THE JACOBIAN AND FORMAL GROUP OF A CURVE OF GENUS 2 OVER AN ARBITRARY GROUND FIELD

E. V. Flynn, Mathematical Institute, University of Oxford

§0. Introduction

The ability to perform practical computations on particular cases has greatly influenced the theory of elliptic curves. First, it has allowed a rich sub-branch of the Mathematics of Computation to develop, devoted to elliptic curves: the search for curves of large rank, large torsion over number fields, and — more recently — the application of elliptic curves to the factorisation of large integers [8]. Second, computation with special curves has motivated, and formed a testing ground for, many of the deep conjectures of the general theory.

For abelian varieties of higher dimension, there is a extensive general theory, which is, however, of little use when we have a particular curve of genus 2 (say) over $\mathbb{Q}$ and want to find its Jacobian, rank and torsion part. One finds that the general theory uses maps which are not defined over the same ground field as the coefficients of the original curve, and therefore are not useful for answering many arithmetic questions. A further legacy of the analytic approach is that nearly all the literature on curves of genus 2 restricts itself to the case $Y^2 =$ quintic, rather than the general form $Y^2 =$ sextic.

The advent of modern computer algebra packages makes it possible to embark on the project of making abelian varieties of dimension 2 as amenable to arithmetic investigation as elliptic curves. The main aim of this paper is to develop tools for such a project.

Section 1 presents an explicit model for the Jacobian variety. We lay the groundwork for Sections 2 and 3 by determining all quadratic relations on the Jacobian, given explicitly in Appendix A. Section 2 develops constructively the theory of formal groups for genus 2, including an explicit pair of local parameters which induce a formal group law defined over the same ring as the coefficients of the original curve. Heavy use is made of the computer algebra package 'Reduce', and some of the results are simply 'proof by algebraic checking' — although we provide a brief description of the methods used to obtain them. As a rule the identities, once formulated, are comparatively easy to verify; the labour required is in finding the correct formulation.

§1. The Jacobian Variety

We shall work with a general curve $\mathcal{C}$ of genus 2, over a ground field K of characteristic not equal to 2, 3 or 5, which may be taken to have hyperelliptic form

$$\mathcal{C} : Y^2 = F(X) = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0 \tag{1}$$

with f_0,. . .,f_6 in K, $f_6 \neq 0$, and $\Delta(F) \neq 0$, where $\Delta(F)$ is the discriminant of F. In $\mathbb{F}_5$ there is, for example, the curve $Y^2 = X^5 - X$ which is not birationally equivalent to the above form.

Most of the literature on genus 2 considers only the case when $F(X)$ is a quintic; we do not impose this restriction, and the theory presented will apply to the general case. This renders unavailable much of the analytic theory of the Jacobian, such as that in [10]. In particular, we may not assume the existence of a Weierstrass point defined over K.

As a group, the Jacobian of a curve of genus 2 has long been well understood in terms of divisor classes modulo linear equivalence (see [1]). The canonical equivalence class of divisors of the form $(x, y) + (x, -y)$, denoted by $\mathcal{O}$, gives the group identity. Any other element of the Jacobian is represented by an unordered pair of points $\{(x_1, y_1), (x_2, y_2)\}$ on $\mathcal{C}$, corresponding to the divisor $(x_1, y_1)+(x_2, y_2)-\mathcal{O}$, where we also allow $+\infty$ and $-\infty$ (the 2 branches of the singularity of $\mathcal{C}$ at infinity) to appear in the unordered pair. Generically, three such elements will sum to $\mathcal{O}$ if there is a function of the form $Y -$ (cubic in X) which meets $\mathcal{C}$ at all 6 component points. The Mordell–Weil group is the subgroup invariant under Galois action. It consists of pairs of points which are either both in K, or are conjugate over K and quadratic. We denote this subgroup by $\mathcal{D}(\mathcal{C})$.

We wish to express the Jacobian as a projective variety; that is to say, we seek an abelian variety of dimension 2 defined over K whose points represent elements of the group described above. Working on $\mathcal{C} \times \mathcal{C}$, we wish to 'blow down' $\mathcal{O}$ to a single point. Let Θ^+, Θ^- be the images of $\mathcal{C}$ in the Jacobian via the embeddings $P \mapsto P - (+\infty)$, $P \mapsto P - (-\infty)$, respectively. If we further let Θ be the image of $\mathcal{C}$ in the Jacobian via the embedding $P \mapsto P - \infty$ (where ∞ is some fixed Weierstrass point over $\overline{K}$), then $\Theta^+ + \Theta^-$ is equivalent over $\overline{K}$ to 2Θ. Now, Θ is ample, and the Riemann-Roch Theorem gives that $\ell(n\Theta) = n^2 \ \ (n \geq 1)$. A theorem of Lefschetz ([6], p.105) implies that a basis for $\mathcal{L}(3\Theta)$ gives a projective embedding of the Jacobian into $\mathbf{P}^8$. David Grant has independently developed this point of view in [4], which assumes a Weierstrass point over K and uses the quintic form for $F(X)$.

