{J}[n](\mathcal{S}')$. For $P \in \mathcal{J}[n](\mathcal{S}')$, there will clearly exist an isomorphism $\alpha : \mathcal{L}_{\mathcal{S}'} \cong \lambda_P^* \mathcal{L}_{\mathcal{S}'}$. A similar proof works for $n = 2$.

For any $\mathcal{S}' \to \mathcal{S}$ we have the exact sequence

$$1 \longrightarrow H^0(\mathcal{S}', O_{\mathcal{S}}'^*) \longrightarrow \mathrm{Aut}(\Lambda)(\mathcal{S}') \longrightarrow \mathcal{J}[n](\mathcal{S}') \longrightarrow 1.$$

Remark C. An n-prepared genus one curve $\Lambda = (\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}, \mathcal{T})$ (resp. $(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, (\mathcal{L}_1, \mathcal{L}_2), \mathcal{T})$) comes with a canonical subset $F^*(\mathcal{T})(S)$ of $\mathrm{Aut}(\Lambda)(S)$, namely pullback of the element corresponding to $\mathcal{T}$ (in the isomorphism of $\mathcal{J}$ with the Jacobian of $\mathcal{C}$) by the functor F as in Claim 3.1. Moreover, by Remark B, if $\mathcal{S}$ is the spectrum of a local ring and we have fixed an embedding $f : \mathcal{C} \longrightarrow \mathbb{P}_{\mathcal{S}}^{n-1}$, there is a unique element of $F^*(\mathcal{T})(S) \subset \mathrm{Aut}(\Lambda)$ which extends the automorphism of Λ to $\mathbb{P}_{\mathcal{S}}^{n-1}$. We call this $\lambda_{\mathcal{T}}(f) = \lambda_{\mathcal{T}}$.

3.2 Setting up over a field

Let C be a smooth curve of genus one over a field K. All smooth curves of genus one defined over a finite field have a rational point, so they are isomorphic to their Jacobian. Thus we may assume K is infinite. Let $n \in \mathbb{N}$ be an integer with $n \geq 3$ (respectively $n = 2$), and suppose $L \in \mathrm{Pic}_K^n(C)$.

Remark A tells us that the global sections of L gives us a closed immersion (resp. a map)

$$f : C \longrightarrow \mathbb{P}_K^{n-1},$$

defined over K, embedding C as a curve of degree n in $\mathbb{P}_K^{n-1}$ (resp. exhibiting C as a double cover of $\mathbb{P}_K^1$) with $f^*(\mathcal{O}(1)) = L$. In fact there will be many such maps; fix one and call it f.

Let E be an elliptic curve over K and λ a principal homogeneous space action of E on C

$$\lambda : C \times_K E \longrightarrow C$$

which gives an isomorphism of E with the Jacobian $\mathcal{E} = \underline{Pic}^0_{C/K}$.

3.3 Translation by T

From now on it will be a standing assumption that n is relatively prime to the characteristic of K. Let $T \in E[n](K')$, for some field extension $K' \subset K_s$ of K. Then $(C_{K'}/K', L_{K'}, T)$ is an n-prepared genus one curve. Restricting the second coordinate of λ from above to T we get the "translation by T map"

$$\lambda_T = \lambda(-,T) : C \times_K K' \longrightarrow C \times_K K',$$

defined over K'.

Claim 3.2 *There exists a unique automorphism $\lambda_T : \mathbb{P}^{n-1}_{K'} \longrightarrow \mathbb{P}^{n-1}_{K'}$ defined over K' such that the following diagram commutes:*

$$\begin{array}{ccc} C \times_K K' & \xrightarrow{f} & \mathbb{P}^{n-1}_{K'} \\ \lambda_T \downarrow & & \downarrow \lambda_T \\ C \times_K K' & \xrightarrow{f} & \mathbb{P}^{n-1}_{K'} \end{array}.$$

Proof. This follows from Remark C on page 6.$\square$

From the above we get the following map:

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

$$T \longmapsto \lambda_T.$$

Claim 3.3 *χ is an injective Galois-invariant homomorphism.*

Proof. χ is injective because $E[n]$ acts faithfully on $C_K \times K_s$. χ is a homomorphism by uniqueness in Claim 3.2. Finally, χ is Galois-invariant because the maps λ and f are defined over K, so $\lambda_T^\sigma = \lambda_{T^\sigma}$. $\square$

Let $M_1, M_2 \in GL_n(K_s)$ be any matrices that lift the images under χ of any two points $T_1, T_2 \in E[n](K_s)$. Then the commutator $[M_1, M_2]$ does not depend on the lifts and is a scalar matrix of determinant 1, so is the identity matrix multiplied by some nth root of unity. Thus we have formed a pairing

$$e : E[n](K_s) \times E[n](K_s) \longrightarrow \mu_n(K_s)$$

which is visibly bilinear and alternating.

By Galois-invariance, e is induced by a bilinear alternating pairing of group schemes over K :

$$\chi : E[n] \times E[n] \longrightarrow \mu_n(K_s),$$

and this is clearly compatible with extensions of the base field.

Claim 3.4 *The above e is the Weil pairing, defined on page 183 of [7].*

Proof. We refine the section on the theta-group associated to a line bundle (pages 221-229 of [7]). A theta-group over K is a system of group schemes and homomorphisms

$$1 \longrightarrow \mathbb{G}_m \xrightarrow{i} G \xrightarrow{\pi} \mathcal{K} \longrightarrow 1$$

where

- $\mathcal{K}$ is commutative,
- $\exists$ an open covering $\{U_i\}$ of $\mathcal{K}$ and section σ_i of π,
- i is a closed immersion, making $\mathbb{G}_m$ into the kernel of π, and
- $\mathbb{G}_m \subset$ center of G.

Let Λ be an n-prepared genus one curve over the field K, and let E an elliptic curve which is isomorphic to the Jacobian of C. From page 6 we have the following exact sequence for any K-scheme S :

$$\epsilon(S) : 1 \longrightarrow H^0(S, O_S^*) \longrightarrow \mathrm{Aut}(\Lambda)(S) \longrightarrow E[n](S) \longrightarrow 1.$$

Theorem 1 on page 225 of [7] states that the functor $S \mapsto \epsilon(S)$ is representable by the theta group sequence associated to the line bundle L :

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{G}(L) \longrightarrow \mathcal{K}(L) \cong E[n] \longrightarrow 1.$$

On page 222 of [7], Mumford defines a skew-symmetric bihomomorphism $e : \mathcal{K} \times_K \mathcal{K} \to \mathbb{G}_m$ for any theta group, which he denotes by e^L in the case of the theta-group $\mathcal{G}(L)$. Using $\mathcal{K}(L) \cong E[n]$, this recovers the pairing e in our theorem. Finally, on page 228 [7], Mumford proves crucial properties of e^L; here the symbols x, y, etc. are to be understood as R-valued points for any $K-$algebra R, and the Weil pairing is denoted $\overline{e_n}$.

- For $x \in \mathcal{K}(L)$ and $y \in [n]^{-1}(\mathcal{K}(L))$, $e^{L^n}(x, y) = e^L(x, ny)$
- Define ϕ_L so that $[n]^{-1}(\mathcal{K}(L)) = \phi_L^{-1}(X[n])$. Then for $x \in E[n]$ and $y \in [n]^{-1}(\mathcal{K}(L)) = \phi_L^{-1}(X[n])$, $\overline{e_n}(x, \phi_L(y)) = e^{L^n}(x, y)$.

In our situation $\mathcal{K}(L) = E[n]$ and $\phi_L = [n]$ since L has degree n, so combining the two properties proves the theorem.□

3.4 Embedding E

Let $\Lambda = (C, L, T)$ (resp. $\Lambda = (C, (L_1, L_2), T)$ be an n-prepared (resp. 2-prepared) genus one curve over K, let $\mathcal{E}$ be the Jacobian of C, and let $T' = \frac{n\,(n-1)}{2} \cdot T \in \mathcal{E}[2](K)$. Using the K-action of $\mathcal{E}(K) = \underline{Pic}^0_{C/K}(K)$ on $\underline{Pic}^n_{C/K}(K)$, $L - T'$ (resp. $L_1 - T'$) $\in \underline{Pic}^n_{C/K}(K)$. Let $x_0 \in C(K_s)$ be such that

$$L - T' \cong \mathcal{O}(n \cdot x_0) \;\; (resp. L_1 - T' \cong \mathcal{O}(n \cdot x_0)).$$

$C \times K_s$ is an elliptic curve and to find x_0 we are asking for the inverse image of a specific point under the multiplication-by-n map.

We would like to have a map from the curve C to its Jacobian $\mathcal{E}$ which is a simple as possible. For example, we could ask for a linear automorphism of $\mathbb{P}^{n-1}$ defined over a field extension K' of K which takes C to $\mathcal{E}$. By Remark B on page 5, this will happen whenever we have an n-prepared genus one curve $\Lambda_{\mathrm{Jac}} = (\mathcal{E}, L_{\mathcal{E}}, T)$ and a morphism from Λ to Λ_{Jac} defined over K'. For an $x_0 \in C(K_s)$ as above there is a $K(x_0)$-morphism

$$\varphi_{x_0} : C \longrightarrow \mathcal{E}$$

which takes a point $x \in C(K_s)$ to the line bundle $\mathcal{O}(x - x_0) \in \mathcal{E}(K_s)$. Then $\varphi_{x_0}^*$ takes a line bundle $\mathcal{L}$ of degree d on $\mathcal{E}$ to $\mathcal{L}^{\Sigma} + d \cdot x_0$, a line bundle of degree d on C (we have identified $\mathcal{E}$ with its Jacobian by sending a line bundle $\mathcal{L}$ on $\mathcal{E}$ to the sum of its points $\mathcal{L}^{\Sigma}$). In order for φ_{x_0} to extend to a morphism from Λ to Λ_{Jac} we need an isomorphism

$$\alpha_{x_0} : L \cong \varphi_{x_0}^*(L_{\mathcal{E}}) \ \ (\text{resp.} \alpha_i : \mathcal{L}_i \cong f^*\mathcal{L}_i').$$

Define

$$L_{\mathcal{E}} = \mathcal{O}((n-1)O_{\mathcal{E}} + T')$$
$$(\text{resp.} (L_{\mathcal{E},1}, L_{\mathcal{E},2}) = (\mathcal{O}((n-1)O_{\mathcal{E}} + T'), L_2 \otimes L_1^{-1} \otimes \mathcal{O}(T))).$$

Using Remark A, fix an embedding $f_{\mathcal{E}}$ of $\mathcal{E}$ in $\mathbb{P}_K^{n-1}$ (resp. $\mathbb{P}_K^1 \times \mathbb{P}_K^1$) such that $f_{\mathcal{E}}^*(\mathcal{O}(1)) = L_{\mathcal{E}}$ (resp. $(pr_i \cdot f_{\mathcal{E}})^*(\mathcal{O}(1)) = L_{\mathcal{E},i}$). Then

$$\varphi_{x_0}^* L_{\mathcal{E}} \cong \mathcal{O}(L_{\mathcal{E}}^{\Sigma} + n \cdot x_0) \cong \mathcal{O}(n \cdot x_0 + T'),$$

so an α_{x_0} exists; by Remark B there is a unique extension of φ_{x_0} to $\mathbb{P}_{K(x_0)}^{n-1}$. We have proved

Claim 3.5 *With notation as above, let*

$$\Lambda = (C, L, T) \ \ \textit{and} \ \ \Lambda_{Jac} = (\mathcal{E}, \mathcal{O}((n-1)O_{\mathcal{E}} + T'), T)$$

be n-prepared genus one curves over K. Then there exists a unique element $\varphi_{x_0} \in PGL_n(K(x_0))$ so that the following diagram commutes:

$$\begin{array}{ccccccc} x & \underline{Pic}^1_{C/K} & = & C & \xrightarrow{f} & \mathbb{P}^{n-1}_{K(x_0)} \\ \bar{\downarrow} & \downarrow & & \varphi_{x_0}\downarrow & & \downarrow\varphi_{x_0} \\ (x-x_0) & \underline{Pic}^0_{C/K} & = & \mathcal{E} & \xrightarrow{f_{\mathcal{E}}} & \mathbb{P}^{n-1}_{K(x_0)} \end{array}.$$

Remark. The same Claim can be made for 2-prepared curves of genus one where $\Lambda = (C, (L_1, L_2), T)$ and $\Lambda_{\text{Jac}} = (\mathcal{E}, (L_{\mathcal{E},1}, L_{\mathcal{E},2}), T)$ are defined as above.

The above Claim motivates the following definition:

Definition 3.1 *For $n \geq 3$, given an n-prepared curve of genus one $\Lambda = (\mathcal{C}/\mathcal{S}, \mathcal{L}, \mathcal{T})$, let*

$$\Lambda_{Jac} = (\mathcal{E}/\mathcal{S}, \mathcal{O}((n-1)O_{\mathcal{E}} + \mathcal{T}'), \mathcal{T})$$

be the "Jacobian n-prepared genus one curve of Λ," where $\mathcal{E}$ is the Jacobian of $\mathcal{C}$ and where $\mathcal{T}' = \frac{n(n-1)}{2} \cdot \mathcal{T}$. Given a 2-prepared genus one curve $\Lambda_2 = (\mathcal{C}, (\mathcal{L}_1, \mathcal{L}_2), \mathcal{T})$, let

$$\Lambda_{2,Jac} = (\mathcal{E}/\mathcal{S}, (\mathcal{O}((n-1)O_{\mathcal{E}} + \mathcal{T}'), \mathcal{L}_2 \otimes \mathcal{L}_1^{-1} \otimes \mathcal{O}(\mathcal{T})), \mathcal{T})$$

be the "Jacobian 2-prepared genus one curve of Λ_2."

Remark. We are identifying $T \in \mathcal{E}[n](K)$ with its image under the canonical isomophism $\mathcal{E} \cong Jac(\mathcal{E})$. Moreover, if we have an elliptic curve $E \cong \mathcal{E}$, we can define $\Lambda_E = (E/K, \mathcal{O}((n-1)O_E + T'), T)$ using the isomorphsim $\mathcal{E} \cong_\lambda E \cong Jac(E)$.

If n is odd, then $T' = O_{\mathcal{E}}$, and the condition in Claim 3.5 on x_0 simplifies considerably:

$$L = \mathcal{O}(n \cdot x_0) \in Pic^n_K(C).$$

In other words, x_0 is a flex point in $\mathbb{P}^2$, and in general if $n = 2m+1$ in $\mathbb{P}^{2m}$ is a hyperosculation point, i.e. a geometric point on C of maximal tangency. This implies that $f_{\mathcal{E}}$ is defined over K even when T is not. Of course, φ_{x_0} will still only be defined over $K(x_0)$.

Recall that E is an elliptic curve over K and λ is a principal homogeneous space action of E on C

$$\lambda : C \times_K E \longrightarrow C$$

which gives an isomorphism of E with the Jacobian $\mathcal{E}$. We can represent the cohomology class of the pair (Λ, λ) in the cohomology group $H^1(G_K, E(K_s))[n]$ by the cocycle $x_0 - x_0^\sigma$ (see Theorem 2.2 on page 285 of [8]). The next Claim shows that it actually lifts to $H^1(G_K, E[n](K_s))$.

Claim 3.6 *With this choice of x_0, the 1-cocycle*

$$\xi : G_K \longrightarrow E[\overline{K}]$$
$$\xi : \sigma \longmapsto \sigma\phi \circ \phi^{-1} = x_0 - x_0^\sigma$$

lands in $E[n](K_s)$.

Proof. $n \cdot (x_0 - x_0^\sigma) \sim n \cdot x_0 - n \cdot x_0^\sigma \sim (L - T') - (L - T')^\sigma = 0$. Here we are using the rationality of L and T'. $\square$

3.5 Finding x_0

We have two good reasons for choosing x_0 as we did. First, It gives us a nice choice for an embedding of E, and second the resulting cocycle $x_0 - x_0^\sigma$ representing C in $H^1(G, E(\overline{K}))$ comes from $E[n](\overline{K})$. A third reason is that we can actually find x_0. To do this we study the geometry arising from the ambient $\mathbb{P}^{n-1}$ automorphisms and standardize the element $\lambda_T \in \mathrm{PGL}_n(K)$.

Lemma 3.2 *λ_T is diagonalizable over K_s.*

Proof. Lift λ_T to some matrix $N \in GL_n(K_s)$ so that $N^n - \kappa \cdot I = 0$ for some $\kappa \in K_s^*$. Since $x^n - \kappa \in K_s[x]$ is separable, N is semisimple and diagonalizable over K_s. $\square$

Now let M be a lift of λ_T such that $M \in GL_n(K)$. The eigenvectors of M correspond to fixed points of λ_T in $\mathbb{P}^{n-1}(K_s)$. Fix n points $\{p_0, p_1, \ldots p_{n-1}\}$ in $\mathbb{P}^{n-1}(K_s)$ fixed by M. We may assume the p_i are in general position, as λ_T is diagonalizable over K_s. Define $\mathbb{H}_i$ to be the unique hyperplane in $\mathbb{P}^{n-1}(K_s)$ containing all the p_j's except p_i.

Claim 3.7 *Let $\mathbb{H}_i, (0 \leq i \leq n-1)$ be as above. Then*

- *$\mathbb{H}_i$ intersects C in n distince $\overline{K}$-rational points, and as we vary i we get n^2 distinct $\overline{K}$-rational points.*

- *Call one such point x. Then x has the property that x_0 has in claim 3.5, namely*
$$L_{\overline{K}} = \mathcal{O}(\, n \cdot x + T' \,) \in Pic^n_{C/K}(\overline{K}).$$

Proof. First we will show the second part. Without loss of generality, let $i = 0$. $\mathbb{H}_0$ is parameterized by $\lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_{n-1} p_{n-1}$, and as each p_j is fixed by M, so is $\mathbb{H}_0$. For each x in $\mathbb{H}_0 \cap C$, $M \cdot x = x + T$ is also on $\mathbb{H}_0$. Fixing some $x \in \mathbb{H}_0 \cap C_{\overline{K}}$, $x + i \cdot T \in \mathbb{H}_0 \cap C_{\overline{K}}$, and so the degree n divisor $\mathbb{H}_0 \cap C_{\overline{K}}$ on $C_{\overline{K}}$ must be the sum of the n distinct points $x + i \cdot T$ so $\mathcal{O}(n \cdot x + \frac{n(n-1)}{2} \cdot T) = \mathcal{O}(n \cdot x + T') = L$.

To see why the n^2 points described above are distinct we will need the following lemma:

Lemma 3.3 *Any n distinct points of $C_{\overline{K}}$ do not lie in a codimension 2 hyperplane in $\mathbb{P}^{n-1}_{\overline{K}}$.*

Proof of Lemma. Say n points of $C(\overline{K})$ lie on a linear subspace V of codimension 2 in $\mathbb{P}^{n-1}_{\overline{K}}$. Let $p \in C_{\overline{K}} \setminus V$ be a closed point. There exists a hyperplane $\mathbb{H}$ containing p and V which intersects C at a divisor of degree $\geq n+1$, contradicting the fact that C is a degree n curve in $\mathbb{P}^{n-1}_K$.□

If x' is on two hyperplanes $\mathbb{H}_i$ and $\mathbb{H}_j$, then $x' + T$ is too, by the above argument, and so indeed the entire orbit of x', consisting of n distinct points, lies on $\mathbb{H}_i \cap \mathbb{H}_j$, contradicting Lemma 3.3.□

Corollary 3.4 *The eigenvalues of M are distinct.*

Proof. Assume not. Say $p_0 \neq p_1$ are fixed by λ_T and correspond to eigenspaces of M with the same eigenvalue. For $\mu \in \overline{K}$, let $\mathbb{H}_\mu$ be the hyperplane containing the $n-1$ points $\mu p_0 + (1-\mu)p_1$, p_2, $p_3, \ldots, p_{n-1}$. As above, $\mathbb{H}_\mu$ is fixed by λ_T and the intersection of $\mathbb{H}_\mu$ with C gives n points $x \in C(\overline{K})$ with the property $L_{\overline{K}} = \mathcal{O}(\, n \cdot x + T' \,)$. Over the algebraic closure of K there are clearly only n^2 such points (the above can be rewritten as $L_{\overline{K}} - \mathcal{O}(T') = \mathcal{O}(\,n \cdot x\,)$, and the map $[n]$ is finite étale with degree n^2). As we vary μ through infinitely many values of $\overline{K}$, we produce a set of n such points which lie in more than one of the $\mathbb{H}_\mu$'s, which contradicts Lemma 3.3. □

3.6 Standardizing λ_T

We say that an element of $\mathrm{PGL}_n(K)$ has distinct eigenvalues if a lift to $\mathrm{GL}_n(K)$ does. This is well-defined.

Claim 3.8 *Assume K is infinite. If $N \in PGL_n(K)$ has order n and if N has distinct eigenvalues, then there exists $G \in PGL_n(K)$ such that*

$$G^{-1}NG = \left[\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ b & 0 & 0 & 0 & \dots & 0 \end{pmatrix}\right],$$

where b is some lift to K^* of $det(N) \cdot (-1)^{n+1}$.

Proof. Lift N to $\tilde{N} \in GL_n(K)$. Define $b = det\,(\tilde{N}) \cdot (-1)^{n+1}$. Say we have a vector v in $\mathbb{A}^n_K$ such that the set of vectors

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

is a basis for $\mathbb{A}^n_K$. Then $\tilde{N}$ sends ω_i to ω_{i+1}, for $0 \leq i \leq n-1$, and sends $\omega_n = N^{n-1}v$ to $N \cdot N^{n-1}v = b \cdot v$. Such a change of basis corresponds to conjugating $\tilde{N}$ as in the statement of the Claim. We define G to be the image of the change of basis matrix in $\mathrm{PGL}_n(K)$. It remains to prove such a v exists. A vector whose orbit under $\tilde{N}$ does not span all of $\mathbb{A}^n_K$ correspond to a point of $\mathbb{P}^{n-1}$ which lies on one of the n hyperplanes $\mathbb{H}_i$ (see Claim 3.7), fixed by N. Take v to be any vector corresponding to a point off of these hyperplanes. Such a v exists since K is infinite. $\Box$

Remarks. Using the above Claim we will now modify the embedding f of C so that

$$\lambda_T = \left[\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ b & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \right].$$

In particular we see the fixed points p_i of λ_T are the n points

$$p_i = \left(1 \ : \ \sqrt[n]{b}\zeta_n^i \ : \dots : \ \sqrt[n]{b^{n-1}}\zeta_n^{(n-1)i}\right) \in \mathbb{P}^{n-1}(\overline{K}),$$

where ζ_n is a primitive nth root of unity. The eigenvalues of the corresponding vectors are the n distinct roots of $b = (-1)^{n-1} \cdot det(\lambda_T)$.

3.7 The invariant b

Starting with an n-prepared genus one curve $\Lambda/K = (C/K, L, T)$ we have the natural action $\lambda_T \in \mathrm{PGL}_n(K)$ on C as it is embedded in (multi-)projective space using the line bundle L. The invariant

$$b = (-1)^{n-1} \cdot det(\lambda_T)$$

arises from this action. We may write $b = b(\Lambda)$. The next section entitled "The map *det*" will interpret b via Galois cohomology but will not completely explain it, for the following reason.

Given the equation(s) of a genus one curve in (multi-)projective space, we would like a formula for its Jacobian. This is like being given the information of C/K and L, the first two parts of Λ. If we were also told that its Jacobian has a rational $n-$torsion point, we would not know how to construct λ_T, so we would not know what b is. This is so even though, given the equation of C, there are only n^2 possible order n fixed-point free actions on it. In other words, b is an invariant of the coefficients of the equations defining C but we have no formula for it. On the other hand b is vitally important and will appear in all of our formulas.

3.8 The map *det*

The following diagram illustrates the fact that elements of $PGL_n(K)$ have determinants which are well defined only up to to nth powers in K.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^* & \longrightarrow & GL_n(K) & \longrightarrow & PGL_n(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow det & & \downarrow det & & \\ 0 & \longrightarrow & (K^*)^n & \longrightarrow & K^* & \longrightarrow & K^*/(K^*)^n & \longrightarrow & 0 \end{array}$$

A different lifting $c \cdot \tilde{N}$ of $\tilde{N}$ in the proof of claim 3.8 will have $det\,(c \cdot \tilde{N}) = c^n \cdot det\,(N)$.

We now give a Galois cohomological interpretation of the det map. Let $\Lambda = (C/K, L, T)$ be an n-prepared genus one curve over the field K. From Λ we have the element $\lambda_T \in \mathrm{PGL}_n(K)$ (see page 7). Then define

$$det : \{\Lambda\} \longrightarrow K^*/K^{*n}$$

$$det : \Lambda \longmapsto det(\lambda_T).$$

We make use of the following short exact sequence (page 197 of [8])

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

Recall that λ (page 7) is a principal homogeneous space action of the elliptic curve E on C which induces an isomorphism of E with $\mathcal{E}$, the Jacobian of C. Then the pair (Λ, λ) is represented by an element in the cohomolgy group $H^1(G, E(\overline{K}))$. Moreover, (Λ, λ) has order dividing n in $H^1(G, E(\overline{K}))$ since the order of $C \cong \underline{Pic}^1_{C/K}$ is the least d such that $\underline{Pic}^d_{C/K}(K) \neq \emptyset$, and we have $L \in \underline{Pic}^n_{C/K}(K)$. Thus the pair (Λ, λ) is represented by an element in $H^1(G, E(\overline{K}))[n]$, the right-most group in the above exact sequence.

We can lift (Λ, λ) to the middle group, namely $H^1(G, E[n](\overline{K}))$, by representing (Λ, λ) by the class of the cocycle $x_0 - x_0^\sigma$, which takes values in $E[n](\overline{K})$ (see Claim 3.6). Recall that such an $x_0 \in C(\overline{K})$ satisfies the relation $\mathcal{O}(n{\cdot}x_0{+}T') \cong L$. 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. Thus we have a well-defined map

$$\{(\Lambda, \lambda)\} \longrightarrow H^1(G, E[n](\overline{K})).$$

Using $T \in \mathcal{E}[n](K)$ and the isomorphism $E \cong \mathcal{E}$ 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

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

Claim 3.9 *The composition map $e^* \circ l$ is $(-1)^{n-1} \cdot det$.*

Remark. This is not a group homomorphism.

Proof. Define $b = (-1)^{n-1} {\cdot} det(\lambda_T)$. We need to show that $(e^* {\circ} l\,)(C, D) = b$. 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 $x_0 - x_0^\sigma \in E(\overline{K})$. By definition, $(e^* \circ l\,)(\Lambda)$ 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 8, we have

$$e(x_0 - x_0^\sigma, T) \cdot I = S_\sigma \, T \, S_\sigma^{-1} \, T^{-1}.$$

In other words, for any σ, the matrix $S_\sigma\, T\, S_\sigma^{-1}\, T^{-1}$ is a multiple of the identity matrix; we need to prove that multiple is $\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$.

We can check this by seeing where one nonzero vector in $\mathbb{A}^n_{\overline{K}}$ is mapped by $S_\sigma\, T\, S_\sigma^{-1}\, T^{-1}$. We will choose this vector carefully. Let v_i be the vector associated to the fixed point p_i of λ_T (see Remark 3.6). Claim 3.7 implies that x_0 is on a hyperplane $\mathbb{H}$ containing $n-1$ of the p_i's. Relabeling if necessary, we may assume x_0 lies on the hyperplane containing $p_1, \ldots, p_{n-1}$. Define $v = v_n$. Then v is a vector whose projectivization is a fixed point of λ_T lying off of $\mathbb{H}$. We may assume that the eigenvalue of v is $\sqrt[n]{b}$ (see Remark 3.6).

Lemma 3.5 *For some* $\varepsilon \in \overline{K}^*$, $S_\sigma^{-1}(v) = \varepsilon \cdot v^\sigma$.

Proof. The fixed points p_i of λ_T are permuted both by "translation by n-torsion" matrices, since all such matrices commute (in $\mathrm{PGL}_n(\overline{K})$) with λ_T, and by elements of the Galois group G, since the set $\{p_i\}$ is Galois invariant (as T is rational).

S_σ^{-1} maps the point x_0 to x_0^σ, since S_σ is the n-torsion point $x_0 - x_0^\sigma$. More generally, S_σ^{-1} maps the point $x_0 + i \cdot T$ to $x_0^\sigma + i \cdot T = (x_0 + i \cdot T)^\sigma$, by commutativity of n-torsion points. Since the n distinct points $x_0 + i \cdot T$ generate the hyperplane $\mathbb{H}$, we know that the hyperplane $\mathbb{H}$ is mapped by S_σ^{-1} to $\mathbb{H}^\sigma$. That means that the fixed points p_1 through p_{n-1}, which are all on $\mathbb{H}$, are mapped by S_σ^{-1} to p_1^σ through p_{n-1}^σ. Then S_σ^{-1} must map p_n to p_n^σ, i.e. S_σ^{-1} maps v to $\varepsilon \cdot v^\sigma$ for some constant ε. $\square$

Now we see how the matrix $S_\sigma\, T\, S_\sigma^{-1}\, T^{-1}$ acts on the vector v. Since $T^{-1} v = v / \sqrt[n]{b}$, we reduce to showing $S_\sigma\, T\, S_\sigma^{-1}\, v = \sigma(\sqrt[n]{b})\, v$. By Lemma 3.5,

$$S_\sigma\, T\, S_\sigma^{-1}\, v = S_\sigma\, T\, \varepsilon \cdot v^\sigma = \varepsilon \cdot S_\sigma\, (T\, v)^\sigma \cdot = \varepsilon \cdot \sigma\left(\sqrt[n]{b}\right) \cdot S_\sigma\, v =$$

$$\sigma\left(\sqrt[n]{b}\right) \cdot \varepsilon \cdot \left(\frac{1}{\varepsilon} \cdot v\right) = \sigma\left(\sqrt[n]{b}\right)\, v.$$

$\square$

Identify $T \in E[n](K)$ with the image of $T \in \mathcal{E}[n](K)$ underthe canonical isomorphism $\mathcal{E} \cong E$. Recall that $T' = \frac{n(n-1)}{2} \cdot T$.

Corollary 3.6 *The map det satisfies the following properties:*

1. *The map* $e^* \circ \delta : E(K)/n\,E(K) \longrightarrow K^*/K^{*n}$ *given by the composition of the usual connecting map* δ *(page 16) in cohomology and the map* e^* *(page 17), can be rewritten as follows: let* $P \in E(K)$*, let* P' *be the point* $P + T'$*, let* $L_P \in Pic^n_{E/K}(K)$ *be the line bundle* $\mathcal{O}((n-1) \cdot O_E + P')$*, and let* $\Lambda_P = (E/K, L_P, T_E)$*. Then* $(e^* \circ \delta)(P) = (-1)^{n-1} det(\Lambda_P)$*.*

2. *If we fix* C/K *and* T *and vary* L*, then the image of*

$$(-1)^{n-1} \cdot det : \{(\Lambda = (C/K, L, T), \lambda)\} \longrightarrow K^*/K^{*n}$$

is a coset of the image of $e^* \circ \delta : E(K)/n\,E(K) \longrightarrow K^*/K^{*n}$*.*

Remark. If n is odd, $T' = \mathcal{O}_E$ so $P' = P$. Also, for n odd we have the simplified formula $(e^* \circ \delta)(P) = det(\Lambda_P)$.

Proof. The connecting map δ brings $P \in E(K)$ to the the class of the cocycle $S - S^\sigma$, where $S \in E(\overline{K})$ and $n \cdot S = P$. A lift of the pair (Λ_P, λ_E) (where λ_E is the obvious action) is the class of the cocycle $x_0 - x_0^\sigma$ such that $\mathcal{O}(n \cdot x_0 + T') \cong L_P$. We would like to see that $S = x_0$. This amounts to asking that $L_P \cong \mathcal{O}(P + T')$.

The difference of two lifts of $(\Lambda, \lambda) \in H^1(G, E)[n]$ to the group $H^1(G, E[n])$ is the image of an element of $E(K)$, because the short exact cohomology sequence (page 16) is exact.

3.9 The Model for E

We use the properties of the det map to further normalize the model for E.

Claim 3.10 *Let* E *be an elliptic curve defined over* K *and let* $T \in E[n](K)$ *be an element of exact order* n*. Let* $T' = \frac{n(n-1)}{2} \cdot T$*. Define the* n*-prepared curve*

$$\Lambda_E = (E/K, \mathcal{O}(n \cdot O_E + T'), T).$$

Then $det\,(\Lambda_E) = (-1)^{n-1}$*.*

Proof. We will use Claim 3.9 to compute $(-1)^{n-1} \cdot det\,(\Lambda_E)$. We first lift the trivial element (Λ_E, λ_E) (where λ_E is the obvious E-action on itself, namely addition) from $H^1(G, E(\overline{K}))[n]$ to $H^1(G, E[n](\overline{K}))$ to the class of the cocycle $x_0 - x_0^\sigma$ where $\mathcal{O}(n \cdot x_0 + T') \cong \mathcal{O}(n \cdot O_E + T')$. Since we can take x_0 to be O_E, we are lifting (Λ_E, λ_E) to the trivial element in $H^1(G, E[n](\overline{K}))$. The image of this in $K^*/K^{*\,n}$ is certainly 1. $\square$

Claim 3.11 *Let*

$$\Lambda_E = (E/K, L_E = \mathcal{O}(n \cdot O_E + T'), T)$$

be as in Claim 3.10. Assume $\zeta_n \in K$. We may choose an embedding f_E (see Remark A, page 4) associated to Λ so that $O_E = (1 : 1 : 1 : \ldots : 1 : 0)$, $i \cdot T = (1 : \zeta_n^i : \zeta_n^{2i} : \ldots : \zeta_n^{(n-2)i} : 0)$, and so that a lift of λ_T to $\mathrm{GL}_n(K)$ is

$$D = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & \zeta_n & 0 & \ldots & 0 \\ 0 & 0 & \zeta_n^2 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \zeta_n^{n-1} \end{pmatrix}.$$

Proof. Claims 3.10 and 3.8 show that there is a choice of f_E so that a lift to $\mathrm{GL}_n(K)$ of λ_T is

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

We would like to show that there is an element G of $\mathrm{GL}_n(K)$ which conjugates M to D. Using the fact that $(\mathrm{char}(K), n) = 1$, take G to be the matrix whose ith column is $vec(1 : \zeta_n^i : \zeta_n^{2i} : \ldots : \zeta_n^{(n-1)i})$. We now assume λ_T is the image in $\mathrm{PGL}_n(K)$ of D. If the coordinates of $\mathbb{P}^{n-1}$ are given by $x_0, \ldots, x_n$, the hyperplanes $\mathbb{H}_j$ (see page 12) fixed by D are defined by $x_j = 0$. Since $L_E = \mathcal{O}(n \cdot O_E + T')$, by Claim 3.7 we know that O_E and its distinct translates by T are on one such hyperplane, say $\mathbb{H}_j$. We can modify our embedding of E by composing it with M, thereby conjugating λ_T by M. Since M commutes with D and cyclically permutes the coordinates of $\mathbb{P}^{n-1}$, this has the net effect of translating j by one. We can thus assume that $j = n$. Therefore we have $i \cdot T \in \mathbb{H}_n \cap E$. We need only put $O_E = (1 : 1 : 1 : \ldots : 1 : 0)$, since we have already fixed D. To do so, it is enough to show the existence of a invertible matrix N which commutes with D (so that upon composition we do not lose the form of λ_T), fixes $\mathbb{H}_n$, and sends $(1 : 1 : 1 : \ldots : 1 : 0)$ to O_E. Any matrix of the form $N_\alpha = \alpha_0 \cdot I + \alpha_1 \cdot D + \ldots + \alpha_{n-1} \cdot D^{n-1}$ commutes with D and fixes $\mathbb{H}_n$. Moreover,

$$N_\alpha \cdot vec((1 : 1 : 1 : \ldots : 1 : 0)) = G^\tau \cdot vec((\alpha_0 : \alpha_1 : \ldots\ \alpha_{n-1} : 0)).$$

Since G^τ is invertible, we can choose the α_i's so that N_α sends $(1 : 1 : 1 : \ldots : 1 : 0)$ to O_E. $\square$

3.10 Jacobians of n-prepared genus one curves over $\mathcal{S}$

Given an n-prepared curve over a large base scheme $\mathcal{S}$ we would like to find its Jacobian. In some cases it is enough to find an elliptic curve over $\mathcal{S}$ whose generic fiber is the Jacobian of the generic fiber of the original curve. Indeed, Remark 1.10 on page 7 of [3] states that any morphism between abelian schemes defined over an open dense subset of a noetherian normal base scheme $\mathcal{S}$ extends to all of $\mathcal{S}$.

Say we have an n-prepared curve $(\mathcal{C} \xrightarrow{\pi} \mathcal{S}, \mathcal{L}, \mathcal{T})$ over a base scheme $\mathcal{S} = \mathrm{Spec}(K[x_1, \ldots, x_n]_\mathcal{P})$, the localisation of a polynomial algebra over a field. Say we also have an (n-prepared) elliptic curve $\mathcal{E}$ over $\mathrm{Spec}(K[x_1, \ldots, x_n])$ whose generic fiber is isomorphic to the Jacobian of the generic fiber of $\mathcal{C}$; moreover, assume there is a map from $\mathcal{E}$ to $\mathcal{C}$ which extends to a linear automorphism of $\mathbb{P}^{n-1}_{\overline{(K(x_1,\ldots,x_n))}}$; then $\mathcal{E}$ is actually smooth over $\mathcal{S}$. The isomorphism between the generic fibers $\mathcal{E}$ and the Jacobian of $\mathcal{C}$ extends to an open set of $\mathcal{S}$ and we can apply the above Remark 1.10 to conclude that $\mathcal{E}/\mathcal{S}$ is actually the Jacobian of $\mathcal{C}$.

4 Curves of genus one in $\mathbb{P}^2$

4.1 Main Theorem

Let K be a field with char(K) not divisible by 3. Assume that $\zeta_3 \in K$. For variables α, β, γ, and δ, define

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

over the base Spec$(K(\alpha,\beta,\gamma,\delta))$. Define $\mathcal{S}$ to be the largest open subscheme of Spec$(K(\alpha,\beta,\gamma,\delta))$ such that $F_{\mathcal{C}}$ defines a smooth flat genus one curve $\mathcal{C}$ over $\mathcal{S}$, embedded in $\mathbb{P}^2_{\mathcal{S}}$ by $f_{\mathcal{C}}$. Let $\mathcal{L} = f_{\mathcal{C}}^*(\mathcal{O}(1))$, and let $\mathcal{E}/\mathcal{S}$ be the Jacobian of $\mathcal{C}$. Note that the matrix

$$M_T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ b & 0 & 0 \end{pmatrix}$$

acts on $F_{\mathcal{C}}$ and thus on $\mathcal{C}$. Moreover, this action is of exact order n and has no fixed points on $\mathcal{C}$; thus it is of the form $\lambda_{\mathcal{T}}$ for some $\mathcal{T} \in \mathcal{E}[n](K)$ of exact order n. We have the n-prepared genus one curves $\Lambda = (\mathcal{C}/\mathcal{S}, \mathcal{L}, \mathcal{T})$ and $\Lambda_{\text{Jac}} = (\mathcal{E}/\mathcal{S}, \mathcal{O}(3 \cdot O_{\mathcal{E}}), \mathcal{T})$.

Theorem 4.1 *With notation as above, $\mathcal{E}$ is given by the cubic*

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

with $\mathcal{O} = (1 : -1 : 0)$.

4.2 Setting up over a field

Let K be a field with char(K) not divisible by 3 and with $\zeta_3 \in K$. Let $\Lambda = (C/K, L, T)$ be an n-prepared curve of genus one over K. Let $\mathcal{E}$ be the

Jacobian of C, and let $\Lambda_{\mathcal{E}} = (\mathcal{E}/K, L_{\mathcal{E}} = \mathcal{O}(3 \cdot O_{\mathcal{E}}), T)$ be the n-prepared Jacobian curve of Λ (see Claim 3.5). By Remark A (page 4), Λ comes with an embedding f of C into $\mathbb{P}^2_K$. By Claim 3.8, we may assume f is such that $\lambda_T \in \mathrm{PGL}_n(K)$ lifts to the matrix

$$M_T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ b & 0 & 0 \end{pmatrix}.$$

Note that b is the determinant of $\lambda_T \in PGL_3(K)$, and as such is only defined up to cubes in K^*. From the embedding f we get a cubic $F_C(X, Y, Z)$ which defines C in $\mathbb{P}^2_K$.