In our case, we wish only to use maps defined over K, and so no analogue of $\mathcal{L}(3\Theta)$ is available. We do, however, have an analogue of $\mathcal{L}(4\Theta)$ — namely $\mathcal{L}\big(2(\Theta^+ + \Theta^-)\big)$, which is defined over K. This is equivalent to the space of symmetric functions on $\mathcal{C} \times \mathcal{C}$ which have at most a double pole at infinity (that is to say, of degree at most 2 in each of X_1, X_2) , a pole of any order at $\mathcal{O}$, and are regular elsewhere. Such functions form a 16-dimensional vector space. A basis has been given in [2]; we find it convenient to adopt the following slightly different basis and notation (where $(x_1, y_1), (x_2, y_2) \in \mathcal{C}$).

Definition 1.1. Let the map $J : \mathcal{D}(\mathcal{C}) \to \mathbf{P}^{15}$ take $D = \{(x_1, y_1), (x_2, y_2)\} \in \mathcal{D}(\mathcal{C})$ to $\mathbf{a} = (a_0, \ldots a_{15})$, where $a_0, \ldots a_{15}$ is the following basis of $\mathcal{L}\big(2(\Theta^+ + \Theta^-)\big)$, given in reverse order.

Regular at $\mathcal{O}$:

$$a_{15} = 1,\ a_{14} = x_1 + x_2,\ a_{13} = x_1 x_2,\ a_{12} = {x_1}^2 + {x_2}^2,\ a_{11} = x_1 x_2 (x_1 + x_2),\ a_{10} = (x_1 x_2)^2.$$

Simple pole at $\mathcal{O}$:

$$a_9 = (y_1 - y_2)/(x_1 - x_2),\ a_8 = (x_2y_1 - x_1y_2)/(x_1 - x_2),$$
$$a_7 = (x_2^2y_1 - x_1^2y_2)/(x_1 - x_2),\ \ a_6 = (x_2^3y_1 - x_1^3y_2)/(x_1 - x_2).$$

Double pole at $\mathcal{O}$:

$$\begin{aligned} a_5 &= (F_0(x_1, x_2) - 2y_1y_2)/(x_1 - x_2)^2, \\ a_4 &= (F_1(x_1, x_2) - (x_1 + x_2)y_1y_2)/(x_1 - x_2)^2, \\ a_3 &= (x_1x_2)a_5, \end{aligned}$$

where

$$\begin{aligned} F_0(x_1, x_2) =& 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\ & + 2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1 + x_2) + 2f_6(x_1x_2)^3, \\ F_1(x_1, x_2) =& f_0(x_1 + x_2) + 2f_1(x_1x_2) + f_2(x_1x_2)(x_1 + x_2) + 2f_3(x_1x_2)^2 \\ & + f_4(x_1x_2)^2(x_1 + x_2) + 2f_5(x_1x_2)^3 + f_6(x_1x_2)^3(x_1 + x_2). \end{aligned}$$

Triple pole at $\mathcal{O}$:

$$\begin{aligned} a_2 &= (G_0(x_1, x_2)y_1 - G_0(x_2, x_1)y_2)/(x_1 - x_2)^3, \\ a_1 &= (G_1(x_1, x_2)y_1 - G_1(x_2, x_1)y_2)/(x_1 - x_2)^3, \end{aligned}$$

where

$$\begin{aligned} G_0(x_1, x_2) =& 4f_0 + f_1(x_1 + 3x_2) + f_2(2x_1x_2 + 2x_2^2) + f_3(3x_1x_2^2 + x_2^3) \\ & + 4f_4(x_1x_2^3) + f_5(x_1^2x_2^3 + 3x_1x_2^4) + f_6(2x_1^2x_2^4 + 2x_1x_2^5), \\ G_1(x_1, x_2) =& f_0(2x_1 + 2x_2) + f_1(3x_1x_2 + x_2^2) + 4f_2(x_1x_2^2) + f_3(x_1^2x_2^2 + 3x_1x_2^3) \\ & + f_4(2x_1^2x_2^3 + 2x_1x_2^4) + f_5(3x_1^2x_2^4 + x_1x_2^5) + 4f_6(x_1^2x_2^5). \end{aligned}$$

Quadruple pole at $\mathcal{O}$:

$$a_0 = a_5^2.$$

The embedding of the Jacobian in $\mathbf{P}^{15}$, given by the image of J, will be denoted $J(\mathcal{C})$. The canonical divisor class $\mathcal{O}$ is mapped by J to $(1, 0, \ldots, 0)$. We observe that 4 of these functions: $a_5, a_{13}, a_{14}, a_{15},$, give a basis for $\mathcal{L}\big(\Theta^+ + \Theta^-\big)$ (that is to to say, they have a pole of order only 1 at infinity); the restriction of the Jacobian to these 4 functions gives the Kummer surface in $\mathbf{P}^3$.

Having embedded the Jacobian into $\mathbf{P}^{15}$, we now wish to give it the structure of a variety by finding a set of defining equations. The space of quadratic forms on $J(\mathcal{C})$ is of dimension 72, and a basis of 72 such forms are given in Appendix A. The number 72 comes from 136 (the number of possible monomials of the form $a_i a_j$) minus 64 (the dimension of $\mathcal{L}\big(4(\Theta^+ + \Theta^-)\big)$). It is easy to verify that these quadratic forms define affine pieces which cover the $J(\mathcal{C})$. Indeed, the following can be verified.