4.3 Standardizing F_C

Claim 4.1 *With notation as in Section 4.2, there exist α, β, γ, and $\delta \in K$ such that*

$$F_C(X, Y, Z) = \alpha \cdot (b^2 X^3 + bY^3 + Z^3) +$$
$$\beta \cdot (bXY^2 + bX^2 Z + YZ^2) + \gamma \cdot (bX^2 Y + Z^2 X + Y^2 Z) + \delta \cdot (3XYZ).$$

Proof. Consider the 10 dimensional vector space V over K generated by the monomials X^3, X^2Y, X^2Z, XY^2, XYZ, XZ^2, Y^3, Y^2Z, YZ^2, and Z^3. M_T acts on this vector space (M_T sends X to Y, Y to Z, and Z to bX) as a linear operator whose third power acts as multiplying by b^3. Therefore the eigenvalues of M_T on V must be in the set $\{b, \zeta_3 b, \zeta_3^2 b\}$. On the other hand it is clear that we have the following linearly independent eigenvectors:

eigenvector	eigenvalue
XYZ	b
$b^2\,\zeta_3^{2i} X^3 + b\,\zeta_3^i\, Y^3 + Z^3$	$b\,\zeta_3^i$
$b\,\zeta_3^i\, XY^2 + b\,\zeta_3^{2i}\, X^2 Z + YZ^2$	$b\,\zeta_3^i$
$b\,\zeta_3^i X^2 Y + \zeta_3^{2i} XZ^2 + Y^2 Z$	$b\,\zeta_3^i$

Since the equation F_C is fixed by the matrix M_T, F_C must be an element of one of the eigenspaces. Say that F_C lives in the eigenspace corresponding to the eigenvalue $b\,\zeta_3$. Every eigenvector listed above with eigenvalue $b\,\zeta_3$ vanishes at the fixed points of M_T, namely $(1; \sqrt[3]{b}\,\zeta_3^i; \sqrt[3]{b^2}\,\zeta_3^{2i})$. Thus F_C must also vanish at these points. But we know that "translation by T" has no fixed points on C. Thus F_C lives in the eigenspace corresponding to the eigenvalue b. $\square$

Remark. We have shown that every n-prepared curve of genus one over the field K is in the family $F_C(X,Y,Z) = \alpha\cdot(b^2X^3+bY^3+Z^3)+\beta\cdot(bXY^2+bX^2Z+YZ^2)+\gamma\cdot(bX^2Y+Z^2X+Y^2Z)+\delta\cdot(3XYZ)$. Let $K' = K(\alpha,\beta,\gamma,\delta,b)$. By Section 3.10 we can prove Theorem 4.1 by proving that $\Lambda\times_K K'$ has Jacobian $\Lambda_{\mathrm{Jac}}\times_K K'$. In other words, we will work over the field K' and treat $\alpha,\beta,\gamma,\delta$, and b as variables.

4.4 Standardizing F_E

Let E be an elliptic curve with a principal homogeneous action on C

$$\lambda : C\times E \longrightarrow C$$

which induces an isomorphism $\mathcal{E}\cong E$. Embed E in $\mathbb{P}^2_{K'}$ by the line bundle $\mathcal{O}(3\cdot O_E)$. Call this embedding f_E. We now have the n-prepared genus one curve $\Lambda_E = (E/K', L_E, T)$ (see the Remark after Definition 3.1). By Claim 3.11, we may assume that the "translation by T on E" matrix class is represented by

$$D = \begin{pmatrix} 1 & 0 & 0\\ 0 & \zeta_3 & 0\\ 0 & 0 & \zeta^2 \end{pmatrix}$$

and that the origin O_E of E in $\mathbb{P}^2$ is $(1;-1;0)$.

Claim 4.2 *Let F_E be the cubic defining E in $\mathbb{P}^2_{K'}$. Then F_E is of the form*

$$F_E = R_1\cdot X^3 + R_2\cdot Y^3 + R_3\cdot Z^3 + R_4\cdot XYZ.$$

Proof. The proof is as in the argument as for Claim 4.1, where the eigenvectors of the linear operator D are the monomials X^3, Y^3, Z^3, and XYZ, and the eigenvalues are the cube roots of unity.

Remark. Going one step further, if we assume that we have another 3−torsion point S which is linearly independent of T and is K'−rational, we can standardize the matrix class of λ_S to be represented by the matrix

$$M_S = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

(proof omitted). The argument of Claim 4.1 tells us E must also be of the form

$$F_E = S_1 \cdot (X^3 + Y^3 + Z^3) + S_2 \cdot (X^2Y + Y^2Z + Z^2X) + \\ S_3 \cdot (XY^2 + YZ^2 + ZX^2) + S_4 \cdot XYZ.$$

Altogether we find that

$$F_E = A \cdot (X^3 + Y^3 + Z^3) + B \cdot XYZ.$$

This is a well-known model for the universal elliptic curve over $Y(3)$, i.e. the moduli space of elliptic curves with full 3-torsion. In our case we only assume one K'−rational 3-torsion point T.

4.5 Finding x_0

Let $\Lambda = (C/K', L, T)$ and $\Lambda_E = (E/K', L_E \cong \mathcal{O}(3 \cdot O_E), T)$ be as above. Let "translation by T on C" be represented by M_T as above, and recall that $b \in K'^*/(K'^*)^3$ is the determinant of $\lambda_T \in PGL_3(K')$. Let "translation by T on E" be represented by D as above, and let $O_E = (1; -1; 0)$.

By Claim 3.5 we are assured of a linear automophism φ_{x_0} of $\mathbb{P}^2_{K'(x_0)}$ bringing C to E. To find φ_{x_0} we must first locate the point $x_0 \in C(\overline{K'})$ in $\mathbb{P}^2(\overline{K'})$ which maps to O_E via φ_{x_0}. Claim 3.7 tells us two ways of searching: first, x_0 is a flex point of the curve C. Unfortunately this seems hard to compute. Second, x_0 is a $\overline{K'}$-point of the intersection of C with a hyperplane $\mathbb{H} \subset \mathbb{P}^2$ defined by the property that it contains two of the fixed points $p_i = (1 : \sqrt[3]{b} \cdot \zeta_3^i : \sqrt[3]{b^2} \cdot \zeta_3^{2i})$ (for$0 \leq i \leq 2$) of M_T. An alternative definition of $\mathbb{H}$ is that it is a hyperplane (a $\overline{K'}-$ point of the dual of $\mathbb{P}^2$) which is fixed by M. There are 3 such $\mathbb{H}$'s. For $0 \leq i \leq 2$, let

$$v_i = \begin{pmatrix} 1 \\ \sqrt[3]{b}\zeta_3^i \\ \sqrt[3]{b^2}\zeta_3^{2i} \end{pmatrix}$$

be vectors corresponding to the fixed points p_i of M, and let $\mathbb{H}$ be the unique hyperplane containing the fixed points p_1 and p_2. Then a $\overline{K'}-$point x of $\mathbb{H}$ will be of the form $proj(\theta_1 \cdot v_1 + \theta_2 \cdot v_2)$.

Choose $\theta \in \overline{K'}$ so that the entries of the vector $v_1 - \theta \cdot v_2$ are all in $K'(x_0)$ and so that $x_0 = proj(v_1 - \theta \cdot v_2)$. Note that we may assume $\theta_1 \neq 0$ since $x_0 \in C(\overline{K'})$ is not fixed by λ_T. Then we have

$$x_0 + T = \lambda_T \cdot x_0 = proj(M_T \cdot (v_1 - \theta \cdot v_2)) =$$

$$proj(v_1\,\zeta_3 - \theta \cdot v_2\,\zeta_3^2) = proj(v_1 - \theta \cdot v_2\,\zeta_3)$$

and similarly we have $x_0 + 2T = proj(v_1 - \theta \cdot v_2\,\zeta_3^2)$. The fact that these points all lie on C means that

$$F(v_1 - \zeta_3^i \cdot \theta \cdot v_2\,) = 0, \quad 0 \leq i \leq 2.$$

For any cubic form G, $G(v + \zeta_3^i w) = 0 \;\; \forall i \Rightarrow G(v) + G(w) = 0$. This additive property can be checked on the elementary forms $X^3, X^2Y, XYZ, \ldots$. This means that $F(v_1) - \theta^3 \cdot F(v_2) = 0$, from which we conclude:

Claim 4.3

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

Claim 4.4

$$K'(x_0) = K'(\theta, \sqrt[3]{b}) \overset{3}{\supset} K'(\sqrt[3]{b}) \overset{3}{\supset} K'.$$

Proof. Clearly x_0 is defined over $K'(\theta, \sqrt[3]{b})$. Moreover, both $\sqrt[3]{b}$ and θ are in $K'(x_0)$: $x_0 + T$ and $x_0 + 2T$ are defined over $K'(x_0)$ (since T is K'-rational), so

$$\sum_{i=0}^{2}(v_1 - \theta \cdot v_2\,\zeta_3^i\,) = -3\,v_1$$

is defined over $K'(x_0)$. This implies that $\sqrt[3]{b} \in K'(x_0)$. Next, $(v_1 - \theta \cdot v_2) - v_1 = -\theta \cdot v_2$ is defined over $K'(x_0)$, so $\theta \in K'(x_0)$. $\square$

4.6 Finding φ_{x_0}

Let the notation be as in Section 4.5. In particular we have

$$i \cdot T = (1; -\zeta_3^i; 0) \in E[3](K').$$

We have determined that

$$x_0 + i \cdot T = proj(v_1 - \theta \cdot v_2 \cdot \zeta_3^i), \text{ where } v_i = \begin{pmatrix} 1 \\ \sqrt[3]{b}\zeta_3^i \\ \sqrt[3]{b^2}\zeta_3^{2i} \end{pmatrix} \text{ and } \theta^3 = \frac{F(v_1)}{F(v_2)}.$$

Using Claim 3.5 we know

$$\varphi_{x_0} : C \longrightarrow E$$

$$\varphi_{x_0} : (x_0 + i \cdot T) \mapsto i \cdot T.$$

Also by Claim 3.5, we know φ_{x_0} is representable by a matrix which we will denote for ease of computation by $\Phi_{x_0}^{-1} \in \mathrm{GL}_n(K'(x_0))$. Then from the above we have

$$\Phi_{x_0}^{-1}(v_1 - \theta \cdot v_2 \cdot \zeta_3^i) = \begin{pmatrix} 1 \\ -\zeta_3^i \\ 0 \end{pmatrix} \Longleftrightarrow v_1 - \theta \cdot v_2 \cdot \zeta_3^i = \Phi \cdot \begin{pmatrix} 1 \\ -\zeta_3^i \\ 0 \end{pmatrix}.$$

We conclude that Φ is of the form

$$\Phi = \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix},$$

for $h_i \in K'(x_0)$, $0 \leq i \leq 2$.

Claim 4.5 *Let $L \subset K'_s$ be the Galois closure of $K'(x_0)$ over K'. Let $\sigma \in Gal(L/K')$ be such that $\sigma(\sqrt[3]{b}) = \sqrt[3]{b}$ and $\sigma(\theta) = \theta \cdot \zeta_3^2$. The automorphism $\varphi^\sigma \varphi^{-1}$ of E is "translation by T."*

Proof of Claim. Such a σ exists since b and $\theta^3 = \frac{F(v_1)}{F(v_2)}$ are transcendental over K. By construction the automorphism $\varphi^\sigma \varphi^{-1}$ is translation by something, so we just need to see where the origin goes: $\varphi^\sigma \varphi^{-1} \mathcal{O} = \varphi^\sigma x_0 = \sigma(\Phi^{-1}) \cdot x_0 = \sigma(\Phi^{-1} \sigma^{-1} x_0) = \sigma(\Phi^{-1}(x_0 + T)) = \sigma T = T$. $\square$

The above Claim tells us that "translation by T on E" is given by the matrix class of $\sigma(\Phi^{-1})\Phi$; on the other hand, we have fixed "translation by T on E" to be represented by the matrix D. We have the following equality for some constant $\kappa \in K'(x_0)$:

$$\kappa \cdot D = \sigma(\Phi^{-1})\, \Phi \Longleftrightarrow \kappa \cdot \sigma(\Phi)\, D = \Phi,$$

so

$$\kappa \cdot \sigma \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{pmatrix} = \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix} \Longrightarrow$$

$$\kappa \cdot \begin{pmatrix} & & \zeta_3^2 \sigma(h_1) \\ v_1 & \theta \cdot v_2 & \zeta_3^2 \sigma(h_2) \\ & & \zeta_3^2 \sigma(h_3) \end{pmatrix} = \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix},$$

from which we conclude

$$\sigma(h_i) = \zeta_3 \cdot h_i.$$

Claim 4.6 *Let $\sigma \in Gal(L/K')$ be as in Claim 4.5, i.e. such that $\sigma(\sqrt[3]{b}) = \sqrt[3]{b}$ and $\sigma(\theta) = \theta \cdot \zeta_3^2$. The automorphism $\varphi_{x_0}^{-1} \varphi^\sigma$ of C is "translation by T."*

Proof. This is similar to the proof of Claim 4.5. $\square$

Thus we have λ_T on C represented two different ways, namely by M_T and by $\Phi\, \sigma(\Phi^{-1})$; for some $\kappa \in K'(x_0)$ we have

$$\kappa \cdot M_T = \Phi\, \sigma(\Phi^{-1}) \iff \kappa \cdot M_T\, \sigma(\Phi) = \Phi \iff$$

$$\kappa \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ b & 0 & 0 \end{pmatrix} \cdot \sigma \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix} = \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix} \iff$$

$$\kappa \cdot \begin{pmatrix} & & \sigma(h_2) \\ \sqrt[3]{b}\,\zeta_3 \cdot v_1 & \theta \cdot \sqrt[3]{b}\,\zeta_3^2 \cdot v_2 \cdot \zeta_3^2 & \sigma(h_3) \\ & & b \cdot \sigma(h_1) \end{pmatrix} = \begin{pmatrix} & & h_1 \\ v_1 & \theta \cdot v_2 & h_2 \\ & & h_3 \end{pmatrix}$$

We conclude from this that $\kappa = \frac{1}{\sqrt[3]{b}\,\zeta_3}$,

$$h_3 = \sqrt[3]{b^2}\,\zeta_3^2 \cdot \sigma(h_1) = \sqrt[3]{b^2} \cdot h_1, \text{ and}$$

$$h_2 = \sigma(h_3)/(\sqrt[3]{b}\,\zeta_3) = h_3/\sqrt[3]{b} = \sqrt[3]{b} \cdot h_1.$$

Replacing h_2 and h_3 by multiples of h_1, we see that the third column of Φ is the vector v_0 multiplied by h_1. In fact we have

Claim 4.7

$$\Phi = \begin{pmatrix} v_1 & \theta \cdot v_2 & \theta^2 \cdot v_0 \cdot l \end{pmatrix},$$

for some $l \in K'(\sqrt[3]{b})$.

Proof. We know that $\sigma(h_1) = \zeta_3 \cdot h_1$. Since by definition $\sigma(\theta^2) = \zeta_3 \cdot \theta^2$, the ratio $h_1/\theta^2 \in K'(x_0)$ is fixed by all elements in $\mathrm{Gal}(K'_s/K'(\sqrt[3]{b}))$. Therefore $h_1/\theta^2 \in K'(\sqrt[3]{b})$. Write $h_1 = \theta^2 \cdot l$ for some $l \in K'(\sqrt[3]{b})$. $\square$

Claim 4.8 $l\,/\,F(v_2) \in K'$.

Proof. Fix a cubic form F_C defining C in $\mathbb{P}^2_{K'}$ with coefficients in K'. Define the map F_C on vectors so that, for a point $x \in \mathbb{P}^2(K'_s)$, $F_C(vec(x)) = F_C(x)$. For vectors A, B, and C, define the trilinear form $\mathcal{T}$ as $\mathcal{T}(A,B,C) = F(A+B+C) - F(A+B) - F(A+C) - F(B+C) + F(A) + F(B) + F(C)$. We will use the equality

$$\begin{aligned} F(A+B+C) &= \mathcal{T}(A,B,C) + F(A+B) + F(A+C) + F(B+C) \\ &\quad - F(A) - F(B) - F(C) \end{aligned} \tag{1}$$

We are going to use the fact that F_E has coefficients defined over K' and that F_E is of a special form (see Claim 4.2). Indeed, we can find F_E since for a point $(x : y : z) \in \mathbb{P}^2_{K'_s}$,

$$F_E(x : y : z) = 0 \iff F_C(\varphi^{-1}(x : y : z)) = 0 \iff$$

$$F_C(\Phi \cdot vec(x : y : z)) = 0 \iff F_C(x \cdot v_1 + y \cdot v_2\, \theta + z \cdot v_0\, \theta^2\, l) = 0.$$

Using the trilinear form associated to F_C, we have

$$F_C(x \cdot v_1 + y \cdot v_2 \theta + z \cdot v_0 \theta^2 l) =$$

$$\mathcal{T}(x \cdot v_1, y \cdot v_2\theta, z \cdot v_0\theta^2 l) + F(x \cdot v_1) + F(y \cdot v_2\theta) + F(z \cdot v_0\theta^2 l) =$$

$$\theta^3\, l \cdot xyz \cdot \mathcal{T}(v_1, v_2, v_0) + x^3 \cdot F(v_1) + \theta^3 \cdot y^3 \cdot F(v_2) + \theta^6\, l^3 \cdot z^3 \cdot F(v_0).$$

The other terms drop out because of Claim 4.2. Dividing by $F(v_1)$ we have proved

$$F_E(X, Y, Z) = X^3 + B \cdot Y^3 + C \cdot Z^3 + D \cdot XYZ,$$

with

- $B = \theta^3 \cdot F(v_2)/F(v_1) = 1$,
- $C = \theta^6\, l^3 \cdot F(v_0)/F(v_1) = l^3 \cdot F(v_0)F(v_1)/F(v_2)^2$, and
- $D = \theta^3\, l \cdot \mathcal{T}(v_1, v_2, v_0)/F(v_1) = l \cdot \mathcal{T}(v_1, v_2, v_0)/F(v_2)$.

Note that

$$C = D^3 \cdot \frac{F(v_0)F(v_1)F(v_2)}{\mathcal{T}(v_1, v_2, v_0)^3},$$

so we have

$$F_E(X, Y, Z) = X^3 + Y^3 + D^3 \cdot \frac{F(v_0)F(v_1)F(v_2)}{\mathcal{T}(v_1, v_2, v_0)^3} \cdot Z^3 + D \cdot XYZ;$$

$D \in K'$ since the coefficients of F_E are K'-rational, so if we change Z by a multiple of D we get

$$F_E(X, Y, Z) = X^3 + Y^3 + \frac{F(v_0)F(v_1)F(v_2)}{\mathcal{T}(v_1, v_2, v_0)^3} \cdot Z^3 + XYZ.$$

Remark. Note that the Galois group $Gal(L/K')$ permutes the v_i's. Thus both the denominator and numerator of $\frac{F(v_0)F(v_1)F(v_2)}{\mathcal{T}(v_1,v_2,v_0)^3}$ are rational. In fact this shows that $\mathcal{T}(v_1,v_2,v_0) \in K'$.

We have proven

Theorem 4.2 *Define $C \subset \mathbb{P}^2_{K'}$ by the cubic*

$$F_C(X,Y,Z) = \alpha \cdot (b^2X^3 + bY^3 + Z^3) + \beta \cdot (bXY^2 + bX^2Z + YZ^2)$$

$$+\gamma \cdot (bX^2Y + Z^2X + Y^2Z) + \delta(3XYZ).$$

If E is an elliptic curve over K' isomorphic to the Jacobian of C, there is a model for E in $\mathbb{P}^2_{K'}$ given by

$$F_E(X,Y,Z) = X^3 + Y^3 + \frac{F_C(v_0)F_C(v_1)F_C(v_2)}{\mathcal{T}(v_1,v_2,v_0)^3} \cdot Z^3 + XYZ.$$

with

$$O_E = \begin{pmatrix} 1 & -1 & 0 \end{pmatrix}$$

and a map

$$\varphi : C \longrightarrow E$$

$$\varphi : x \longmapsto \mathcal{O}(x - x_0)$$

is given by the class of the matrix Φ^{-1}, where

$$\Phi = \begin{pmatrix} v_1 & \theta \cdot v_2 & \theta^2\, v_0 \cdot F_C(v_2)/\mathcal{T}(v_1,v_2,v_0) \end{pmatrix}, \quad v_i = \begin{pmatrix} 1 \\ \sqrt[3]{b}\zeta_3^i \\ \sqrt[3]{b^2}\zeta_3^{2i} \end{pmatrix},$$

$\theta^3 = \frac{F_C(v_1)}{F_C(v_2)}$, *and where $\mathcal{T}$ is the trilinear form associated to F (see page 29). We have*

$$F_E(X,Y,Z) = X^3+Y^3+\frac{(\alpha b+\delta)^3 + \beta^3 b^2 + \gamma^3 b - 3(\alpha b+\delta)\beta\gamma b}{(3(2\alpha b-\delta))^3} \cdot Z^3 + XYZ.$$

So far, we have only fixed $\mathcal{O}$ and the image of T, namely the matrix D. There is still some freedom in choosing the model for E. A concrete way to see this ambiguity is by composing Φ with the matrix $N_c = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & c' \end{pmatrix}$, for $c \in K'$. N_c conjugates the cocyle $\varphi^\sigma \varphi^{-1}$:

$$\sigma(\Phi \cdot N_c)^{-1}(\Phi \cdot N_c) = N_c^{-1} \cdot (\sigma\Phi^{-1}\Phi) \cdot N_c$$

A cocycle matrix will be fixed if it commutes with N_c. Since the matrix D commutes with N_c and $\mathcal{O}$ is fixed by N_c, a choice of c will fix the model of E and the image of χ.