Theorem 1.2. *The* 72 *quadratic forms given in Appendix A are a set of defining equations for the projective variety given by the embedding of Definition 1.1.* □

Of course, the proof of Theorem 1.2 (as with many of the results in this paper) is simply by 'algebraic verification', for checking that each identity in Appendix A does indeed hold between the functions of Definition 1.1, to show that all 72 forms given are linearly independent, and to check non-singularity at the origin. We note that Theorem 1.2. is a special case of a Theorem of Mumford, that Jacobian varieties may be defined by the intersection of quadrics (see [9]).

However, we shall try, at this stage, to give the reader a brief idea of the techniques used to *derive* such identities. We first introduce two weights on $X, Y,$ and f_i with respect to which $\mathcal{C}$ is homogeneous.

Definition 1.3. Let

$$wt_1(X) = 0,\ wt_1(Y) = 1,\ wt_1(f_i) = 2, \quad \text{for all } i,$$

$$wt_2(X) = 1,\ wt_2(Y) = 0,\ wt_2(f_i) = -i, \quad \text{for all } i.$$

Then $\mathcal{C}$ is homogeneous with respect to either weight. Each a_i is homogeneous with respect to the *induced weights*:

$$wt_1 : \begin{array}{cccccccccccccccc} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ 4 & 3 & 3 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$$wt_2 : \begin{array}{cccccccccccccccc} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ -4 & -2 & -3 & 0 & -1 & -2 & 2 & 1 & 0 & -1 & 4 & 3 & 2 & 2 & 1 & 0 \end{array}$$

The technique used to find the quadratic forms of Appendix A first searches for pairs of quadratic monomials: $a_i a_j$, $a_k a_l$ which have poles at $\mathcal{O}$ of the same order, but whose difference has a pole of lower order at $\mathcal{O}$ in the function field of $\mathcal{C}^{(2)} = (\mathcal{C} \times \mathcal{C})/\mathrm{Sym}$. The difference $a_i a_j - a_k a_l$ then gives the 'initial part' of a quadratic form. For example, a_4^2 and $a_0 a_{13}$ both have a pole of order 4 at $\mathcal{O}$, but $a_4^2 - a_0 a_{13}$ (the 'initial part' of equation (A.23)) has only a pole of order 2 at $\mathcal{O}$. If we anticipate §2, this corresponds to the fact that the local power series expansions of a_4^2 and $a_0 a_{13}$ at $\mathcal{O}$ have the same leading terms. Having found an initial part, one then successively reduces the remaining poles at $\mathcal{O}$ and at infinity, with terms of the form: $\lambda_{m,n} a_m a_n$ ($\lambda_{m,n} \in \mathbb{Z}[f_0, \ldots, f_6]$), until an identity in the function field of $\mathcal{C}^{(2)}$ is obtained.

The quadratic forms of Appendix A have also been chosen to be homogeneous with respect to wt_1 and wt_2. As well as giving forms with a more natural appearance, these homogeneity requirements proved to be a useful computational device, in that they placed severe restrictions on the possible monomials $\lambda_{m,n} a_m a_n$ which could occur in a given quadratic form.

§2. A Pair of Local Parameters

In this section, we find a pair of local parameters on the Jacobian. The approach is entirely constructive, and it allows the power series which give the expansion of a point near $\mathcal{O}$ to be written out explicitly over the ring of coefficients of $\mathcal{C}$.

We let R be a ring, complete with respect to a discrete non-Archimedean valuation, with maximal ideal $\mathcal{M}$. We shall assume that $f_0, \ldots, f_6 \in R$ (of course $\mathcal{C}$ can always be transformed to this form even if $f_0, \dots, f_6$ are originally only in the field of fractions of R) and, for $0 \leqslant i \leqslant 15$ we define $s_i = a_i/a_0$. We let $J(\mathcal{C})$ be as in Definition 1.1, and let $\mathcal{N}$ denote the following neighbourhood of the origin:

$$\mathcal{N} = \{\mathbf{a} \in J(\mathcal{C}) : |s_i| < 1, \forall\ 1 \leqslant i \leqslant 15\}. \tag{2}$$

For each $i = 3, \dots 15,$ consider $a_0 a_i$, a function on $\mathcal{C}^{(2)}$ with a pole of order at most 4 at infinity, and at most 6 at $\mathcal{O}$. Each $a_0 a_i$, for $i = 3, \dots, 15$, may be written as a quadratic form in $a_1, \dots a_{15}$ defined over R. These are given explicitly by equations (A.1),. . .,(A.13) in Appendix A. Dividing each of these through by a_0^2 gives equations of the form:

$$\begin{aligned} s_3 &= s_1^2 - f_0 s_5^2 + \dots \\ s_4 &= s_1 s_2 + f_0 f_3 s_5 s_{15} + \dots \\ &\vdots \\ s_{15} &= s_5^2, \end{aligned}$$

where each right hnd side lies in $R[s_1, \dots, s_{15}]$.

We define one 'iteration' to be the alteration of the above equations by the substitution of each equation into each right hand side. It is clear that after n iterations we have

$$s_i = \text{ polynomial in } R[s_1, s_2] + \text{ (terms in } R[s_1, \dots, s_{15}] \text{ of degree } > n).$$

Hence we may derive power series $\sigma_1, \dots, \sigma_{15} \in R[[s_1, s_2]]$ which converge to $s_1, \dots, s_{15}$ whenever $(a_0, \dots, a_{15}) \in \mathcal{N}$.

Reduce is ideal for generating as many terms as desired of each power series — one simply inputs the quadratic form substitutions repeatedly, until all terms up to the required degree involve only s_1 and s_2. The first few terms of each σ_i are given in Appendix B. The following result is now immediate.

Theorem 2.1. *The functions s_1, s_2 are a pair of local parameters for $J(\mathcal{C})$ at the origin.*

□

Note that we could also have deduced this result from the fact that the tangent plane at $\mathcal{O}$ is given by $a_3 = \dots = a_{15} = 0$. The advantage of the above is that it shows that the power series expansions are defined over R, and gives us a way of writing them out explicitly, which will prove useful in §3.

Corollary 2.2. *For $P = (a_0, \ldots, a_{15}) = (1, s_1, \ldots, s_{15}) \in \mathcal{N}$, the map $\phi : P \mapsto (s_1, s_2)$ gives a bijection between $\mathcal{N}$ and $\mathcal{M} \times \mathcal{M}$.*

Proof. The definition of $\mathcal{N}$, $P \in \mathcal{N} gives \implies s_1, s_2 \in \mathcal{M}$; so ϕ is into $\mathcal{M} \times \mathcal{M}$. Now, for any $(s_1, s_2) \in \mathcal{M} \times \mathcal{M}$, take $s_i = \sigma_i(s_1, s_2)$ (which converges in $\mathcal{M}$) for $3 \leqslant i \leqslant 15$. Then the point $(1, s_1, \ldots, s_{15}) \in \mathcal{N}$ maps to (s_1, s_2). Hence ϕ is onto. Finally for a given P, $P' \in \mathcal{N}$ with the same s_1 and s_2, the power series $\sigma_3, \ldots, \sigma_{15}$ uniquely determine $s_3, \ldots, s_{15}$, and so $P = P'$. □

We finally note, as an analogue of an elliptic curves result (see [12], p.111), that the local power series σ_i are homogeneous with respect to wt_1 and wt_2, since each of the equations used in the recursive substitutions are homogeneous.

§3. The Formal Group Associated with J(C)

The aim of this section is to show that the local parameters s_1, s_2 of §2 give a formal group law which is defined over R, the ring of $f_0, \ldots, f_6$ (the coefficients of $\mathcal{C}$). For this section we retain the requirement of §2, namely that R is a ring, complete with respect to a discrete non-Archimedean valuation, with maximal ideal $\mathcal{M}$ and field of fractions K. Let

$$\mathbf{a} = (a_0, \ldots, a_{15}) = (1, s_1 \ldots, s_{15}),$$

$$\mathbf{b} = (b_0, \ldots, b_{15}) = (1, t_1 \ldots, t_{15}),$$

$$\mathbf{c} = (c_0, \ldots, c_{15}) = (1, u_1, \ldots, u_{15}),$$

be such that $\mathbf{c} = \mathbf{a} + \mathbf{b}$. From §1, $s = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$, $t = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$ and $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$ are local parameters for $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$, respectively. We first note that, if we view $J(\mathcal{C})$ as an abelian variety over K, the field of fractions of R, then it is an analytic group (see [7]). We therefore have the following from the general theory of analytic groups.

Lemma 3.1. *There is a formal group law* $\mathcal{F} = \begin{pmatrix} \mathcal{F}_1 \\ \mathcal{F}_2 \end{pmatrix}$ *defined over* K *such that* $u = \mathcal{F}(s,t)$ *in some neighbourhood* $\mathcal{N}_{\mathcal{F}}$ *of* $\mathcal{O}$.

For the proof of Lemma 3.1 it is necessary to sift through Chapter 4 of [11] (or some equivalent), which shows that every analytic group is locally just a formal group over K. The result we need is on p. 4.22 of [11], that any analytic group chunk contains an open subgroup which is standard (that is to say, has a group law determined on an open subgroup by a formal power series over K).

It now remains to show that the $\mathcal{F}$ of Lemma 3.1 is defined over R (and so to deduce that $\mathcal{N}_{\mathcal{F}}$ is the same as the $\mathcal{N}$ given by equation (2)). Our strategy will be to express $\mathcal{F}_1$ and $\mathcal{F}_2$ as quotients of power series over R, and then to apply a version of Gauss' Lemma. The size of the intermediary expressions will be kept to a minimum by use of the following definitions.