4.7 Main Theorem with $\zeta_3 \notin K$

Corollary 4.1 *Let notation be as in Section 4.1 with the exception of having $\zeta_3 \in K$ (and thus in K'). $\mathcal{E}$ is given by the cubic $F_{\mathcal{E}}(X,Y,Z) =$*

$$(3H+G)(X^3+Y^3+Z^3)+(3G-3H)(X^2Y+XY^2+Y^2Z+YZ^2+Z^2X+ZX^2)$$
$$+(3H+2G)(3XYZ),$$

- $\mathcal{O} = \begin{pmatrix} 1 & -1 & 0 \end{pmatrix}$,
- $G = (\alpha b + \delta)^3 + \beta^3 b^2 + \gamma^3 b - 3(\alpha b + \delta)\beta\gamma b$, *and*
- $H = (3(2\alpha b - \delta))^3$.

Proof. Assume that $\zeta_3 \notin K$. Let σ be the nontrivial Galois element of $\mathrm{Gal}(K'(\zeta_3)/K')$. We work with an elliptic curve E which is K'-isomorphic to $\mathcal{E}$. For a field extension L of K' let E_L be the Jacobian of $C \otimes_{K'} L$ over the field L. Then $E_{K'(\zeta_3)} \cong E_{K'} \otimes_{K'} K'(\zeta_3)$; this isomorphism will be realized as a linear automorphism of $\mathbb{P}^2_{K'(\zeta_3)}$, so for some $W \in \mathrm{PGL}_3(K'(\zeta_3))$, we have:

$$\begin{array}{ccccc} C \otimes K'(\zeta_3) & \xrightarrow{\varphi} & E_{K'(\zeta_3)} & \xrightarrow{W} & E_{K'} \otimes_{K'} K'(\zeta_3) \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{P}^2_{K'(\zeta_3)} & \xrightarrow{\varphi} & \mathbb{P}^2_{K'(\zeta_3)} & \xrightarrow{W} & \mathbb{P}^2_{K'(\zeta_3)} \end{array}.$$

Using Claim 3.10 we can assume the "translation by T on E" matrix is of the form

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

and so F_E has the following form (see the proof of Claim 4.1):

$$F_E(X,Y,Z) = j(X^3+Y^3+Z^3) + k(X^2Y+Y^2Z+Z^2X)+$$
$$l(XY^2+YZ^2+ZX^2)+mXYZ.$$

Claim 4.9 *Let $(E/K', \mathcal{O}(3O_E), T)$ be a 3-prepared elliptic curve, and assume that we have embedded E (via Remark A) in $\mathbb{P}^2_{K'}$ such that the "translation by T on E" matrix class is represented by*

$$M_E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

We can modify the embedding $f : E \longrightarrow \mathbb{P}^2_{K'}$ by a $K'-$linear automorphism of $\mathbb{P}^2_{K'}$ so that M_E is as unaffected and $\mathcal{O} = (1:-1:0)$.

Proof. $\mathcal{O}$ is one of the nine flex points on the embedded curve, since $f^*\mathcal{O}(1) = \mathcal{O}(3O_E)$. By the same argument as in Section 4.5, we can write $O_E = proj(v_1 - \theta v_2)$, where

$$v_1 = \begin{pmatrix} 1 \\ \zeta_3 \\ \zeta_3^2 \end{pmatrix} \quad \text{and} \quad v_2 = \begin{pmatrix} 1 \\ \zeta_3^2 \\ \zeta_3 \end{pmatrix}$$

are the vectors associated to fixed points of M_E and

$$\theta = \sqrt[3]{F_E(v_1)/F_E(v_2)}.$$

To finish the proof we need $\theta = \zeta$.

We have already fixed the shape of M_E; we'd like to see how much this has rigidified the value of δ_E. If we compose the embedding of E in $\mathbb{P}^2$ with a linear automorphism V^{-1}, the automorphism M_E changes by its conjugation by $V^{-1} : M_E \mapsto V^{-1} \cdot M_E \cdot V$. In order to leave M_E fixed, V should commute with M_E in $PGL_3(K')$. For example, we could let $V = \alpha M_E + \beta M_E^2 + \gamma I$, for some constants $\alpha, \beta, \gamma \in K'$. Then V^{-1} sends δ_E to

$$\sqrt[3]{(V^{-1}F_E)(v_1)/(V^{-1}F_E)(v_2)} = \sqrt[3]{F_E(V \cdot v_1)/F_E(V \cdot v_2)} =$$

$$\sqrt[3]{F_E((\alpha\zeta_3 + \beta\zeta_3^2 + \gamma)v_1)/F_E((\alpha\zeta_3^2 + \beta\zeta_3 + \gamma)v_2)} =$$

$$\theta \cdot \frac{\alpha\zeta_3 + \beta\zeta_3^2 + \gamma}{\alpha\zeta_3^2 + \beta\zeta_3 + \gamma}.$$

If we let $r = \alpha\zeta_3 + \beta\zeta_3^2 + \gamma$ and let $\sigma \in \mathrm{Gal}(K'(\zeta_3)/K')$ be as above, we have

$$\theta \overset{V}{\longmapsto} \theta \cdot \frac{r}{\sigma(r)}.$$

Since O_E is rational, $\sigma O_E = \sigma(v_1 + \theta v_2) = v_2 + \sigma(\theta) \cdot v_1 = O_E$, so $\sigma\theta \cdot \theta = 1$. In other words, θ is in the kernel of the norm map from $K'(\zeta_3)$ to K'. Since $Gal(K'(\zeta_3)/K')$ is cyclic, we know that the kernel of the norm map is the same as the set of elements of the from $a/\sigma(a)$ for $a \in K'(\zeta_3)$ (see page 108 of [1]). Thus for some $a \in K'(\zeta_3)$, $\theta = a/\sigma(a)$. We have shown that we can change θ by multiplying it by $r/\sigma(r)$ (for any $r \in K'(\zeta_3)$) while fixing M_E. Let $r = 1/(\zeta_3 \cdot a)$; then

$$\theta = a/\sigma(a) \overset{V_r}{\longmapsto} \theta \cdot \frac{r}{\sigma(r)} = \frac{\sigma(\zeta_3)}{\zeta_3} = \zeta_3.$$

□

We have now shown that we may take $\theta = \sqrt[3]{F_E(v_1)/F_E(v_2)} = \zeta_3$; in terms of the coefficients of F_E, this means

$$\sqrt[3]{(j + k\zeta_3 + l\zeta_3^2 + m)/(j + k\zeta_3^2 + l\zeta_3 + m)} = \zeta_3 \Longrightarrow k = l.$$

Using Claim 3.11 we may assume that $E_{K'(\zeta_3)}$ has $O_{E_{K'(\zeta_3)}} = (1 : -1 : 0)$ and "translation by T on $E_{K'(\zeta_3)}$" is given by a diagonal matrix with entries the distinct cubes roots of unity. We are now searching for $W \in \mathrm{PGL}_n(K'(\zeta_3))$ such that

- $W \cdot O_{E_{K'(\zeta_3)}} = W \cdot (1:-1:0) = (1:-1:0) = O_E$,
- $W \cdot T_{E_{K'(\zeta_3)}} = W \cdot (1:-\zeta_3:0) = (1:0:-1) = T_E$,
- $W \cdot 2T_{E_{K'(\zeta_3)}} = W \cdot (1:-\zeta_3^2:0) = (0:1:-1) = 2T_E$, and
- $W \cdot M_{E_{K'(\zeta_3)}} \cdot W^{-1} = W \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{pmatrix} \cdot W^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = M_E$.

Claim 4.10 *We may take* $W = \begin{pmatrix} 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \\ 1 & 1 & 1 \end{pmatrix}$.

Proof. First note that the above matrix satisfies the four properties above. Say we knew that $W \circ \varphi$ moves C to an elliptic curve E defined over K'. Then to see that E is actually the Jacobian of C, we need to check that the cocycle $\xi : Gal(\overline{K'}/K') \longrightarrow Aut(E)$, $\xi : \sigma \longmapsto \sigma(W \circ \varphi)\,(W \circ \varphi)^{-1}$ lands in the subgroup $E \subset Aut(E)$. We will now simplify this problem. Rewrite $\sigma(W \circ \varphi)\,(W \circ \varphi)^{-1} = \sigma(W \cdot \Phi^{-1})\,(W \cdot \Phi^{-1})^{-1} = \sigma W\,(\sigma\Phi^{-1}\,\Phi\,)W^{-1}$. For $\sigma \in Gal(\overline{K'}/K')$ such that $\sigma(W) = W$ ($\Leftrightarrow \sigma(\zeta_3) = \zeta_3$), $\xi(\sigma)$ has been examined in the context of $E_{K'(\zeta_3)}$ and was found be a translation map. That means we know ξ takes values in E for half of the relevant elements of $\mathrm{Gal}(\overline{K'}/K')$.

To finish, we need only show that $\xi(\sigma') \in E$ for some σ' such that $\sigma'(\zeta_3) = \zeta_3^2$: writing an element of $\mathrm{Gal}(\overline{K}'/K')$ as the product $\epsilon \cdot \sigma'$ where ϵ fixes ζ_3, we have $\xi(\epsilon \cdot \sigma') = \xi(\epsilon)^{\sigma'} \cdot \xi(\sigma')$, and the translation maps are clearly a Galois-invariant subgroup of $Aut(E)$.

Let us choose σ' to be such that $\sigma'(\zeta_3) = \zeta_3^2$, $\sigma'(\sqrt[3]{b}) = \sqrt[3]{b}$ ($\Rightarrow \sigma'(v_1) = v_2$ and $\sigma'(v_0) = v_0$), and $\sigma'(\delta) = 1/\delta$. Then σ' acts on the flex points of C in the following way:

- $\sigma'(x_0) = \sigma'(v_1 + \delta v_2) = v_2 + 1/\delta v_1 = x_0$, and more generally
- $\sigma'(x_0 + i \cdot T) = \sigma'(v_1 + \delta\,\zeta_3^i\,v_2) = v_2 + (1/\delta)\,\zeta_3^{2\cdot i}\,v_1 = x_0 + i \cdot T$.

We have, for $i \in \mathbb{Z}$,

$$\xi(\sigma')(i\,T) = \sigma'(W\,\Phi^{-1})\,(\Phi\,W^{-1})\,(i\,T) = \sigma'(W\,\Phi^{-1})(x_0 + i\,T) =$$
$$\sigma'(W\,\Phi^{-1}\sigma'^{-1}(x_0 + i\,T)) = \sigma'(i\,T) = i\,T.$$

This means that $\xi\,(\sigma')$ lands in $Aut^0(E)$ and has at least three fixed points in the three-torsion subgroup, so $\xi\,(\sigma')$ could only be trivial or ρ, of order three. Since ρ is an automorphism that acts only on curves with j-invariant 0, $\xi(\sigma') = \rho$ would mean that our family consisting of all curves of genus one whose Jacobian has a rational 3-torsion point all have j-invariant 0, which is clearly false. □

Finally, let's see why $W \circ \varphi$ brings C to an elliptic curve defined over K'. This is the same thing as acting on $E_{K'(\zeta_3)}$ by W.

$$F_E(X,Y,Z) = F_{E_{K'(\zeta_3)}}(X + \zeta_3 Y + \zeta_3^2 Z, X + \zeta_3^2 Y + \zeta_3 Z, X + Y + Z)$$
$$= (X + \zeta_3 Y + \zeta_3^2 Z)^3 + (X + \zeta_3^2 Y + \zeta_3 Z)^3 + \frac{G}{H}\,(X + Y + Z)^3 +$$
$$(X + \zeta_3 Y + \zeta_3^2 Z)(X + \zeta_3^2 Y + \zeta_3 Z)(X + Y + Z) =$$
$$(3+\frac{G}{H})(X^3+Y^3+Z^3)+(-3+3\frac{G}{H})(X^2Y+XY^2+Y^2Z+YZ^2+Z^2X+ZX^2)$$
$$+(3 + 2\frac{G}{H})(3XYZ),$$

where $G = (\alpha b + \delta)^3 + \beta^3 b^2 + \gamma^3 b - 3(\alpha b + \delta)\beta\gamma b$ and $H = (3(2\alpha b - \delta))^3$. □

4.8 Uniqueness of E's Model

F_E and all of the translation by three-torsion matrices for E are independent of the lift of b to K from $K^*/(K^*)^3$. That is, a different choice bu^3 instead of b, given by composing f by a simple matrix, changes many of our variables (for example, it sends $\alpha \mapsto \alpha/u^6, \beta \mapsto \beta/u^5$, etc.) but not the equation F_E and the matrices D and W. The equation F_E is defined up to a scalar multiple of F_C- that is, if we multiply α, β, γ, and δ by some number in K, we get the same Jacobian and the same maps.

5 Curves of Genus One in $\mathbb{P}^4$

5.1 Setting Up

Let K be a field with char(K) not divisible by 5. Assume that $\zeta_5 \in K$. Let

$$(\mathcal{C}/\mathcal{S}, \mathcal{L}, \mathcal{T})$$

be a 5-prepared genus one curve. When $\mathcal{S} = \mathrm{Spec}(K)$, we know that (Remark A on page 4) the line bundle $\mathcal{L}$ embeds $\mathcal{C}$ in $\mathbb{P}^4_K$ as a degree 5 curve; in fact $\mathcal{C}$ will be given as the intersection of five quadrics.

Remark. A particularly nice way to get five such quadrics was explained to me by Prof. Shepherd-Baron: Give yourself a 5-by-5 skew-symmetric matrix (so the diagonal elements will be 0). There are then 5 4-by-4 minors along the diagonal; the determinants of these 5 matrices turn out to be perfect squares. The resulting 5 square roots are homogeneous degree 2 polynomials in the original entries; if the entries are linear in the 5 coordinates of $\mathbb{P}^4$, the resulting intersection of five quadrics is generically (over the space of the matrix entries) a smooth curve of genus one.

Let E be an elliptic curve with a principal homogeneous space action λ on $\mathcal{C}$ that induces an isomorphism of E with the Jacobian of $\mathcal{C}$. We will sometimes identify the two elliptic curves by this isomorphism. We have the automorphism $\lambda_{\mathcal{T}}$ on $\mathcal{C}$ which by Remark C (page 6) extends to an automorphism of $\mathbb{P}^4_K$. Let $M_{\mathcal{T}}$ be a lift of $\lambda_{\mathcal{T}}$ to $\mathrm{GL}_n(K)$.

Fix five quadrics which define $\mathcal{C}$, and let V be the vector space generated by those quadrics. Lemma 5.8.1 of [8] tells us that since V is a $\overline{K}-$vector space and since $G = Gal(\overline{K}/K)$ acts continuously on V in a compatible manner with the $\overline{K}-$ action, V has a basis of $G-$invariant vectors. $M_{\mathcal{T}}$ acts on V. Let $Q \in V$ be a rational quadric (i.e. invariant by the $G-$action) such that $< M^i_{\mathcal{T}} \cdot Q >= V$. Such a Q exists by the same argument that proved Claim 3.8. Given such a Q we have, for any point $x \in \mathcal{C}$ and for $0 \le i \le 4$,

$$M^i_{\mathcal{T}} \cdot Q(x) = 0 \Longleftrightarrow Q(M^{-i}_{\mathcal{T}} \cdot (x)) = 0.$$

In essence, by finding such a Q, we have reduced the number of quadrics needed to define C from five to one. Let

$$Q(x) = \sum_{0 \le i \le j \le 4} a_{i,j}\, x_i\, x_j.$$

Let $\mathcal{S}$ be the largest subscheme of $\mathrm{Spec}(K[b, a_{i,j}])$ over which the scheme defined by the formula

$$\{x \in \mathbb{P}^4_{\mathcal{S}} \mid M^i_{\mathcal{T}} \cdot Q(x) = 0 \ \forall i\}$$

is a smooth curve over $\mathcal{S}$. Let $\Lambda_{\mathcal{S}} = (\mathcal{C}/\mathcal{S}, \mathcal{L}, \mathcal{T})$ be the 5-prepared genus one curve defined by these quadrics $M^i_{\mathcal{T}} \cdot Q(x)$.

5.2 The Main Theorem

Theorem 5.1 *Let $\mathcal{S}, \Lambda_{\mathcal{S}} = (\mathcal{C}/\mathcal{S}, \mathcal{L}, \mathcal{T})$ be as above. Let*

$$\Lambda_{Jac,\mathcal{S}} = (\mathcal{E}/\mathcal{S}, \mathcal{O}(5 \cdot O_{\mathcal{E}}), \mathcal{T})$$

be the Jacobian of $\Lambda_{\mathcal{S}}$. Then $\mathcal{E}$ is given by quadrics $D^i_{\mathcal{T}} \cdot Q_{\mathcal{E}}(x), 0 \le i \le 4$, where

- $D_{\mathcal{T}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \zeta_5 & 0 & 0 & 0 \\ 0 & 0 & \zeta_5^2 & 0 & 0 \\ 0 & 0 & 0 & \zeta_5^3 & 0 \\ 0 & 0 & 0 & 0 & \zeta_5^4 \end{pmatrix}$,
- $Q_{\mathcal{E}}(x) = Q(\Phi(x))$, *where* $\Phi \in PGL_3(K(b, a_{i\,j})_s)$ *is given by the matrix*

  $$\Phi = \begin{pmatrix} v_0 & \sqrt[5]{d} \cdot v_1 & \sqrt[5]{d^2} \cdot \alpha \cdot v_2 & \sqrt[5]{d^3} \cdot \beta \cdot v_3 & \sqrt[5]{d^4} \cdot \gamma \cdot v_4 \cdot k \end{pmatrix}, \textit{ with}$$

- $v_i, 0 \le i \le 4$, *are the eigenvectors of* $M_{\mathcal{T}}$,
- $B(X, Y)$ *is the bilinear form* $Q(X + Y) - Q(X) - Q(Y)$
- $d = \frac{Q(v_0) \cdot B(v_0, v_3) \cdot B(v_0, v_2)^2}{B(v_2, v_3) \cdot B(v_1, v_2) \cdot Q(v_1)^2}$, $\alpha = -\frac{Q(v_2)}{B(v_1, v_3)}$, $\beta = -\frac{Q(v_2) \cdot Q(v_1)^2}{B(v_1, v_3) \cdot B(v_0, v_2)^2}$, $\gamma = \frac{Q(v_0)}{d \cdot B(v_1, v_4)}$, $k \in K$,

- $vec(x_0) = v_0 + \sqrt[5]{d} \cdot v_1 + \sqrt[5]{d^2} \cdot \alpha \cdot v_2 + \sqrt[5]{d^3} \cdot \beta \cdot v_3$ *is the pre-image of* $\mathcal{O}$ *under* φ, *and*

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

To prove Theorem 5.1 we would like to use the comments in Section 3.10 to reduce to proving it over the generic point of the base $\mathcal{S}$. The snag is that we would have to prove that $\mathcal{S}$ as defined above is normal. I believe it is, but I do not have an elegant proof. Instead we will prove our theorem first over the generic point and then deduce it for all other smooth fibers of our family of curves. Let $K' = K(b, a_{ij})$. We need to find the Jacobian of the 5-prepared genus one curve $\Lambda = (C/K', L, T)$ where $C \in \mathbb{P}^4_{K'}$ is given by the formula

$$\{x \in \mathbb{P}^4_{\mathcal{S}} \mid M_T^i \cdot Q(x) = 0 \; \forall i\}.$$

5.3 Standardizing the model for C

We already know that C is given in $\mathbb{P}^4_{K'}$ by the five quadrics $M_T^i \cdot Q$. By Claim 3.8 we may assume

$$M_T = \left[\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ b & 0 & 0 & 0 & 0 \end{pmatrix} \right],$$

where b is some lift to K^* of $\det(M_T)$.

By standardizing M_T we get also change Q but its salient properties remain- it is still K'-rational and its M_T-orbit still generates V.

5.4 Finding x_0

Let $\Lambda_E = (E/K', \mathcal{O}(5 \cdot O_E), T)$ be isomorphic to the Jacobian of Λ. From Claim 3.7, page 12 we know that x_0, the point of C which maps to O_E by φ_{x_0} (Claim 3.5), lives on the hyperplane in $\mathbb{P}^4$ which contains four of the five fixed $\overline{K}$-points of M_T: $p_i = \left(1 : \sqrt[5]{b}\zeta_5^i : \ldots : \sqrt[5]{b^4}\zeta_5^{4i}\right) \in \mathbb{P}^4(\overline{K})$. The vectors v_i associated to the p_i are the eigenvectors of M, where v_i has eigenvalue $\sqrt[5]{b} \cdot \zeta_5^i$. Then $x_0 = proj(\lambda_0 \cdot v_0 + \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3)$ for some $\lambda_i \in K'_s, 0 \leq i \leq 3$. Since x_0 is also a point on C, we know $Q(M^i \cdot x_0) = 0$, $0 \leq i \leq 4$. We have

$$M^i(x_0) = M^i(proj(\lambda_0 \cdot v_0 + \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3))$$
$$= proj(\lambda_0 \cdot M^i(v_0) + \lambda_1 \cdot M^i(v_1) + \lambda_2 \cdot M^i(v_2) + \lambda_3 \cdot M^i(v_3))$$
$$= proj(\lambda_0 \cdot v_0 + \lambda_1 \cdot \zeta_5^i \cdot v_1 + \lambda_2 \cdot \zeta_5^2 i \cdot v_2 + \lambda_3 \cdot \zeta_5^3 i \cdot v_3).$$

We have:

$$Q(M^i \cdot x_0) = 0 \text{ for all } i,\ 0 \leq i \leq 4.$$
$$\Updownarrow$$
$$Q(\lambda_0 \cdot v_0 + \lambda_1 \cdot \zeta_5^i \cdot v_1 + \lambda_2 \cdot \zeta_5^{2i} \cdot v_2 + \lambda_3 \cdot \zeta_5^{3i} \cdot v_3) = 0 \text{ for all } i,\ 0 \leq i \leq 4.$$

Claim 5.1 *Write $x_0 = proj(\lambda_0 \cdot v_0 + \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3)$. Then*

- $\frac{\lambda_1}{\lambda_0} = \sqrt[5]{d}$ *for some* $d \in K'(\sqrt[5]{b})$
- $\frac{\lambda_2}{\lambda_0} = \sqrt[5]{d^2} \cdot \alpha$ *for some* $\alpha \in K'(\sqrt[5]{b})$
- $\frac{\lambda_3}{\lambda_0} = \sqrt[5]{d^3} \cdot \beta$ *for some* $\beta \in K'(\sqrt[5]{b})$

Proof. We will be studying the following diagram of fields:

$$\begin{array}{c} K'(x_0) \\ | \\ K'(\sqrt[5]{b}) \\ | \\ K' \end{array}$$

There are five points in the intersection of C with the hyperplane

$$\mathbb{H} = \lambda_0 \cdot v_0 + \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3.$$

Once we rationalize one point, all of them are rational, since once we have x_0 we also have $x_0 + i \cdot T$, and toegether they make up the intersection (see Claim 3.7). Any field over which all of the $x_0 + i \cdot T$'s are defined contains $\sqrt[5]{b}$. Thus to rationalize one point of intersection will require an extension of degree five of $K'(\sqrt[5]{b})$; that is, $[K'(x_0) : K'(\sqrt[5]{b})] = 5$. Moreover, $K'(x_0)/K'(\sqrt[5]{b})$ is a Galois extension, since the points in the intersection are sent only to each other by elements of $\mathrm{Gal}(\overline{K'(\sqrt[5]{b})}/K'(\sqrt[5]{b}))$ (since $\mathbb{H}$ is fixed). Let σ generate the group $\mathrm{Gal}(K'(x_0)/K'(\sqrt[5]{b})) \cong \mathbb{Z}/5\mathbb{Z}$. We may assume that $\sigma(x_0) = x_0 + T$. We now have:

$$\sigma(x_0) = \lambda_0 \cdot v_0 + \lambda_1 \cdot \zeta_5 \cdot v_1 + \lambda_2 \cdot \zeta_5^2 \cdot v_2 + \lambda_3 \cdot \zeta_5^3 \cdot v_3.$$

We can also write

$$\sigma(x_0) = \sigma(\lambda_0) \cdot v_0 + \sigma(\lambda_1) \cdot v_1 + \sigma(\lambda_2) \cdot v_2 + \sigma(\lambda_3) \cdot v_3,$$

since the v_j's are defined over $K(\sqrt[5]{b})$. Over $K(\sqrt[5]{b})$, $\mathbb{H} \cong \mathbb{P}^3_{K(\sqrt[5]{b})}$, with coordinates $\lambda_0, \lambda_1, \lambda_2$, and λ_3. We have

$$(\lambda_0 : \lambda_1 : \lambda_2 : \lambda_3) \overset{\sigma}{\mapsto} \left(\lambda_0 : \lambda_1 \cdot \zeta_5 : \lambda_2 \cdot \zeta_5^2 : \lambda_3 \cdot \zeta_5^3\right).$$

We conclude

$$\sigma\left(\frac{\lambda_1}{\lambda_0}\right) = \zeta_5 \cdot \frac{\lambda_1}{\lambda_0}, \qquad \sigma\left(\frac{\lambda_2}{\lambda_0}\right) = \zeta_5^2 \cdot \frac{\lambda_2}{\lambda_0}, \qquad \text{and} \qquad \sigma\left(\frac{\lambda_3}{\lambda_0}\right) = \zeta_5^3 \cdot \frac{\lambda_3}{\lambda_0}.$$

Define $d = \left(\frac{\lambda_1}{\lambda_0}\right)^5$. The norm of $\left(\frac{\lambda_1}{\lambda_0}\right)$ is d :

$$\mathbb{N}_{K(x_0)/K(\sqrt[5]{b})}\left(\frac{\lambda_1}{\lambda_0}\right) = \prod_{i=0}^{4} \sigma^i \left(\frac{\lambda_1}{\lambda_0}\right) = \prod_{i=0}^{4} \zeta_5^i \cdot \frac{\lambda_1}{\lambda_0} = \frac{\lambda_1}{\lambda_0}^5 = d \in K(\sqrt[5]{b}).$$

This implies $K(x_0) = K(\sqrt[5]{b}, \sqrt[5]{d})$. Since $\sigma(\frac{\lambda_2}{\lambda_0}) = \zeta_5^2 \cdot \frac{\lambda_2}{\lambda_0}$, we see that $\frac{\lambda_2}{\lambda_0}/\sqrt[5]{d^2}$ is fixed by σ, so define $\alpha = \frac{\lambda_2}{\lambda_0}/\sqrt[5]{d^2} \in K(\sqrt[5]{b})$. Similarly, define $\beta = \frac{\lambda_3}{\lambda_0}/\sqrt[5]{d^3} \in K(\sqrt[5]{b})$. □

It remains to describe d, α, β, and γ. Let $B(X,Y)$ be the bilinear form associated to Q, i.e.

$$B(X,Y) = Q(X+Y) - Q(X) - Q(Y).$$

We may write

$$x_0 = \lambda_0 \cdot v_0 + \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \lambda_3 \cdot v_3,$$

where $\frac{\lambda_1}{\lambda_0} = \sqrt[5]{d}$, $\frac{\lambda_2}{\lambda_0} = \sqrt[5]{d^2} \cdot \alpha$, and $\frac{\lambda_3}{\lambda_0} = \sqrt[5]{d^3} \cdot \beta$. Fixing k,

$$M^{-k} \cdot Q(x_0) = Q(M^k(x_0)) = Q(\lambda_0 \cdot v_0 + \lambda_1 \, \zeta_5^k \cdot v_1 + \lambda_2 \, \zeta_5^{2k} \cdot v_2 + \lambda_3 \, \zeta_5^{3k} \cdot v_3) =$$

$$\sum_{i=0}^{4} \lambda_i^2 \, \zeta_5^{2\,i\,k} \cdot Q(v_i) + \sum_{i \neq j} \lambda_i \, \lambda_j \, \zeta_5^{k\,(i+j)} \cdot B(v_i, v_j) = 0 \tag{2}$$

The above equation depends on k, and as we vary k we get five different equations. If we add up all those equations, we get:

$$5\,(\lambda_0^2 \cdot Q(v_0) + \lambda_2 \, \lambda_3 \cdot B(v_2, v_3)) = 0,$$

because $\sum_{i=0}^4 \zeta_5^i = 0$. However if we divide each equation by the appropriate power of ζ_5 and then add, we get:

$$5\,(\lambda_1^2 \cdot Q(v_1) + \lambda_0 \, \lambda_2 \cdot B(v_0, v_2)) = 0,$$

$$5\,(\lambda_2^2 \cdot Q(v_2) + \lambda_1 \, \lambda_3 \cdot B(v_1, v_3)) = 0,$$

$$5\,(\lambda_3^2 \cdot Q(v_3) + \lambda_0 \, \lambda_1 \cdot B(v_0, v_1)) = 0,$$

and finally

$$5\,(\lambda_0 \, \lambda_3 \cdot B(v_0, v_3) + \lambda_1 \, \lambda_2 \cdot B(v_1, v_2)) = 0.$$

Since $\mathrm{char}(K') \neq 5$, we can divide and rearrange to get:

$$d \cdot \alpha \cdot \beta = \frac{\lambda_2 \, \lambda_3}{\lambda_0^2} = -\frac{Q(v_0)}{B(v_2, v_3)}$$

$$\alpha = \frac{\lambda_0 \, \lambda_2}{\lambda_1^2} = -\frac{Q(v_1)}{B(v_0, v_2)}$$

$$\frac{\beta}{\alpha^2} = \frac{\lambda_1 \, \lambda_3}{\lambda_2^2} = -\frac{Q(v_2)}{B(v_1, v_3)}$$

$$\frac{1}{\beta^2 \cdot d} = \frac{\lambda_0\,\lambda_1}{\lambda_3^2} = -\frac{Q(v_3)}{B(v_0,v_1)}$$

$$\frac{\alpha}{\beta} = \frac{\lambda_1\,\lambda_2}{\lambda_0\,\lambda_3} = -\frac{B(v_0,v_3)}{B(v_1,v_2)}.$$

From the above equalities we deduce the value of d, α, and β in terms of the values of B and Q on the fixed points v_i of M.

5.5 Standardizing the Model for E

By Claim 3.11 we may assume that "translation by T" on E is given by the matrix D, where

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \zeta_5 & 0 & 0 & 0 \\ 0 & 0 & \zeta_5^2 & 0 & 0 \\ 0 & 0 & 0 & \zeta_5^3 & 0 \\ 0 & 0 & 0 & 0 & \zeta_5^4 \end{pmatrix},$$

and that

$$O_E = (1 : 1 : 1 : 1 : 0).$$

The quadrics defining E are the quadrics that Q and its orbit under M_T are sent to under φ_{x_0}. Define Q_E to be the quadric that Q is sent to by φ_{x_0}.

Claim 5.2 *E is defined by the five quadrics Q_E, $D \cdot Q_E$, $D^2 \cdot Q_E$, $D^3 \cdot Q_E$, and $D^4 \cdot Q_E$.*

Proof. Let $\sigma \in \mathrm{Gal}(K_s'/K')$ be an element such that $\sigma(\sqrt[5]{b}) = \sqrt[5]{b}$ and $\sigma(\sqrt[5]{d}) = \zeta_5^4 \sqrt[5]{d}$. The "translation by T map on E" is given by the map $D = \varphi_{x_0}^{\sigma}\,\varphi_{x_0}^{-1}$, and the "translation by T map on C" is given by the map $D = \varphi_{x_0}^{-1}\,\varphi_{x_0}^{\sigma}$ (see the proof of Claim 4.5). But $\varphi_{x_0}^{\sigma}\,\varphi_{x_0}^{-1} = (\varphi_{x_0}\varphi_{x_0}^{-1})\varphi_{x_0}^{\sigma}\,\varphi_{x_0}^{-1} = \varphi(\varphi_{x_0}^{-1}\varphi_{x_0}^{\sigma})\varphi_{x_0}^{-1} = \varphi_{x_0}[M]\varphi_{x_0}^{-1}$. The map $\varphi_{x_0}^{-1}$ takes the quadrics defining E to the quadrics defining C, M permutes them, and φ_{x_0} brings them back. $\square$

5.6 Finding φ_{x_0}

We hope to find φ_{x_0}, the map from C to E which exists by Claim 3.5. Lift $\varphi_{x_0} \in \mathrm{PGL}_n(K'(x_0))$ to the matrix $\Phi^{-1} \in GL_5(K(x_0))$. We have already fixed

$$\varphi_{x_0}(x_0 + i \cdot T) = (1\,;\,\zeta_5^i\,;\,\zeta_5^{2i}\,;\,\zeta_5^{3i}\,;\,0).$$

Then

$$\Phi^{-1} \cdot M^i(x_0) = (1\,;\,\zeta_5^i\,;\,\zeta_5^{2i}\,;\,\zeta_5^{3i}\,;\,0) \Longleftrightarrow M^i(x_0) = \Phi \cdot (1\,;\,\zeta_5^i\,;\,\zeta_5^{2i}\,;\,\zeta_5^{3i}\,;\,0).$$

Since we already know the form of each $M^i(x_0)$ (see page 40) we deduce that there exist $h_i \in K'(x_0)$ such that

$$\Phi = \begin{pmatrix} v_0 & v_1\sqrt[5]{d} & v_2\sqrt[5]{d^2}\alpha & v_3\sqrt[5]{d^3}\beta & h \end{pmatrix}, \quad \text{for} \quad h = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \end{pmatrix}.$$

Claim 5.3 Φ *is of the form*

$$\Phi = \begin{pmatrix} v_0 & v_1\sqrt[5]{d} & v_2\sqrt[5]{d^2}\alpha & v_3\sqrt[5]{d^3}\beta & v_4\sqrt[5]{d^4}\gamma \end{pmatrix},$$

for $\gamma \in K'(\sqrt[5]{b})$.

Proof. Let σ^{-1} be as in the proof of Claim 4.5, i.e. such that $\sigma^{-1}(\sqrt[5]{b}) = \sqrt[5]{b}$, $\sigma^{-1}(\sqrt[5]{d}) = \zeta_5^4\sqrt[5]{d}$, and the map $\varphi_{x_0}^{\sigma^{-1}}\varphi_{x_0}^{-1}$ is "translation by T on E." In terms of matrices this means that for some $\kappa \in K'(x_0), \sigma^{-1}(\Phi^{-1}) \cdot \Phi = \kappa \cdot D$. We rewrite this as $\sigma\Phi = \kappa \cdot \Phi \cdot D$:

$$\begin{aligned} \sigma\Phi &= \sigma \begin{pmatrix} v_0 & v_1\sqrt[5]{d} & v_2\sqrt[5]{d^2}\alpha & v_3\sqrt[5]{d^3}\beta & h \end{pmatrix} \\ &= \begin{pmatrix} v_0 & v_1\sqrt[5]{d}\zeta_5 & v_2\sqrt[5]{d^2}\zeta_5^2\alpha & v_3\sqrt[5]{d^3}\zeta_5^3\beta & \sigma(h) \end{pmatrix} \\ &= \kappa \cdot \Phi \cdot D = \kappa \cdot \begin{pmatrix} v_0 & v_1\sqrt[5]{d}\zeta_5 & v_2\sqrt[5]{d^2}\zeta_5^2\alpha & v_3\sqrt[5]{d^3}\zeta_5^3\beta & \zeta_5^4 \cdot h \end{pmatrix}. \end{aligned}$$

Similarly we know the map $\varphi_{x_0}^{-1}\varphi_{x_0}^{\sigma^{-1}}$ is "translation by T on C." This means that for some $\kappa' \in K'(x_0), \Phi \cdot \sigma^{-1}\Phi^{-1} = \kappa' \cdot M$, or in other words $\sigma\Phi = \kappa' \cdot M \cdot \Phi$:

$$\sigma\Phi = \begin{pmatrix} v_0 & v_1\sqrt[5]{d}\zeta_5 & v_2\sqrt[5]{d^2}\zeta_5^2\alpha & v_3\sqrt[5]{d^3}\zeta_5^3\beta & \sigma(h) \end{pmatrix} = \kappa' \cdot M \cdot \Phi$$

$$= \kappa' \cdot \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ b & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} & & & & h_1 \\ & & & & h_2 \\ v_0 & v_1\sqrt[5]{d} & v_2\sqrt[5]{d^2}\alpha & v_3\sqrt[5]{d^3}\beta & h_3 \\ & & & & h_4 \\ & & & & h_5 \end{pmatrix}$$

$$= \kappa' \cdot \sqrt[5]{b} \cdot \begin{pmatrix} & & & & h_2 \\ & & & & h_3 \\ v_0 & v_1\zeta_5\sqrt[5]{d} & v_2\zeta_5^2\sqrt[5]{d^2}\alpha & v_3\zeta_5^3\sqrt[5]{d^3}\beta & h_4 \\ & & & & h_5 \\ & & & & bh_1 \end{pmatrix}.$$

We know that $\sigma(h_1) = h_2$ and $\sigma(h_1) = \zeta_5^4 h_1$, from which we conclude $h_2 = h_1\zeta_5^4$. We continue this way and conclude that the right-most column of Φ is $h_1 \cdot v_4$. Moreover, we know $h_1 \in K'(x_0)$ and we know how σ from above acts on h_1; namely, $\sigma(h_1) = \zeta_5^4 h_1$. This means that $\frac{h_1}{\sqrt[5]{d^4}} \in K'(\sqrt[5]{b})$, or in other words $h_1 = \sqrt[5]{d^4} \cdot \gamma$ for some $\gamma \in K'(\sqrt[5]{b})$. $\square$

It remains to find γ. We already know $\gamma \in K(\sqrt[5]{b})$, so if we understand how γ moves under a Galois element moving $\sqrt[5]{b}$ to $\sqrt[5]{b}\cdot\zeta_5$, we will understand γ up to a multiple of something in K. To find γ we will investigate the model for E :

$$Q_E(y) = 0 \Longleftrightarrow Q(\varphi_{x_0}^{-1}(y)) = Q(\Phi y) = 0.$$

Let $y = (V : W : X : Y : Z)$; then up to scalar multiples,

$$\begin{aligned} Q_E(y) &= Q(\Phi \cdot y) \\ &= Q(V\,v_0 + W\,v_1\zeta_5\sqrt[5]{d} + X\,\zeta_5^2\sqrt[5]{d^2}\alpha + Y\,\zeta_5^3\sqrt[5]{d^3}\beta + Z\,\zeta_5^4\sqrt[5]{d^4}\gamma). \end{aligned}$$

We expand to get

$$Q_E(y) = V^2 \cdot Q(v_0) + W^2 \cdot \zeta_5^2\,\sqrt[5]{d^2}\,Q(v_1) + \ldots + YZ \cdot \zeta_5^7\,\sqrt[5]{d^7}\,\beta\,\gamma\,B(v_3, v_4).$$

We now find a new representation of E; we will find five quadrics which still define E but are fixed by a multiple of D. The reason we do so is that a quadratic form fixed by D has many fewer terms than the general quadratic form. Define

$$R_k = \sum_{i=0}^{4} (D/\zeta_5^k)^i \, Q_E.$$

Claim 5.4 *Each R_k is fixed by D/ζ_5^k.*

Proof.

$$D/\zeta_5^k\,(R_k) = D/\zeta_5^k\,\Big(\sum_{i=0}^{4}(D/\zeta_5^k)^i\,Q_E\Big) = \sum_{i=0}^{4}(D/\zeta_5^k)^{i+1}\,Q_E = R_k. \square$$

If we write

$$R_k = \sum_{0\le i\le j\le 4} r_{i,j}\, x_i\, x_j,$$

then all $r_{ij} = 0$ unless $i + j - 2\cdot k \equiv 0 \pmod{5}$, since R_k is fixed by D/ζ_5^k. For each k, we have three terms in R_k (for example, $R_0 = r_{00}\,x_0^2 + r_{14}\,x_1\,x_4 + r_{23}\,x_2\,x_3$).

Claim 5.5 *Let $\tau \in Gal(\overline{K}/K)$ be an element such that $\sigma(\sqrt[5]{b}) = \zeta_5\sqrt[5]{b}$. In particular, this means $\tau v_i = v_{i+1}$. Then $\tau\varphi\,\varphi^{-1}$ is represented by the matrix*

$$S_\tau = \left[\begin{pmatrix} 0 & \sqrt[5]{d} & 0 & 0 & 0 \\ 0 & 0 & \alpha\sqrt[5]{\frac{d^2}{\tau d}} & 0 & 0 \\ 0 & 0 & 0 & \frac{\beta}{\tau\alpha}\sqrt[5]{\frac{d^3}{(\tau d)^2}} & 0 \\ 0 & 0 & 0 & 0 & \frac{\gamma}{\tau\beta}\sqrt[5]{\frac{d^4}{(\tau d)^3}} \\ \frac{1}{\tau\gamma}\sqrt[5]{\frac{1}{(\tau d)^4}} & 0 & 0 & 0 & 0 \end{pmatrix}\right].$$

Proof. We need to see why $\tau\Phi^{-1}\,\Phi = S_\tau$, or in other words why $\kappa\cdot\Phi = \tau\Phi\, S_\tau$ for some $\kappa \in K'(x_0)$:

$$\tau\Phi\, S_\tau = \tau\begin{pmatrix} v_0 & \sqrt[5]{d}\cdot v_1 & \sqrt[5]{d^2}\cdot\alpha\cdot v_2 & \sqrt[5]{d^3}\cdot\beta\cdot v_3 & \sqrt[5]{d^4}\cdot\gamma\cdot v_4 \end{pmatrix}\cdot S_\tau =$$

$$\begin{pmatrix} v_1 & \sqrt[5]{\tau d}\cdot v_2 & \sqrt[5]{(\tau d)^2}\cdot\tau\alpha\cdot v_3 & \sqrt[5]{(\tau d)^3}\cdot\tau\beta\cdot v_4 & \sqrt[5]{(\tau d)^4}\cdot\tau\gamma\cdot v_0 \end{pmatrix}\cdot S_\tau =$$

$$\begin{pmatrix} v_0 & \sqrt[5]{d}\cdot v_1 & \sqrt[5]{d^2}\cdot\alpha\cdot v_2 & \sqrt[5]{d^3}\cdot\beta\cdot v_3 & \sqrt[5]{d^4}\cdot\gamma\cdot v_4 \end{pmatrix} = \Phi.$$

Corollary 5.1 *S_τ permutes the quadrics R_k.*

Proof. The matrix S_τ moves x_i to some multiple of x_{i+1} ($i \in \mathbb{F}_5$), so S_τ moves the term $r_{i\,j}\, x_i\, x_j$ of R_k to $b_{i+1\,j+1}\, x_{i+1}\, x_{j+1}$, with $i + j - 2 \cdot k \equiv 0 \pmod{5} \Leftrightarrow (i+1) + (j+1) - 2 \cdot (k+1) \equiv 0 \pmod{5}$. In other words S_τ moves R_0 to a quadric which has exactly the same non-zero coefficients as R_1. By a dimension count we conclude that $S_\tau \cdot R_0$ is a multiple of R_1. We can rescale the R_k's so that S_τ actually permutes them; rescaling will keep them fixed by D/ζ_5^k and won't change E.