Definition 3.2. A homogeneous polynomial in several variables defined over R is *weightless* if at least one of its coefficients is a unit in R. A power series in several variables over R is *weightless* if its polynomial of smallest degree is weightless. A quotient of power series is *n-weightless* (respectively *d-weightless*) if it may be written in the form N/D, where N, and D are power series over R, with N (respectively D) weightless. Such a quotient is *weightless* if it is both n-weightless and d-weightless. For any power series ϕ, we let $v(\phi)$ denote the degree of the lowest degree polynomial of ϕ. We extend this to quotients of power series by setting $v(\phi/\theta) = v(\phi) - v(\theta)$. Let $\approx$ denote the following equivalence relation on quotients of power series: $\psi_1 \approx \psi_2$ if and only if $v(\psi_1 - \psi_2) < v(\psi_1) = v(\psi_2)$ and $\psi_1 - \psi_2$ is d-weightless. This extends the 'has the same polynomial of lowest degree as' equivalence relation on power series.

In our case, we shall be working exclusively with power series in $R[[s,t]]$, and quotients of power series in $R((s,t))$, the field of fractions of $R[[s,t]]$. The following properties are immediate.

Lemma 3.3. *The properties weightless, n-weightless and d-weightless are all unaffected by multiplication or division by anything weightless; d-weightless times d-weightless is again d-weightless (and similarly for n-weightless). Furthermore,*

$$(\phi_1 \approx \phi_2 \text{ and } \psi_1 \approx \psi_2) \Rightarrow \phi_1\psi_1 \approx \phi_2\psi_2$$

and

$$(\phi_1\psi \approx \phi_2\psi \text{ and } \psi \text{ weightless}) \Rightarrow \phi_1 \approx \phi_2.$$

We shall also make use of the following generalisation of Gauss' Lemma (see [5], p.55).

Lemma 3.4. *Let $\phi = \psi\theta$, where ϕ, ψ and θ are power series in several variables defined over K. If θ and ϕ are defined over R, and θ is weightless (so that $\psi = \phi/\theta$ is d-weightless), then ψ is defined over R.*

We now proceed to express $\mathcal{F}_1$, $\mathcal{F}_2$ as members of $R((s,t))$ (that is, as quotients of power series over R in s_1, s_2, t_1, t_2), using Lemma 3.3 to simplify the intermediate expressions. We assume that $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{N}$, corresponding to the divisors $\{(x_1,y_1),(x_2,y_2)\}$, $\{(x_3,y_3),(x_4,y_4)\}$, $\{(x_5,y_5),(x_6,y_6)\}$, respectively. It is easy to verify algebraically that the function $\mu Y - (\alpha X^3 + \beta X^2 + \gamma X + \delta)$ meets $\mathcal{C}$ at the points (x_1,y_1), (x_2,y_2), (x_3,y_3), (x_4,y_4) where

$$\begin{aligned}
\mu &= a_{10}b_{15} + b_{10}a_{15} - a_{14}b_{11} - b_{14}a_{11} + a_{13}(b_{12}+b_{13}) + b_{13}(a_{12}+a_{13})\\
\alpha &= a_7b_{15} + b_7a_{15} + a_{13}b_9 + b_{13}a_9 - a_{14}b_8 - b_{14}a_8\\
\beta &= -a_6b_{15} - b_6a_{15} + a_8(b_{12}+b_{13}) + b_8(a_{12}+a_{13}) - a_{11}b_9 - b_{11}a_9\\
\gamma &= a_6b_{14} + b_6a_{14} - a_7(b_{12}+b_{13}) - b_7(a_{12}+a_{13}) + a_9b_{10} + b_9a_{10}\\
\delta &= -a_6b_{13} - b_6a_{13} + a_7b_{11} + b_7a_{11} - a_8b_{10} - b_8a_{10}.
\end{aligned}$$

We now divide each of these equations by a_0b_0 (which has the effect of replacing each a_i, b_i by s_i, t_i, respectively) to obtain the localisations:

$$\begin{aligned}
\mu_\ell &:= \mu/(a_0b_0) = s_{10}t_{15} + \ldots + t_{13}(s_{12}+s_{13}) \in R[[s,t]],\\
\alpha_\ell &:= \alpha/(a_0b_0) = s_7t_{15} + \ldots - t_{14}s_8 \in R[[s,t]],
\end{aligned} \tag{3}$$

and similarly for $\beta_\ell, \gamma_\ell, \delta_\ell \in R[[s,t]]$. Then $(\mu_\ell, \alpha_\ell, \beta_\ell, \gamma_\ell, \delta_\ell) = (\mu, \alpha, \beta, \gamma, \delta)$, and so the function $\mu_\ell Y - (\alpha_\ell X^3 + \beta_\ell X^2 + \gamma_\ell X + \delta_\ell)$ also meets $\mathcal{C}$ at the points (x_i, y_i), $i = 1, \ldots, 4$. Furthermore, the quadratic forms of Appendix A allow us to write out the power series for each $s_i \in R[[s]]$, $t_i \in R[[t]]$, which we may use to express $\mu_\ell, \alpha_\ell, \beta_\ell, \gamma_\ell, \delta_\ell$ as members of $R[[s,t]]$. For our present purposes we require only the polynomial of lowest degree for each power series:

$$\begin{aligned}
&s_0 \approx 1,\ s_1 \approx s_1,\ s_2 \approx s_2,\ s_3 \approx s_1^2,\\
&s_4 \approx s_1 s_2,\ s_5 \approx s_2^2,\ s_6 \approx s_1^3,\\
&s_7 \approx s_1^2 s_2,\ s_8 \approx s_1 s_2^2,\ s_9 \approx s_2^3,\\
&s_{10} \approx s_1^4,\ s_{11} \approx 2 s_1^3 s_2,\ s_{12} \approx 2 s_1^2 s_2^2,\\
&s_{13} \approx s_1^2 s_2^2,\ s_{14} \approx 2 s_1 s_2^3,\ s_{15} \approx s_2^4,
\end{aligned} \tag{4}$$

and similarly for each s_i replaced by t_i. We now substitute $Y = (\alpha_\ell X^3 + \beta_\ell X^2 + \gamma_\ell X + \delta_\ell)/\mu_\ell$ into $\mathcal{C} : Y^2 = F(X)$ to give a sextic in X, four of whose roots are x_1, x_2, x_3, x_4. From the discussion at the beginning of §1 (following [1]) we see that the remaining two roots are x_5, x_6 from which we may express (c_{13}, c_{14}, c_{15}) projectively by

$$\begin{aligned}
&s_{15}^2 t_{15}^2 (\delta_\ell^2 - f_0 \mu_\ell^2),\\
&s_{13} t_{13} \big(s_{15} t_{15} (f_5 \mu_\ell^2 - 2\alpha_\ell \beta_\ell) - (s_{15} t_{14} + s_{14} t_{15})(\alpha_\ell^2 - f_6 \mu_\ell^2) \big),\\
&s_{13} t_{13} s_{15} t_{15} (\alpha_\ell - f_6 \mu_\ell^2),
\end{aligned} \tag{5}$$

respectively. On subtituting (3) and then (4) into (5), we may regard these as members of $R[[s,t]]$ with respective initial terms:

$$\begin{aligned}
&s_1^2 t_1^2 s_2^8 t_2^8 (s_2 t_1 - s_1 t_2)^4 (s_1 + t_1)^2,\\
&2 s_1^2 t_1^2 s_2^8 t_2^8 (s_2 t_1 - s_1 t_2)^4 (s_1 + t_1)(s_2 + t_2),\\
&s_1^2 t_1^2 s_2^8 t_2^8 (s_2 t_1 - s_1 t_2)^4 (s_2 + t_2)^2.
\end{aligned}$$

Hence, on multiplying each of these by the weightless $(s_2 + t_2)^2 / s_1^2 t_1^2 s_2^8 t_2^8 (s_2 t_1 - s_1 t_2)^4$, we obtain (c_{13}, c_{14}, c_{15}) projectively as members of $R((s,t))$ with simple initial terms:

$$\begin{aligned} c_{13} &\approx (s_1+t_1)^2(s_2+t_2)^2, \\ c_{14} &\approx 2(s_1+t_1)(s_2+t_2)^3, \\ c_{15} &\approx (s_2+t_2)^4. \end{aligned} \tag{6}$$

Note that, up to the relation $\approx$, our c_{13}, c_{14}, c_{15} are the same as s_{13}, s_{14}, s_{15} in (4), but with each occurrence of parameters s_1, s_2 replaced by $(s_1+t_1), (s_2+t_2)$ respectively. It may be verified algebraically that the same is true of the $c_0, \ldots, c_{12} \in R((s,t))$ which projectively extend the c_{13}, c_{14}, c_{15} of (6) to give $\mathbf{c}$. This verification may be done by hand, if one makes use of the defining equations of Appendix A (with each a_i replaced by c_i) and uses Lemma 3.3 to simplify intermediary expressions; the details are not given here. Note that, since we require only initial terms, we may ignore all terms involving the f_i's in each quadratic form (in view of wt_1 defined in 1.3). In particular, we have the following initial approximations for $c_0, c_1, c_2 \in R((s,t))$:

$$c_0 \approx s_2+t_2,\ c_1 \approx s_1+t_1,\ c_2 \approx 1. \tag{7}$$

We are now in a position to prove:

Theorem 3.5. *The formal group law $\mathcal{F}$ of Lemma 3.1 is defined over R, and so converges for all $\mathbf{a}$, $\mathbf{b} \in \mathcal{N}$.*

Proof. Since $\mathcal{F}_1 = u_1 = c_1/c_0$, $\mathcal{F}_2 = u_2 = c_2/c_0$, it follows from (7) that $\mathcal{F}_1$, $\mathcal{F}_2$ are d-weightless in $R((s,t))$. Since, by Lemma 3.1, $\mathcal{F}_1$ and $\mathcal{F}_2$ are power series over K, we may appeal to Lemma 3.4 to deduce that $\mathcal{F}_1, \mathcal{F}_2 \in R[[s,t]]$, as required. □

The benefit of using the relation $\approx$ to assist the proof of Theorem 3.5 may be seen by attempting to express u_1 and u_2 as members of $R((s,t))$ without any intermediary simplifications. Using this rather crude approach (which was our original proof of Theorem 3.5), it is necessary to check the weightlessness of a polynomial of degree 76.