Claim 5.6 *γ can be taken to be $\frac{Q(v_0)}{d \cdot B(v_1, v_4)}$.*

Proof. First note that

$$\begin{pmatrix} V \\ W \\ X \\ Y \\ Z \end{pmatrix} \overset{S_\tau}{\mapsto} \begin{pmatrix} W\, \sqrt[5]{d} \\ X\, \frac{\sqrt[5]{d^2}}{\tau d}\, \alpha \\ Y\, \frac{\sqrt[5]{d^3}}{(\tau d)^2}\, \frac{\beta}{\tau\alpha} \\ Z\, \frac{\sqrt[5]{d^4}}{(\tau d)^3}\, \frac{\gamma}{\tau\beta} \\ V\, \frac{1}{(\tau d)^4}\, \frac{1}{\tau\gamma} \end{pmatrix},$$

so

$$S(R_0) = S(V^2 \cdot Q(v_0) + W\,Z \cdot B(v_1,\, v_4)\, d\,\gamma + X\,Y \cdot B(v_2,\, v_3)\, d\,\alpha\,\beta) =$$

$$W^2 \cdot Q(v_0)\, \sqrt[5]{d^2} + X\,V \cdot B(v_1, v_4)\, \frac{d\,\gamma\alpha}{\tau\gamma} \sqrt[5]{\frac{d^2}{(\tau d)^5}} + Y\,Z \cdot B(v_3,\, v_3)\, \frac{d\,\alpha\,\beta^2\,\gamma}{\tau\alpha\,\tau\beta} \sqrt[5]{\frac{d^7}{(\tau d)^5}}.$$

Since

$$R_1 = W^2 \cdot Q(v_1)\, \sqrt[5]{d^2} + V\,X \cdot B(v_0,\, v_2)\, \sqrt[5]{d^2}\, \alpha + Y\,Z \cdot B(v_3,\, v_4)\, \sqrt[5]{d^7}\, \beta\,\gamma,$$

we have

$$\frac{B(v_0,\, v_2)\, \sqrt[5]{d^2}\, \alpha}{Q(v_1)\, \sqrt[5]{d^2}} = \frac{B(v_1, v_4)\, \frac{d\,\gamma\alpha}{\tau\gamma} \sqrt[5]{\frac{d^2}{(\tau d)^5}}}{Q(v_0)\, \sqrt[5]{d^2}}.$$

This simplifies to

$$\frac{\gamma}{\tau\gamma} = \frac{\tau d \cdot Q(v_0) \cdot B(v_0,\, v_2)}{d \cdot Q(v_1) \cdot B(v_1,\, v_4)} = \frac{\tau d \cdot Q(v_0) \cdot \tau B(v_4,\, v_1)}{d \cdot \tau Q(v_0) \cdot B(v_1,\, v_4)},$$

so we have

$$\frac{\gamma}{\tau\gamma} = \frac{Q(v_0)}{d \cdot B(v_1,\, v_4)} \cdot \tau\left(\frac{d \cdot B(v_1,\, v_4)}{Q(v_0)}\right).$$

In other words we have an element $\gamma \cdot \frac{d \cdot B(v_1,\, v_4)}{Q(v_0)}$ of $K'(\sqrt[5]{b})$ which is fixed by τ - this means that it is in K'. We conclude that $\gamma = k \cdot \frac{Q(v_0)}{d \cdot B(v_1,\, v_4)}$ for some $k \in K'$.

We can choose k as we wish; once we do we will have completely rigidified the model for E.

We have found the Jacobian of the generic point of our family $\mathcal{C}/\mathcal{S}$ from Theorem 5.1. Now say $C_{a_{ij},b}$ is a smooth curve over K with $a_{ij}, b \in K$. Note that φ_{x_0} brings $C_{a_{ij},b}$ to some elliptic curve over K. We want to show this is (isomorphic to) the Jacobian of $C_{a_{ij},b}$. We will do this directly, i.e. by looking at the cocycle created by φ_{x_0}. Let L be the Galois closure of $K(x_0)$. If $\sqrt[5]{b}, \sqrt[5]{d} \notin K$, then our previous Galois theory computations have already found the Jacobian of $C_{a_{ij},b}$. If $\sqrt[5]{b} \in K$, then we see that

$$\Phi = \begin{pmatrix} v_0 & \sqrt[5]{d} \cdot v_1 & \sqrt[5]{d^2} \cdot \alpha \cdot v_2 & \sqrt[5]{d^3} \cdot \beta \cdot v_3 & \sqrt[5]{d^4} \cdot \gamma \cdot v_4 \cdot k \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta_5 & \zeta_5^2 & \zeta_5^3 & \zeta_5^4 \\ 1 & \zeta_5^2 & \zeta_5^4 & \zeta_5 & \zeta_5^3 \\ 1 & \zeta_5^3 & \zeta_5^3 & \zeta_5^4 & \zeta_5^2 \\ 1 & \zeta_5^4 & \zeta_5 & \zeta_5^2 & \zeta_5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \sqrt[5]{d} & 0 & 0 & 0 \\ 0 & 0 & \sqrt[5]{d^2} \cdot \alpha & 0 & 0 \\ 0 & 0 & 0 & \sqrt[5]{d^3} \cdot \beta & 0 \\ 0 & 0 & 0 & 0 & \sqrt[5]{d^4} \cdot \gamma \end{pmatrix}.$$

If we modify our embedding of $C_{a_{ij},b}$ by the left matrix, then we get a "Selmer-like" curve where "Translation by T" is represented by D both on $C_{a_{ij},b}$ and on E. Moreover, the map φ_{x_0} is now a diagonal matrix. The proof that this matrix (the one on the right above) actually maps $C_{a_{ij},b}$ to its Jacobian is very similar to the proof of Theorem 6.2. If $\sqrt[5]{d} \in K$, we have $L = K(\sqrt[5]{b})$. Note if both $\sqrt[5]{d} \in K$, and $\sqrt[5]{b} \in K$, there is a rational point on C and Φ is an K-isomorphism of C with its Jacobian. So assume that $K(\sqrt[5]{b})/K$ is a degree five extension, and let σ generate the Galois group. We just need to show that the map $\varphi_{x_0}^{\sigma} \cdot \varphi_{x_0}^{-1}$ on E is a translation map. It is enough to show that $\varphi_{x_0}^\sigma \cdot \varphi_{x_0}^{-1}(x) = x + T'$ for five values of $x \in E$ and some $T' \in E[5](\overline{K})$, since composing $\varphi_{x_0}^\sigma \cdot \varphi_{x_0}^{-1}$ with $\lambda_{-T'}$ gives an automorphism of E fixing the origin and four other points, so it must be the identity. By construction we know $\varphi_{x_0}(x_0 + i \cdot T) = i \cdot T$. This means

$$(\varphi_{x_0} \cdot \lambda_{T,C}^i) \cdot x_0 = (\lambda_{T,E}^i \cdot \varphi_{x_0}) \cdot x_0.$$

The two maps $\varphi_{x_0} \cdot \lambda_{T,C}^i$ and $\lambda_{T,E}^i \cdot \varphi_{x_0}$ act the same on the five points $x_0 + i \cdot T$, which by the above argument means $\varphi_{x_0} \cdot \lambda_{T,C}^i = \lambda_{T,E}^i \cdot \varphi_{x_0}$. Then because T is rational, $\lambda_{T,E}$ commutes with the cocycle $\varphi_{x_0}^\sigma \cdot \varphi_{x_0}^{-1}$. we can take for x the five points of any orbit of $x \in E$ by $\Lambda_{T,E}$.

6 Curves of genus one in $\mathbb{P}^1 \times \mathbb{P}^1$

6.1 Setting up

Let K be a field with $\mathrm{char}(K)$ not divisible by 2. Let

$$(\mathcal{C}/\mathcal{S}, (\mathcal{L}_1, \mathcal{L}_2), \mathcal{T})$$

be a 2-prepared genus one curve over some base $\mathcal{S}$. When $\mathcal{S} = \mathrm{Spec}(K)$, we know that (Remark A on page 4) the pair $(\mathcal{L}_1, \mathcal{L}_2)$ embeds (see Remark A) $\mathcal{C}$ in $\mathbb{P}_K^1 \times_K \mathbb{P}_K^1$ as a double cover of each $\mathbb{P}_K^1$.; in fact $\mathcal{C}$ will be given by a $(2,2)$-form. There are two involutions κ_1 and κ_2 of $\mathcal{C}$ given an embedding $\mathcal{C}$ in $\mathbb{P}_K^1 \times_K \mathbb{P}_K^1$; namely, since each map $\mathcal{C} \longrightarrow \mathbb{P}_K^1$ is a double cover, let for $i = 1, 2, x \in C$,

$$\kappa_i(x) = y \in C \;\text{ such that }\; \mathcal{O}(y + x) \cong L_i.$$

Let E be an elliptic curve with a principal homogeneous space action λ on $\mathcal{C}$ that induces an isomorphism of E with the Jacobian of $\mathcal{C}$. We will sometimes identify the two elliptic curves by this isomorphism.

Assume that $\mathcal{S} = \mathrm{Spec}(K)$. We have the automorphism $\lambda_{\mathcal{T}}$ on $\mathcal{C}$ which by Remark C (page 6) extends to an automorphism of $\mathbb{P}_K^1 \times_K \mathbb{P}_K^1$. Let (M_1, M_2)

be a lift of $\lambda_{\mathcal{T}}$ to $\mathrm{GL}_n(K)\times\mathrm{GL}_n(K)$. By Claim 3.8 we may modify the embedding of $\mathcal{C}$ in $\mathbb{P}^1_K \times_K \mathbb{P}^1_K$ by a linear automorphism so that

$$(M_1, M_2) = \left(\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \right).$$

Fix a $(2,2)$-form $F_{\mathcal{C}}$ which defines $\mathcal{C}$. Then (M_1, M_2) acts on $(2,2)$-forms, and if we represent

$$F_{\mathcal{C}} = s^2(f_1x^2 + f_2xy + f_3y^2) + st\,(g_1x^2 + g_2xy + g_3y^2) + t^2(h_1x^2 + h_2xy + h_3y^2)$$

by the matrix

$$M_{F_{\mathcal{C}}} = \begin{pmatrix} f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \\ h_1 & h_2 & h_3 \end{pmatrix},$$

the condition that (M_1, M_2) fixes $F_{\mathcal{C}}$ means that $M_{F_{\mathcal{C}}}$ actually has the form (see Section 6.3)

$$M_{F_{\mathcal{C}}} = \begin{pmatrix} bf_3 & f_2 & f_1 \\ bg_3 & g_2 & g_3 \\ abf_1 & af_2 & af_3 \end{pmatrix}.$$

Let $\mathcal{S}$ be the largest subscheme of $\mathrm{Spec}(K[a, b, f_1, f_2, f_3, g_2, g_3])$ over which the scheme defined by the formula

$$\{x \in \mathbb{P}^1_{\mathcal{S}} \times_{\mathcal{S}} \mathbb{P}^1_{\mathcal{S}} \mid F_{\mathcal{C}}(x) = 0\}$$

is a smooth curve over $\mathcal{S}$. Let $\Lambda_{\mathcal{S}} = (\mathcal{C}/\mathcal{S}, (\mathcal{L}_1, \mathcal{L}_1), \mathcal{T})$ be the 2-prepared genus one curve defined by F_C.

6.2 The Main Theorem

Theorem 6.1 *Let $\mathcal{S}, \Lambda_{\mathcal{S}}$ be as above. Then*

$$\Lambda_{Jac,\mathcal{S}} = (\mathcal{E}/\mathcal{S}, (\mathcal{O}(O_{\mathcal{E}} + \mathcal{T}), \mathcal{L}_2 \otimes \mathcal{L}_1^{-1} \otimes \mathcal{O}(\mathcal{T})), \mathcal{T})$$

is the Jacobian of $\Lambda_{\mathcal{S}}$. The elliptic curve $\mathcal{E}$ is given by the $(2,2)$-form

$$F_{\mathcal{E}} = -\frac{(a(f_1+f_3)^2 - g_3^2)\, S_1^2}{(f_3 - f_1)^2} s^2x^2 + st\left(\frac{b\, S_1^2}{S_2}x^2 - S_2\, y^2\right)$$

$$+t^2\left(b\,\frac{S_1^2}{S_2}x^2 + S_2\,xy + S_2\,y^2\right),$$

where

$$S_1 = 2\sqrt{a}\frac{2f_2g_3 - f_1g_2 - f_3g_2}{a(f_1+f_3)^2 - g_3^2}, \qquad S_2 = \frac{4b(a(f_1+f_3)^2 - g_3^2) - 4af_2^2 - g_2^2}{a(f_1+f_3)^2 - g_3^2},$$

and with $\mathcal{O} = ((1:0),(1:0))$.

To prove Theorem 6.1 we will use the comments in Section 3.10 to reduce to proving it over the generic point of the base $\mathcal{S}$. Let

$$K' = K(a, b, f_1, f_2, f_3, g_2, g_3).$$

Then we need to find the Jacobian of the 2-prepared genus one curve

$$\Lambda = (C/K', (L_1, L_2), T)$$

where

$$C \xrightarrow{f_C} \mathbb{P}^1_{K'} \times_{K'} \mathbb{P}^1_{K'}$$

is given by the equation $F_{\mathcal{C}}(x) = 0$, for

$$F_{\mathcal{C}} : s^2(bf_3x^2+f_2xy+f_1y^2)+st\,(bg_3x^2+g_2xy+g_3y^2)+t^2(abf_1x^2+af_2xy+af_3y^2),$$

T is a K'-rational point of exact order two of the Jacobian of C, and

$$L_i = (pr_i \circ f_C)^*\mathcal{O}(1).$$

6.3 Standardizing the Model for C

Claim 6.1 *With the above representation (M_1, M_2) of λ_T acting on C, the equation for C is of the following form:* $M_F = \begin{pmatrix} bf_3 & f_2 & f_1 \\ bg_3 & g_2 & g_3 \\ abf_1 & af_2 & af_3 \end{pmatrix}$.

Proof. (M_1, M_2) is a linear operator on $V = < s^2x^2, s^2xy, s^2y^2, stx^2, \ldots >$, a nine dimensional K-vector space. Moreover, $(M_1, M_2)^2 = (M_1^2, M_2^2)$ acts by multiplcation by a^2b^2 on every basis vector $s^2x^2, s^2xy, \ldots$ of V. This means that λ_T has eigenspaces in V corresponding to the eigenvalues $\pm ab$. We have the following table which lists these eigenspaces:

eigenvector	eigenvalue
$bs^2x^2 \pm at^2y^2$	$\pm ab$
$s^2xy \pm at^2xy$	$\pm ab$
$s^2y^2 \pm abt^2x^2$	$\pm ab$
$bstx^2 \pm sty^2$	$\pm ab$
$stxy$	ab

The claim follows from the simple observation that every eigenvector with eigenvalue $-ab$ vanishes at the point $\begin{pmatrix} \sqrt{a} & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ \sqrt{b} \end{pmatrix}$. That means every $(2,2)$-form coming form the eigenspace corresponding to $-ab$ has a fixed point under λ. Since F has no such fixed point, it lives in the eigenspace corresponding to ab.$\square$

Remark. We have not demonstrated an algorithm which produces the f_i's, g_j's, a and b from the coefficients of a $(2,2)$-form; however, we have demonstrated that every 2-prepared genus one curve over K is in the family of $(2,2)$-forms above.

6.4 A Selmer-like Example

Assume for now that $a = b = 1$, that is the determinants of M_1 and M_2 are both 1 (mod squares). Then by Claim 3.11 we may assume

$$(M_1, M_2) = \left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right).$$

Since (M_1, M_2) fixes F_C we have

$$(M_1, M_2) \cdot M_{F_C} = \begin{pmatrix} f_1 & -f_2 & f_3 \\ -g_1 & g_2 & -g_3 \\ h_1 & -h_2 & h_3 \end{pmatrix} = M_{F_C} = \begin{pmatrix} f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \\ h_1 & h_2 & h_3 \end{pmatrix}$$

$$\Longrightarrow M_{F_C} = \begin{pmatrix} f_1 & 0 & f_3 \\ 0 & g_2 & 0 \\ h_1 & 0 & h_3 \end{pmatrix}.$$

Theorem 6.2 *Let $\Lambda = (C, (L_1, L_2), T)$ be a 2-prepared curve of genus one over K whose embedding in $\mathbb{P}^1_K \times \mathbb{P}^1_K$ is given by*

$$M_F = \begin{pmatrix} f_1 & 0 & f_3 \\ 0 & g_2 & 0 \\ h_1 & 0 & h_3 \end{pmatrix}.$$

Then the Jacobian $Jac(C) = E$ also embeds in $\mathbb{P}^1 \times \mathbb{P}^1$ with an equation given by

$$M_E = \begin{pmatrix} f_1 & 0 & -f_1 \\ 0 & g_2 & 0 \\ -h_1 f_3/f_1 & 0 & h_3 \end{pmatrix}$$

The map from C to E is given by an $L-$linear automorphism of $\mathbb{P}^1 \times \mathbb{P}^1$, where L is the field $K(\sqrt{-\frac{f_3}{f_1}})$.

Proof. We can assume that $f_1 \neq 0$ since if $f_1 = 0$, C is not smooth. I claim that the map $\phi_{x_0} : C \longrightarrow J(C) = E$ is the restriction of a linear automorphism of $\mathbb{P}^1 \times \mathbb{P}^1$ defined over $K(\sqrt{-\frac{f_3}{f_1}})$, namely the map

$$\phi : \begin{pmatrix} s & t \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} s & t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-\frac{f_3}{f_1}} \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-\frac{f_1}{f_3}} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$= \begin{pmatrix} s & \sqrt{-\frac{f_3}{f_1}}\, t \end{pmatrix}, \begin{pmatrix} x \\ \sqrt{-\frac{f_1}{f_3}}\, y \end{pmatrix}$$

This is clearly a map from C to E. Also, note that

$$E : s^2 \left(x^2 - y^2\right) + \frac{g_2}{f_1} s\, t\, x\, y + t^2 \left(-\frac{h_1 f_3}{f_1^2} x^2 + \frac{h_3}{f_1} y^2\right) = 0$$

has the rational point $(1:0), (1:1)$ so we can assign a group structure to E by letting this point be the origin.

To prove that E is actually isomorphic to the Jacobian of C, we form the cocycle $\xi \in H^1(Gal(\bar{K})/K), Aut(E)(K_s))$ defined by $\xi(\sigma) = \phi^\sigma \phi^{-1}$ for $\sigma \in Gal(\overline{K}/K)$. We'd like to show that ξ takes values in the group $E(K_s)$, thinking of $E(K_s)$ sitting inside $Aut(E)(K_s)$ as the translation maps. The image of ξ naturally falls into two cases; in the first, $\sigma(\sqrt{-a}) = \sqrt{-a}$, which clearly means that $\xi = \phi^\sigma \phi^{-1} = Id_E$. In the second, $\sigma(\sqrt{-a}) = -\sqrt{-a}$, and we calculate

$$\xi\left((s:t),(x:y)\right) = (-s:t),(-x:y).$$

Notice we can think of ξ as acting on the whole of $\mathbb{P}^1 \times \mathbb{P}^1$, since ϕ does. But this action is fixed-point free when we restrict to E, and so must be translation by some point of E. Moreover, the origin $(1:0),(1:1)$, is clearly mapped to $(1:0),(-1:1)$, and since the map is clearly an involution, we also conclude that $(1:0),(-1:1)$ is a two-torsion point of E. $\square$[1]

6.5 A Locally Trivial Sub-family

A main motivation for this thesis is to understand elements of Sha better. In that light we have the following example coming from $\mathbb{P}^1 \times \mathbb{P}^1$:

Let a and c be relatively prime integers, with a even. Define $b = c^2 + 4a$. Giving the coordinates (s,t) to the first $\mathbb{P}^1$ and the coordinates (x,y) to the second, define the following family of curves:

$$C_{a,c} : s^2(x^2 - ay^2) + c(a-b)\,stxy - ab\,t^2\,(x^2 - ay^2) = 0. \tag{1}$$

From Theorem 6.2, the Jacobian of this curve is the following:

$$E_{a,c} : s^2\,(x^2 - a^2y^2) + c(a-b)\,stxy - b\,t^2(x^2 - a^2y^2) = 0. \tag{2}$$

The origin of the Jacobian curve can be taken to be $\mathcal{O} = (1:0),(a:1)$; then there is full rational 2-torsion, given by

$$T = (1:0),(-a:1), \quad T' = (0:1),(a:1), \quad \text{and} \quad T+T' = (0:1),(-a:1).$$

The action of the non-trivial rational two-torsion point T is given on both curves by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

[1] This proof is similar to the proof in the "Construction of the Jacobian" chapter of Cassel's book [2].

sending t to $-t$ and y to $-y$ and fixing s and x. This is because the above curve is a "Selmer-like" curve. The action of "translation by T' on C" is given by

$$\begin{pmatrix} 0 & -1 \\ ab & 0 \end{pmatrix}, \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix},$$

and on E is given by

$$\begin{pmatrix} 0 & -1 \\ b & 0 \end{pmatrix}, \begin{pmatrix} 0 & a^2 \\ 1 & 0 \end{pmatrix}.$$

Claim 6.2 *The above family $C_{a,c}$ is locally trivial.*

Proof. Assume that a, b, and c are in $\mathbb{Z}$. Let's see why there is a rational point over $\mathbb{Q}_p$. If we let $t = 0, s = 1$, we are cutting the curve in a line and we get two point which are rational as a pair so either they are rational or they are conjugates defined over a quadratic field. This is determined by whether there is a solution to the equation $x^2 - ay^2 = 0$, i.e. whether a is a square in $\mathbb{Q}_p$. If instead we let $x = 1, y = 0$, we are asking whether ab is a square in $\mathbb{Q}_p$. Finally, if we let $s = a, t = 1$, we have

$$x^2(a^2 - ab) + xyac(a - b) + y^2\,(a^2b - a^3) = 0,$$

Which has a solution in $\mathbb{Q}_p$ whenever the discriminant $(c(a-b)a)^2 + 4(a^2 - ab)a(a^2 - ab)$ is a square in $\mathbb{Q}_p$. This is the same as asking whether $c^2 + 4a = b$ is a square in $\mathbb{Q}_p$. Now for any $p \not| 2ab$, one of a, b, and ab will be a square mod p, and by Hensel's Lemma we can lift to a solution in $\mathbb{Q}_p$. For $p|2ab$, we let $x = y = 1$, and we have $s^2(1-a) + c(a-b)\,st - ab\,t^2\,(1-a) = 0$,
Which has a solution in $\mathbb{Q}_p$ whenever the discriminant $c^2(a-b)^2 + 4ab(1-a)^2$ is a square in $\mathbb{Q}_p$. If $p|ab$, $p \neq 2$, this is congruent to a non-zero square mod p. To see that it is non-zero, assume $p \mid c(a-b)$; if $p \mid c$, since $p \mid ab$ and since $(a, c) = 1$ we have $p \mid b = c^2 + 4a \Rightarrow p \mid 4a$. If $p \mid (a-b)$, since $p \mid ab$ we have $p \mid a$ and $p \mid b \Rightarrow p \mid c$. If $p = 2$, we need to check that $c^2(a-b)^2 + 4ab(1-a)^2$ is 1 mod 8. Since $c^2(a-b)^2$ is an odd square and thus 1 mod 8, we want $4ab(1-a)^2$ 0 mod 8. Since a is even, we are done. □

Claim 6.3 *For specific choices a_0 and c_0 of a and c, The curve C_{a_0,c_0} is non-trivial in the Sha group of its Jacobian E_{a_0,c_0} whenever E_{a_0,c_0} has Mordell-Weil rank 0.*

Proof. We will make use of Claim 3.9 and Corollary 3.6. Let $E = E_{a_0,c_0}$ and $C = C_{a_0,c_0}$. We will again use the short exact sequence (page 197 of [8])

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

in conjunction with the map $e_2(-,T')^* : H^1(G, E[n](\overline{\mathbb{Q}})) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ which comes from pairing a cocycle with the 2-torsion point T'. First let's look at the composition of δ with $e(-,T')^*$. Certainly $\mathcal{O}$ is mapped to 1, since $e(-,T')^* \circ \delta$ is a homomorphism. Next, by Corollary 3.6, to find the image of $T+T'$ we need to map E to $\mathbb{P}^1$ by the divisor $(T+T')+T' \sim \mathcal{O}+T$, define the action "translation by T'" on this embedding to get an element $\lambda_{T'}$, and finally take the negative of its determinant. We already have a map like this, namely the projecion onto the first $\mathbb{P}^1$ of the above embedding $E \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1$. Since $\lambda_{T'}$ on this $\mathbb{P}^1$ is $\begin{pmatrix} 0 & -1 \\ b & 0 \end{pmatrix}$, the image of $T+T'$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is $-b$. So we know the image of $\mathcal{O}$ and $T+T'$ so far.

Lift $C \in H^1(G, E(\overline{\mathbb{Q}}))[n]$ to the pair $(C, 2\cdot x_0 + T') \in H^1(G, E[n](\overline{\mathbb{Q}}))$; by Claim 3.9 its image in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is the negative of the determinant of $\lambda_{T'}$ acting on the second projection of the embedding $C \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1$, i.e. the map to $\mathbb{P}^1$ corresponding to the divisor $2\cdot x_0 + T'$. We have seen above this $\lambda_{T'}$ is $\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$, so the image of C is a. To finish we want to see two things, firstly that the image of C in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is disjoint from the image of $E[2](\overline{\mathbb{Q}})$, and secondly that the image of $E[2](\overline{\mathbb{Q}})$ is non-trivial. The latter will let us conclude that there are no rational four-torsion points, which means the contribution of the left-hand group $E(Q)/n\,E(Q)$ in the above exact sequanece comes only from 2-torsion and possibly rank; the former will let us conclude that C does not come from the 2-torsion, so must either be nontrivial in Sha or correspond to a point of infinite order in the Mordell-Weil group of $E(K)$. To finish it is sufficient to show that the image of T' is not in general $-ab$. we will study the map $e(-,T')^* \circ \delta$ directly. δ maps T' to the cocycle class of $S - S^\sigma$, where $2\cdot S = T'$. This means S is a point of strict order 4. Using properties of the Weil pairing from [8], $e(-,T')^*(S-S^\sigma) = e_2(S-S^\sigma, T) = e_2(S-S^\sigma, 2\cdot S) = e_2(2\cdot S, S-S^\sigma)^{-1} = e_4(S, S-S^\sigma)^{-1} = e_4(S-S^\sigma, S) = e_4(S,S)/e_4(S^\sigma, S) = e_4(S, S^\sigma)$. Given an explicit formula for S, we can ascertain this cocycle. Since $E \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{pr_2} \mathbb{P}^1$ is given by the divisor $\mathcal{O} + T'$, such an S will be a ramification point of this double cover of

$\mathbb{P}^1$. In other words S will be fixed by one of the two geometric involutions. We see that S is one of the four points that has fixed $(x : y)$ coordinates under the second involution. We can find S from the formula for E by looking for x/y in terms of s and t and seeing where we get a double root. $E : s^2\,(x^2 - a^2y^2) + c(a-b)\,stxy - b\,t^2(x^2 - a^2y^2) = 0$. We rewrite this as $E : x^2 \cdot \alpha + xy \cdot \beta + y^2 \cdot \gamma = 0$, with $\alpha = s^2 - b \cdot t^2$, $\beta = s \cdot t \cdot c(a-b)$, and $\gamma = -a^2 \cdot \alpha$. The solution

$$x/y = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$$

will have a double root when the discriminant $\beta^2 - 4\alpha \cdot \gamma$ is zero, i.e. when $\beta^2 = 4\alpha \cdot \gamma = -4a^2 \cdot \alpha^2$. This happens when $\beta = \pm 2ai \cdot \alpha$. Choosing $\beta = 2ai \cdot \alpha$ and solving for s and t we find

$$s/t = \frac{c(a-b) \pm \sqrt{(c(a-b))^2 - 4(2ai)(-2abi)}}{2ai} =$$

$$\frac{c(a-b) \pm \sqrt{(c(a-b))^2 - 16a^2b}}{2ai}$$

Also we see that $x/y = -\beta/(2\alpha) = ai$. So the point S is given by

$$(s : t), (x : y) = \left(\frac{c(a-b) + \sqrt{(c(a-b))^2 - 16a^2b}}{2ai} : 1 \right), (ai : 1).$$

There are two obvious Galois elements that act on S; first, complex conjugation $\bar{\ }$ which takes i to $-i$, and second τ with $\tau(\sqrt{(c(a-b))^2 - 16a^2b}) = -\sqrt{(c(a-b))^2 - 16a^2b}$. The Galois conjugates of S are the four points of exact order 4 whose double is T', namely $S, S+T, S+T'$, and $S+T+T'$. Only $S+T$ and $S+T+T'$ pair with S non-trivially. We can act on S by λ_T to find $S+T$, and we get $S+T = \left(-\frac{c(a-b) \pm \sqrt{(c(a-b))^2 - 16a^2b}}{2ai} : 1 \right), (-ai : 1)$ Also, $(ai : 1)$ is mapped to $(-ai : 1)$ by $\lambda_{T'}$. Thus $\lambda_{T+T'}$ must fix $(ai : 1)$, so

$$S + T + T' = \left(\frac{c(a-b) - \sqrt{(c(a-b))^2 - 16a^2b}}{2ai} : 1 \right), (ai : 1)$$

and we find that $\tau(S) = S + T + T'$ so $\tau \in ker(e^*(S - S^\sigma, T))$. This means that the image of T' is $(c(a-b))^2 - 16a^2b$. Whenever a is not equivalent mod squares to $-b$, $(c(a-b))^2 - 16a^2b$, and $b \cdot ((c(a-b))^2 - 16a^2b)$, and when $(c(a-b))^2 - 16a^2b$ is not a square itself, C does not come from the two-torsion group. $\square$

Corollary 6.1 *There is no global section in the family $C_{a,c}$*

Proof. The curve $E_{a=-4,\,c=3}$ has a conductor which is not divisible by 9 (so E is modular) and an $L-$series which does not vanish at $s=1$ (both were computed by gp with the help of Adam Logan). We need only check that $(c(a-b))^2 - 16a^2b = (3\cdot 3)^2 - 16 \cdot 4^2 \cdot (-7) = 1873$ is not a square and that is not congruent modulo sqaures to -4 or 7. It is prime. $\square$

6.6 Finding x_0

By Claim 3.7, we are searching for a point x_0 such that $\mathcal{O}(x_0 + (x_0 + T)) \cong L_1$. The cocycle $x_0 - x_0^\sigma$ will then take values in $E[2](K_s)$ (see Claim 3.6). Moreover as in the proof of Claim 3.5 we will be able to extend a map $\varphi_{x_0} : C \longrightarrow E$ to the entire multi-projective space $\mathbb{P}^1_{K'} \times \mathbb{P}^1_{K'}$ We can use geometry to locate the potential x_0's as follows: We want (see page 49)

$$\mathcal{O}(x_0 + (x_0 + T)) \cong L_1 \iff \kappa(x_0) = x_0 + T = (M_1, M_2) \cdot x_0.$$

We observe that κ_1 fixes the first coordinate of points, whereas

$$M_1 = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}.$$

Thus the first coordinate of x_0 is a fixed point under that matrix, i.e. $(\sqrt{a} : 1)$ or $(-\sqrt{a} : 1)$. We will denote these v_0 and v_1, respectively, to maintain consistent notation with the other chapters. There are four possible choices for x_0, so it makes sense that we have two possible choices for the first coordinate; let's choose the first coordinate of x_0 to be $v_0 = \begin{pmatrix} \sqrt{a} & 1 \end{pmatrix}$. Then the fact that x_0 is in C means that the second coordinate of x_0 must satisfy the equation

$$F_C(x_0) = F_C((\sqrt{a} : 1), (X : Y)) = 0,$$

or in other words

$$\begin{pmatrix} a & \sqrt{a} & 1 \end{pmatrix} \begin{pmatrix} bf_3 & f_2 & f_1 \\ bg_3 & g_2 & g_3 \\ abf_1 & af_2 & af_3 \end{pmatrix} \begin{pmatrix} X^2 \\ XY \\ Y^2 \end{pmatrix} = 0.$$

We simplify to get the quadratic equation

$$bX^2 + \frac{2af_2 + \sqrt{a}g_2}{a(f_1 + f_3) + \sqrt{a}g_3} XY + Y^2 = 0.$$

For ease of notation, define

$$B = \frac{2af_2 + \sqrt{a}g_2}{a(f_1 + f_3) + \sqrt{a}g_3} \text{ and } B' = \frac{2af_2 - \sqrt{a}g_2}{a(f_1 + f_3) - \sqrt{a}g_3}.$$

Then we have the equation $bX^2 + BXY + Y^2 = 0$, which we solve for Y/X and get two solutions $\delta_0 = (-B + \sqrt{B^2 - 4b})/2$ and $\delta_1 = (-B - \sqrt{B^2 - 4b})/2$, with the properties

- $\delta_0 + \delta_1 = -B$
- $\delta_0 \cdot \delta_0 = b$
- $\delta_0 - \delta_1 = \sqrt{B^2 - 4b}$
- δ_0 and δ_1 are defined over the field $K'\left(\sqrt{a}, \sqrt{B^2 - 4b}\right)$.

Let $\Delta_0 = \begin{pmatrix} 1 \\ \delta_0 \end{pmatrix}$ and $\Delta_1 = \begin{pmatrix} 1 \\ \delta_1 \end{pmatrix}$; we now have $x_0 = (v_0, \Delta_0)$ and $x_0 + T = (v_0, \Delta_1)$. The map φ from C to E is defined over $K'(x_0) = K'(\sqrt{a}, \sqrt{B^2 - 4b})$.

Remark. Work for the duration of this Remark over the field K, where we consider f_i's, g_j's, a and b as elements of K. It doesn't look as if the field of definition of φ is well-defined, since a and b are only defined "up to squares" in K. If we change a by u^2 we see that $K(\sqrt{a})$ hasn't changed, but it doesn't look like $\sqrt{B^2 - 4b}$ behaves well with such a change. We will see that it does, however. M_C, the matrix of coefficients, has the property that it is fixed by the map

$$\lambda_T = (\alpha, \beta) = \left(\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \right).$$

That is, we have $\Psi(\alpha) \cdot M_C \cdot \Phi(\beta) = M_C$. Changing b by a square v^2 must change $M_C = M_C(a,b)$ to $M_C(a, bv^2)$ such that it is fixed by the map $\lambda_T(a, bv^2)$, i.e. such that $\Psi(\alpha) \cdot M_C(a, bv^2) \cdot \Phi(\beta(a, bv^2)) = M_C$. Since

$$\begin{pmatrix} v & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ bv^2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix},$$

the equality $\Psi(\alpha) \cdot M_C \cdot \Phi(\beta) = M_C$ is equivalent to

$$\Psi(\alpha) \left(M_C \cdot \Phi \begin{pmatrix} v & 0 \\ 0 & 1 \end{pmatrix} \right) \Phi \begin{pmatrix} 0 & 1 \\ bv^2 & 0 \end{pmatrix} = \left(M_C \cdot \Phi \begin{pmatrix} v & 0 \\ 0 & 1 \end{pmatrix} \right),$$

and hence we have

$$M_C(a, bv^2) = M_C \cdot \Phi \begin{pmatrix} v & 0 \\ 0 & 1 \end{pmatrix} = M_C \cdot \begin{pmatrix} v^2 & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} bv^2 f_3 & f_2 v & f_1 \\ bv^2 g_3 & g_2 v & g_3 \\ abv^2 f_1 & af_2 v & af_3 \end{pmatrix}.$$

We see that the change $b \mapsto bv^2$ transforms $f_1 \mapsto f_1, f_3 \mapsto f_3, g_3 \mapsto g_3, f_2 \mapsto vf_2$, and $g_2 \mapsto vg_2$. Thus $B \mapsto Bv$, and the field $K(\sqrt{a}, \sqrt{B^2 - 4b})$ is indeed well-defined.

Claim 6.4 *The normal closure L of $K'(x_0)$ is a degree eight extension of K' with a dihedral Galois group; it is the field of definition of x_0 and its conjugates.*

Proof. Neither $\sqrt{a}$ is in K' nor $\sqrt{B^2 - 4b}$ is in $K'(\sqrt{a})$. Notice that the set of points x such that $\mathcal{O}(2 \cdot x + T) \cong L_1$ is a Galois invariant set, contains x_0 by construction, and is in fact the orbit of x_0 under the translation by two-torsion point maps, since for $T' \in E[2](K'_s)$,

$$\mathcal{O}(2 \cdot (x + T') + T) \cong L_1 \Leftrightarrow \mathcal{O}(2 \cdot x + T) \cong L_1.$$

In the Galois group G of the normal closure L of $K'(x_0)$ there will be some element σ such that $\sigma(\sqrt{a}) = -\sqrt{a}$; Then σ brings x_0 to $x_0 + T'$, where

$T' \in E[2](\overline{K})$. We know $T \neq T'$ because $x_0 + T$ has the same first coordinate as x_0, namely v_0. The second coordinate of $x_0 + T'$ must satisfy the equation

$$(Y/X)^2 + (\sigma B)\, Y/X + b = 0,$$

so $x_0 + T'$ is defined over the field $K(-\sqrt{a}, \sqrt{(\sigma B)^2 - 4b})$. Note that σB is B' from above. We have exhibited that L is at most a degree 8 extension of K, as all of the possible conjugates of x_0 are defined over the field $K(\sqrt{a}, \sqrt{(B')^2 - 4b}, \sqrt{B^2 - 4b})$. Moreover, L is the splitting field of the following polynomial defined over K:

$$[Z^2+BZ+b]\cdot[Z^2+B'Z+b] = Z^4+(B+B')Z^3+(BB'+2b)Z^2+b(B+B')Z+b^2.$$

The Galois group is a non-commutative group, since the field extension $K(\sqrt{a}, \sqrt{(B')^2 - 4b})$ is not normal. Thus it must be the dihedral group of eight elements. □

6.7 Standardizing the Model for E

Claim 6.5 *We may assume that E is embedded in $\mathbb{P}^1 \times \mathbb{P}^1$ with the following properties:*

- $\mathcal{O} = (1:0)\,, (1:0)$
- $T = (1:0)\,, (0:1)$
- *Let T' and $T' + T$ be the other two-torsion points in $E(\overline{K})$. They both have first coordinate* $(0:1)$.
- *"Translation by T" $= \lambda_{T,E}$ on E is given by*

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ ab & 0 \end{pmatrix} \right).$$

Proof. The first representative matrix of $\lambda_{T,E}$ can be put in the above form by Claim 3.10. The map $proj_2 \circ f_E$ from E to the second $\mathbb{P}^1$ is given by the divisor $L_2 \otimes L_1^{-1} \otimes \mathcal{O}(T)$ (see the discussion at the beginning of Section 6.6), and by the properties of the det map (see Claim 3.6) we have

$$det(E, Q_2) = \frac{det(C, D_2) \cdot det(E, T)}{det(C, D_1)} = -a/b.$$

Since det takes values in K^*/K^{*2}, we may lift

$$det(E, Q_2) = -ab,$$

and we can compose f_E with a linear map to put λ_T in the above form. Since $proj_1 \circ f_E$ is given by the divisor $\mathcal{O} + T$, we know the points $\mathcal{O}$ and T lie on a (1,0)-form which is stable under the action of λ_T, and the same can be said about the points T' and $T' + T$. Then the first coordinate of $\mathcal{O}$ is either $(1:0)$ or $(0:1)$, and if it's $(0:1)$ we compose f_E with the map

$$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, I\right);$$

this permutes the two coordinates and commutes with λ_T.