The above method provides a way of writing out the terms of the formal group up to any required degree. We observe that our proof gives the initial (linear) term of $\mathcal{F}$, namely $s+t$, as we would hope. In general, if we know that $\psi = \phi/\theta$ and wish to know the lowest n degree polynomials of ψ, we may derive them from the lowest n degree polynomials of ϕ and θ. So, in theory, we may repeat the intermediary stages given above, but working mod lowest n degrees (rather than mod lowest degree) to obtain the first n degree terms of $\mathcal{F}$. Up to cubic terms in s, t, the formal group is:

$$\mathcal{F}_1(s,t) = s_1 + t_1 + 2f_4 s_1^2 t_1 + 2f_4 s_1 t_1^2 - f_1 s_2^2 t_2 - f_1 s_2 t_2^2 + \ldots$$

$$\mathcal{F}_2(s,t) = s_2 + t_2 + 2f_2 s_2^2 t_2 + 2f_2 s_2 t_2^2 - f_5 s_1^2 t_1 - f_5 s_1 t_1^2 + \ldots$$

However we observe that, for elliptic curves, it is possible to infer the existence of the induced formal group without requiring an appeal to the theory of analytic groups to guarantee the existence of a power series over K. In this respect, the above development is somewhat unsatisfactory; it seems to the author that it should be possible to imitate the elliptic curves development. For this purpose, it would be sufficient to express the global group law in the form: $\mathbf{a} + \mathbf{b} = (\nu_0(\mathbf{a},\mathbf{b}), \ldots, \nu_{15}(\mathbf{a},\mathbf{b}))$, where each $\nu_i(\mathbf{a},\mathbf{b})$ is a biquadratic form over R in $\mathbf{a}, \mathbf{b}$, and $\nu_0(\mathbf{a},\mathbf{b})$ contains the term $a_0^2 b_0^2$. The localisation of $\nu_0(\mathbf{a},\mathbf{b})$ would then have a local power series expansion over R containing 1, would be invertible, and would therefore (without appeal to Lemma 3.1) divide the localisations of $\nu_1(\mathbf{a},\mathbf{b})$ and $\nu_2(\mathbf{a},\mathbf{b})$. Progress towards an explicit expression of this type for the global group law is described in Chapter 3 of [3]. An alternative proof of Theorem 3.5 along these lines, as well as being more direct, would be likely to provide a more efficient method of computing terms of the formal group.

Appendix A. A Set of Defining Equations for the Jacobian

The following 72 quadratic forms are a set of defining equations for the Jacobian variety, given by the embedding of Definition 1.1.

$$a_0a_3 = a_1a_1 - a_5^2f_0 - a_3^2f_4 + 4a_4a_{13}f_0f_5 + a_5a_{10}f_1f_5 + 8a_4a_{10}f_1f_6 + a_3a_{10}(4f_2f_6 - f_3f_5) + 8a_4a_{11}f_0f_6 + 2a_{13}a_{15}f_0f_1f_5 + a_{10}a_{15}(4f_0f_2f_6 + 2f_0f_3f_5 + 3f_1^2f_6) + 4a_{11}a_{15}f_0f_1f_6 + 2a_{10}a_{13}(f_0f_5^2 + 3f_1f_3f_6) + 8a_{11}a_{13}f_0f_3f_6 + a_{10}^2(4f_1f_5f_6 + 4f_2f_4f_6 - f_2f_5^2 - f_3^2f_6) + a_{10}a_{11}(4f_0f_5f_6 + 4f_1f_4f_6 - f_1f_5^2) + a_{11}^2f_0(4f_4f_6 - f_5^2) \tag{A.1}$$

$$a_0a_4 = a_1a_2 + a_5a_{15}f_0f_3 + a_3a_{15}(9f_0f_5 + f_1f_4) + 2a_5a_{14}f_0f_4 + a_4a_{13}(20f_0f_6 + 3f_1f_5) + a_5a_{10}(7f_1f_6 + f_2f_5) + 4a_4a_{10}f_2f_6 + a_3a_{10}f_3f_6 + 4a_7a_9f_0f_5 + 4a_6a_9f_0f_6 - 4a_8^2f_0f_5 - 4a_7a_8f_0f_6 + 4a_6a_8f_1f_6 - 2a_7^2f_1f_6 + 4a_{15}^2f_0^2f_5 + 2a_{14}a_{15}f_0(2f_0f_6 + f_1f_5) + a_{13}a_{15}(14f_0f_1f_6 + 6f_0f_2f_5 + f_1^2f_5) + a_{13}a_{14}(8f_0f_2f_6 + 3f_0f_3f_5 - f_1^2f_6) + a_{10}a_{14}(8f_0f_4f_6 + f_0f_5^2 + 3f_1f_3f_6) + 2a_{13}^2(10f_0f_3f_6 + 2f_0f_4f_5 + 2f_1f_2f_6 + f_1f_3f_5) + a_{10}a_{13}(18f_0f_5f_6 + 6f_1f_4f_6 + f_1f_5^2 + 2f_2f_3f_6) + 4a_{12}a_{13}f_0f_3f_6 + 2a_{10}^2f_6(f_1f_6 + f_2f_5) + 2a_{10}a_{11}f_6(2f_0f_6 + f_1f_5) + 2a_{10}a_{12}f_0f_5f_6 \tag{A.2}$$