Finally, to see that we can fix the second coordinates of $\mathcal{O}$ and T as above, note that we need only fix the second coordinate of $\mathcal{O}$ since we can act by λ_T to get T; to do so, we note that $\mathcal{O}$ is not fixed by λ_T, so since the first coordinate is fixed, the second coordinate isn't. We can compose f_E by the linear map

$$\left(I, \alpha I + \beta \begin{pmatrix} 0 & 1 \\ ab & 0 \end{pmatrix}\right),$$

and for appropriate α and β we can move the second coordinate of $\mathcal{O}$ to $(1:0)$.□

6.8 Finding φ

Let L be the Galois closure of $K'(x_0)$ as in Claim 6.4. Fix $\sigma \in Gal(L/K')$ such that $\sigma(\sqrt{a}) = -\sqrt{a}$. There will be four such elements, since the natural map

$$Gal(L/K') \longrightarrow Gal(K'(\sqrt{a})/K')$$

is surjective with kernel $Gal(L/K'(\sqrt{a}))$, of size four. Let $\tau \in Gal(L/K')$ be an element such that $\tau(\sqrt{a}) = \sqrt{a}$ and $\tau(\sqrt{B^2 - 4b}) = -\sqrt{B^2 - 4b}$. Then $\tau(\delta_0) = \delta_1, \tau(\delta_1) = \delta_0, \tau(\Delta_0) = \delta_1, \tau(\Delta_1) = \Delta_0$, and $\tau^2 = 1$.

Claim 6.6 *Let σ and τ be as above. Let φ be the linear automorphism carrying C to $Jac(C) = E$. Then if φ is represented by the automorphism $(\alpha^{-1}, \beta^{-1}, \epsilon = 0) \in Aut(\mathbb{P}^1_L \times_L \mathbb{P}^1_L)$, we have*

$$\tau\alpha^{-1}\alpha = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \qquad \text{and} \qquad \beta\tau\beta^{-1} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}.$$

Moreover, $\sigma\alpha^{-1}\alpha$ and $\beta\sigma\beta^{-1}$, which correspond to translation by another two-torsion point on C, are both non-trivial elements of $PGL_2(L)$ of order two and have trace zero.

Proof. By the choice of x_0, we know that the cocycle created by φ on C, namely $\xi_C(\gamma) = \varphi^{-1}\varphi^{\gamma}$ for $\gamma \in Gal(L/K')$, will be the translation map by some two torsion point; which will be determined by seeing where x_0 goes.

$$\begin{aligned} \varphi^{\gamma}(x_0) &= (\alpha^{-1}, \beta^{-1})^{\gamma} \circ (v_0, \Delta_0) \\ &= \begin{pmatrix} \sqrt{a} & 1 \end{pmatrix} (\alpha^{-1})^{\gamma},\ (\beta^{-1})^{\gamma} \begin{pmatrix} 1 \\ \delta_0 \end{pmatrix} \\ &= \left(\begin{pmatrix} \gamma^{-1}(\sqrt{a}) & 1 \end{pmatrix} \alpha^{-1}, \beta^{-1} \begin{pmatrix} 1 \\ \gamma^{-1}\delta_0 \end{pmatrix} \right)^{\gamma}. \end{aligned}$$

Let's replace γ by τ above:

$$\varphi^{\tau}(x_0) = \left(\begin{pmatrix} \sqrt{a} & 1 \end{pmatrix} \alpha^{-1}, \beta^{-1} \begin{pmatrix} 1 \\ \delta_1 \end{pmatrix} \right)^{\tau} = (\varphi(x_0 + T))^{\tau} = \tau(T) = T.$$

By Claim 3.4 we know "translation by torsion point matrices" (defined over $\overline{K}'$) have distinct eigenvalues. Since any such element of $PGL_2(\overline{K}')$ of order two can be conjugated over $\overline{K}'$ to a diagonal matrix with eigenvalues ± 1, its trace is zero. Note that the trace function is invariant under conjugation and although it is not invariant under scaling, the vanishing of the trace function is well-defined for elements of $PGL_n(K')$.

Let's see what the previous conditions impose on the cocycle on E: for τ as in Claim 6.6,

$$\tau\alpha\alpha^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \& \quad \beta^{-1}\tau\beta = \begin{pmatrix} 0 & 1 \\ ab & 0 \end{pmatrix}$$

$$\implies \tau\alpha = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \alpha \quad \& \quad \tau\beta = \beta \cdot \begin{pmatrix} 0 & 1 \\ ab & 0 \end{pmatrix}.$$

Since φ sends x_0 to $\mathcal{O}$, we have

$$v_0 \cdot \alpha^{-1} = \begin{pmatrix} * & 0 \end{pmatrix}.$$

The first coordinate of T' is also known up to a scalar:

$$v_1 \cdot \alpha^{-1} = \begin{pmatrix} 0 & *' \end{pmatrix}.$$

We conclude that α is of the form

$$\alpha = \begin{pmatrix} v_0 \\ c \cdot v_1 \end{pmatrix},$$

for some $c \in K'(x_0)$. A similar analysis of β reveals that

$$\beta = \begin{pmatrix} d \cdot \Delta_0 & \Delta_1 \end{pmatrix}$$

for some $d \in K'(x_0)$.

The above conditions on α and β give

$$\tau\alpha = \begin{pmatrix} \tau(v_0) \\ \tau(c \cdot v_1) \end{pmatrix} = \begin{pmatrix} v_0 \\ \tau(c) \cdot v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \alpha = \begin{pmatrix} v_0 \\ -c \cdot v_1 \end{pmatrix}.$$

Then $\tau(c) = -c$. We know α has coefficients in $K'(x_0)$, and since $c/\sqrt{B^2 - 4b}$ is fixed by the non-trivial Galois element in $\mathrm{Gal}(K'(x_0)/K'(\sqrt{a}))$,

$$c = c' \cdot \sqrt{B^2 - 4b} = c'(\delta_0 - \delta_1)$$

for some $c' \in K'(\sqrt{a})$:

$$\alpha = \begin{pmatrix} v_0 \\ c' \cdot (\delta_0 - \delta_1) \cdot v_1 \end{pmatrix},$$

Similarly for β, we write $\tau\beta =$

$$\begin{pmatrix} \tau(d) \cdot \Delta_1 & \Delta_0 \end{pmatrix} = \beta \begin{pmatrix} 0 & 1 \\ ab & 0 \end{pmatrix} = \begin{pmatrix} ab \cdot \Delta_1 & d \cdot \Delta_0 \end{pmatrix} = \begin{pmatrix} \frac{ab}{d} \cdot \Delta_1 & \Delta_0 \end{pmatrix},$$

from which we conclude that $\tau(d) = ab/d$.

From Claim 6.6 we have the "Translation by T on C" matrices:

$$\tau\alpha^{-1}\alpha = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \beta\tau\beta^{-1} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}.$$

This doesn't give us any new information about α, but for β we have:

$$\beta = \begin{pmatrix} d\cdot\Delta_0 & \Delta_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}\cdot\tau\beta = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}\cdot\begin{pmatrix} \tau(d)\cdot\Delta_1 & \Delta_0 \end{pmatrix} =$$

$$\begin{pmatrix} \tau(d)\cdot\delta_1 & \delta_0 \\ \tau(d)\cdot b & b \end{pmatrix} = \begin{pmatrix} \tau(d)\cdot\delta_1/\delta_0 & 1 \\ \tau(d)\cdot b/\delta_0 & b/\delta_0 \end{pmatrix} = \begin{pmatrix} (\tau(d)\delta_1/\delta_0)\cdot\Delta_0 & \Delta_1 \end{pmatrix},$$

since $\delta_0\,\delta_1 = b$. We conclude that $d/\tau(d) = \delta_1/\delta_0 = \delta_1/\tau\delta_1$. That is, d/δ_1 is fixed by τ, which is a nontrivial element of $\mathrm{Gal}(K'(x_0)/K'(\sqrt{a}))$; therefore $d = d'\cdot\delta_1$, for some $d' \in K'(\sqrt{a})$. We have

$$\alpha = \begin{pmatrix} v_0 \\ c'(\delta_0-\delta_1)\cdot v_1 \end{pmatrix}, \beta = \begin{pmatrix} d'\delta_1\cdot\Delta_0 & \Delta_1 \end{pmatrix}.$$

We are left to find $c', d' \in K(\sqrt{a})$. Let F_E be (2,2)-form which gives E. Since the coefficients of F_E are rational, we will be able to deduce c' and d'.

The linear operators α and β also act linearly on the nine dimensional vector space V of $(2,2)$-forms in the following way:

$$\gamma\circ M_{F_C} = \Psi(\alpha)\cdot M_{F_C}\cdot\Phi(\beta),$$

where Ψ and Φ are the "Sym^2" homomorphisms

$$\Psi,\Phi : PGL_2(\overline{K}) \longrightarrow PGL_3(\overline{K}),$$

with $\Psi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix}$ and $\Phi(\alpha^\tau) = \Psi(\alpha)^\tau$. If M_{F_C} is the matrix of coefficients of C, then $M_{F_E} = \Psi(\alpha)\cdot M_{F_C}\cdot\Phi(\beta)$ is the matrix of coefficients of E. The top left and right corners of M_{F_E} the product vanish, since $\mathcal{O} = ((1:0),(1:0))$ and $T = ((1:0),(0:1))$ are on the curve E.

The middle entry in the matrix is also zero, since:

$$\begin{pmatrix} 2ac'(\delta_0-\delta_1) & 0 & -2c'(\delta_0-\delta_1) \end{pmatrix} \cdot \begin{pmatrix} bf_3 & f_2 & f_1 \\ bg_3 & g_2 & g_3 \\ abf_1 & af_2 & af_3 \end{pmatrix} \cdot \begin{pmatrix} 2d'\delta_1 \\ d'(\delta_1^2+b) \\ 2d'b\delta_1 \end{pmatrix} =$$

$$(-2c'(\delta_0-\delta_1)\cdot d'\delta_1) \begin{pmatrix} -a & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} bf_3 & f_2 & f_1 \\ bg_3 & g_2 & g_3 \\ abf_1 & af_2 & af_3 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ \delta_1+\delta_0 \\ 2b \end{pmatrix} =$$

$$(-2c'(\delta_0-\delta_1)\cdot d'\delta_1) \begin{pmatrix} ab(f_1-f_3) & 0 & -a(f_1-f_3) \end{pmatrix} \cdot \begin{pmatrix} 2 \\ \delta_1+\delta_0 \\ 2b \end{pmatrix} = 0.$$

So far we have computed the following coefficients of M_{F_E}: $M_{F_E}(1,1) = M_{F_E}(1,3) = M_{F_E}(2,2) = 0$. In order to compute the other entries, we will define two bilinear forms that will be useful. Since F_C is a (2,2)-form, if we fix one of the coordinates it becomes a quadratic function of the other coordinates. Then we can define the following:

$$B_L(v,v',w) = F_C(v+v',w) - F_C(v,w) - F_C(v',w)$$

$$B_R(v,w,w') = F_C(v,w+w') - F_C(v,w) - F_C(v,w')$$

Then:

$M_{F_E}(1,2) = B_R(v_0, d'\delta_1\Delta_0, \Delta_1) = B_R(v_0,\Delta_0,\Delta_1)\cdot d'\delta_1$
$M_{F_E}(2,1) = B_L(v_0, c'(\delta_0-\delta_1)v_1, d'\delta_1\Delta_0) = B_L(v_0,v_1,\Delta_0)\cdot c'(\delta_0-\delta_1)(d'\delta_1)^2$
$M_{F_E}(2,3) = B_L(v_0, c'(\delta_0-\delta_1)v_1, \Delta_1) = B_L(v_0,v_1,\Delta_1)\cdot c'(\delta_0-\delta_1)$
$M_{F_E}(3,1) = F_C(c'(\delta_0-\delta_1)v_1, d'\delta_1\Delta_0) = F_C(v_1,\Delta_0)\cdot (c'(\delta_0-\delta_1)d'\delta_1)^2$
$M_{F_E}(3,2) = B_R(c'(\delta_0-\delta_1)v_1, d'\delta_1\Delta_0, \Delta_1) = B_R(v_1,\Delta_0,\Delta_1)\cdot (c'(\delta_0-\delta_1))^2 d'\delta_1$
$M_{F_E}(3,3) = F_C(c'(\delta_0-\delta_1)v_1, \Delta_1) = F_C(v_1,\Delta_1)\cdot (c'(\delta_0-\delta_1))^2$

We compute

$B_R(v_0,\Delta_0,\Delta_1) = (a(f_1+f_3)+\sqrt{a}g_3)(4b-B^2)$
$B_L(v_0,v_1,\Delta_0) = 2a\delta_0(\delta_1-\delta_0)(f_1-f_3)$
$B_L(v_0,v_1,\Delta_1) = -2a\delta_1(\delta_1-\delta_0)(f_1-f_3)$
$F_C(v_1,\Delta_0) = \delta_0(B'-B)(a(f_1+f_3)-\sqrt{a}g_3)$
$B_R(v_1,\Delta_0,\Delta_1) = (4b-BB')(a(f_1+f_3)-\sqrt{a}g_3)$
$F_C(v_1,\Delta_1) = \delta_1(B'-B)(a(f_1+f_3)-\sqrt{a}g_3)$

From the above we can determine c' and d' up to multiplication by an element of K'. Since E is defined over K', the ratios of the above coefficients are in K' : we can divide out by any non-zero coefficient to get rational coefficients. In general the above coefficients are non-zero. Then

$$M_{F_E}(3,2)/M_{F_E}(3,3) = \frac{B_R(v_1, \Delta_0, \Delta_1) \cdot (c'(\delta_0 - \delta_1))^2 d'\delta_1}{F_C(v_1, \Delta_1) \cdot (c'(\delta_0 - \delta_1))^2} = d'' \in K',$$

so we have

$$d' = d'' \frac{F_C(v_1, \Delta_1)}{B_R(v_1, \Delta_0, \Delta_1) \cdot \delta_1}.$$

We simplify and expand this to get

$$d' = d'' \frac{(B' - B)}{(4b - BB')}$$

If σ is the nontrivial element of $\mathrm{Gal}(K'(\sqrt{a})/K')$, then $\sigma(d') = -d'$, since $\sigma(B) = B'$ and $\sigma(B') = B$.

Next we find c' up to an element of K'.

$$M_{F_E}(3,1)/M_{F_E}(2,1) = \frac{F_C(v_1, \Delta_0) \cdot (c'(\delta_0 - \delta_1) d'\delta_1)^2}{B_L(v_0, v_1, \Delta_0) \cdot c'(\delta_0 - \delta_1)(d'\delta_1)^2} = c'' \in K',$$

so

$$c' = c'' \frac{B_L(v_0, v_1, \Delta_0)}{F_C(v_1, \Delta_0) \cdot (\delta_0 - \delta_1)}.$$

This simplifies to

$$c' = c'' \frac{2a(f_3 - f_1)}{(B' - B)(a(f_1 + f_3) - \sqrt{a} g_3)}, c'' \in K'.$$

Now we have almost finished defining the map φ; the ambiguities remaining are the constants c'' and d'' in K'. As in the cases of $\mathbb{P}^2$ and $\mathbb{P}^4$, we will have more rigidity if we fixed the other translation by two torsion matrices on the Jacobian curve. However, unlike those cases, we will not be completely rigid even when we do that- the reason is that the centralizer of the image of χ is no longer itself. Indeed since the image of χ lands in the product space $PGL_2(\overline{K}) \times PGL_2(\overline{K})$, any element of $\{I\} \times Im(pr_2 \circ \chi)$ is in the centralizer of χ. Altogether we have

$$\alpha = \begin{pmatrix} v_0 \\ c'' \frac{a(f_3-f_1)(\delta_0-\delta_1)}{(B'-B)(a(f_1+f_3)-\sqrt{a}g_3)} \cdot v_1 \end{pmatrix}, \beta = \begin{pmatrix} d'' \frac{(B'-B)}{(4b-BB')}\delta_1 \cdot \Delta_0 & \Delta_1 \end{pmatrix}.$$

Let $S = (c'(\delta_0 - \delta_1))^2(d'\delta_1)(a(f_1 + f_3) - \sqrt{a}g_3)$. Then upon dividing $M_{F_E}(3,2)$ by S, we get

$$M_{F_E}(3,2)/S = \frac{B_R(v_1,\Delta_0,\Delta_1)}{(a(f_1+f_3)-\sqrt{a}g_3)} = 4b - BB' \in K'.$$

Similarly, we get

$$M_{F_E}(3,3)/S = \frac{F_C(v_1,\Delta_1)}{(d'\delta_1)(a(f_1+f_3)-\sqrt{a}g_3)} = \frac{B'-B}{d'} = \frac{(4b-BB')}{d''},$$

$$M_{F_E}(3,1)/S = \frac{d'\delta_1 F_C(v_1,\Delta_0)}{a(f_1+f_3)-\sqrt{a}g_3} = d'\delta_1\delta_0(B'-B) = d''b\frac{(B'-B)^2}{(4b-BB')},$$

$$M_{F_E}(1,2)/S = \frac{B_R(v_0,\Delta_0,\Delta_1)}{(c'(\delta_0-\delta_1))^2(a(f_1+f_3)-\sqrt{a}g_3)} =$$

$$\frac{(a(f_1+f_3)+\sqrt{a}g_3)(4b-B^2)}{(c'(\delta_0-\delta_1))^2(a(f_1+f_3)-\sqrt{a}g_3)} = \frac{-(a(f_1+f_3)^2-g_3^2)(B'-B)^2}{(c''(f_3-f_1))^2},$$

$$M_{F_E}(2,1)/S = \frac{B_L(v_0,v_1,\Delta_0)d'\delta_1}{c'(\delta_0-\delta_1)(a(f_1+f_3)-\sqrt{a}g_3)} = \frac{-2a\delta_0(f_1-f_3)d'\delta_1}{c'(a(f_1+f_3)-\sqrt{a}g_3)} =$$

$$\frac{-2a\delta_0(f_1-f_3)d''\frac{(B'-B)}{(4b-BB')}\delta_1}{c''\frac{2a(f_3-f_1)}{(B'-B)(a(f_1+f_3)-\sqrt{a}g_3)}(a(f_1+f_3)-\sqrt{a}g_3)} = \frac{bd''(B'-B)^2}{c''(4b-BB')},$$

$$M_{F_E}(2,3)/S = \frac{B_L(v_0,v_1,\Delta_1)}{c'd'(\delta_0-\delta_1)\delta_1(a(f_1+f_3)-\sqrt{a}g_3)} = \frac{2a(f_1-f_3)}{c'd'(a(f_1+f_3)-\sqrt{a}g_3)}$$

$$= \frac{-(4b-BB')}{c''d''}$$

We have now shown:

Claim 6.7 *The resulting matrix for E is given by:*

$$M_{F_E} = \begin{pmatrix} 0 & \frac{-(a(f_1+f_3)^2-g_3^2)(B'-B)^2}{(c''(f_3-f_1))^2} & 0 \\ \frac{bd''(B'-B)^2}{c''(4b-BB')} & 0 & \frac{-(4b-BB')}{c''d''} \\ d''b\frac{(B'-B)^2}{(4b-BB')} & 4b-BB' & \frac{(4b-BB')}{d''} \end{pmatrix}$$

Now our earlier observation that $\tau dd = ab$ tells us $(d'')^2 = 1$.

Note that if we multiplied the (2,2)-form F_C by a constant, we would not have a different matrix for E; this is because each coefficient has "weight zero" in terms of the coefficients of F. A simple calculation shows that

$$B' - B = 2\sqrt{a}\frac{2f_2g_3 - f_1g_2 - f_3g_2}{a(f_1+f_3)^2 - g_3^2}$$

and

$$4b - BB' = \frac{4b(a(f_1+f_3)^2 - g_3^2) - 4af_2^2 - g_2^2}{a(f_1+f_3)^2 - g_3^2}.$$

To finish the proof of Theorem 6.1 let $c'' = d'' = 1$.

References

[1] Atiyah, M.F. and Wall, Cohomology of Groups, in Cassels, Fröhlich, (eds.), *Algebraic Number Theory,* 94-115, Academic Press, London, 1967.

[2] Cassels, J. W. S., *Lectures on Elliptic Curves,* Cambridge University Press, Cambridge (1991)

[3] Faltings, G., and Chai, C.-L, *Degenerations of Abelian Varieties,* Springer-Verlag, Berlin, 1980.

[4] Hartshorne, Robin, *Algebraic Geometry,* Springer-Verlag, New York, 1977.

[5] Milne, J. S., Abelian Varieties, in Cornell, G, Silverman, (eds.), *Arithmetic Geometry,* 103-150, Springer-Verlag, New York, 1986.

[6] Milne, J. S., Jacobian Varieties, in Cornell, G, Silverman, (eds.), *Arithmetic Geometry,* 167-212, Springer-Verlag, New York, 1986.

[7] Mumford, David, *Abelian Varieties,* Oxford University Press, Oxford, 1970.

[8] Silverman, Joseph H., *The Arithmetic of Elliptic Curves,* Springer-Verlag, New York (1986)