$$a_0a_5 = a_2a_2 - a_5^2f_2 - a_3^2f_6 + a_5a_{15}(4f_0f_4 - f_1f_3) + a_3a_{15}f_1f_5 + 4a_5a_{14}f_0f_5 + 8a_4a_{14}f_0f_6 - 2a_3a_{14}f_1f_6 + 4a_4a_{12}f_1f_6 - 4a_6a_9f_1f_6 + 4a_7a_8f_1f_6 + a_{15}^2(4f_0f_2f_4 - f_0f_3^2 - f_1^2f_4) + a_{14}a_{15}f_5(4f_0f_2 - f_1^2) + 2a_{13}a_{15}(4f_0f_2f_6 + f_0f_3f_5 - 3f_1^2f_6) + a_{10}a_{15}(4f_0f_4f_6 - f_0f_5^2 - 4f_1f_3f_6) + 4a_{11}a_{15}f_6(2f_0f_3 - f_1f_2) + a_{12}a_{15}f_6(4f_0f_2 - f_1^2) + 4a_{10}a_{14}f_6(f_0f_5 - f_1f_4) - 4a_{10}a_{13}f_1f_5f_6 - 4a_{10}a_{11}f_1f_6^2 \tag{A.3}$$

$$a_0a_6 = a_1a_3 - a_2a_{10}f_3 - a_3a_9f_1 + 4a_5a_8f_0 + 4a_4a_8f_1 + 2a_3a_8f_2 + 2a_3a_7f_3 + a_8a_{15}(4f_0f_2 + f_1^2) + 4a_7a_{15}f_0f_3 + 4a_6a_{15}f_0f_4 + 2a_8a_{13}(2f_0f_4 + f_1f_3) + 2a_7a_{13}(2f_0f_5 + f_1f_4) + 2a_6a_{13}(2f_0f_6 + f_1f_5) - 2a_9a_{10}f_0f_5 + 3a_8a_{10}f_1f_5 + 2a_6a_{11}f_1f_6 + 4a_7a_{12}f_0f_5 + 4a_6a_{12}f_0f_6 \tag{A.4}$$

$$a_0a_7 = a_1a_4 + a_1a_{15}f_1 + a_5a_9f_0 - a_4a_6f_4 + a_7a_{14}(f_0f_5 - f_1f_4) - a_6a_{14}f_2f_4 + a_9a_{13}f_0f_4 + 2a_8a_{13}(-f_0f_5 + f_1f_4) + 2a_7a_{13}f_2f_4 + a_6a_{13}f_1f_6 - a_9a_{10}f_1f_5 + a_8a_{10}(-f_2f_5 + f_3f_4) + a_7a_{10}(-f_3f_5 + f_4^2) - a_6a_{10}f_3f_6 + a_9a_{12}f_0f_4 + a_8a_{12}(-f_0f_5 + f_1f_4) + a_7a_{12}f_2f_4 \tag{A.5}$$

$$a_0a_8 = a_1a_5 + a_3a_7f_5 + 2a_3a_6f_6 \tag{A.6}$$

$$a_0a_9 = a_2a_5 + a_4a_9f_3 + 3a_3a_8f_5 + 2a_5a_7f_4 + 4a_3a_7f_6 - a_8a_{15}f_2f_3 + a_7a_{15}(2f_1f_5 - f_3^2) + a_6a_{15}(2f_1f_6 - f_3f_4) + 4a_9a_{14}f_0f_5 - a_6a_{14}f_3f_5 - 4a_9a_{13}(-f_0f_6 - f_1f_5) + a_8a_{13}(4f_2f_5 - f_3f_4) + 2a_7a_{13}(2f_2f_6 + f_3f_5) + a_6a_{13}f_3f_6 + 4a_9a_{10}f_2f_6 + 4a_8a_{10}f_3f_6 + 2a_7a_{10}(2f_4f_6 - f_5^2) - 2a_6a_{10}f_5f_6 + 4a_9a_{11}f_1f_6 + 4a_9a_{12}f_0f_6 - a_6a_{12}f_3f_6 \tag{A.7}$$

$$a_0a_{10} = a_3a_3 \tag{A.8}$$

$$a_0a_{11} = 2a_3a_4 + a_3a_{15}f_1 + a_5a_{10}f_3 + a_3a_{10}f_5 \tag{A.9}$$

$$a_0a_{12} = 2a_2a_7 + 2a_3a_{15}f_2 + a_5a_{14}f_1 + 2a_3a_{10}f_6 + 2a_4a_{12}f_3 - 2a_6a_9f_3 + 2a_7a_8f_3 + 4a_7^2f_4 + 4a_6a_7f_5 - a_{13}a_{15}f_1f_3 + a_{10}a_{15}(8f_0f_6 + f_1f_5 - 3f_3^2) + 2a_{11}a_{15}(f_0f_5 - f_2f_3) - 2a_{10}a_{13}f_3f_5 + 2a_{11}a_{13}(3f_1f_6 - f_3f_4) + 12a_{12}a_{13}f_0f_6 + a_{10}^2f_5^2 + 2a_{10}a_{11}f_3f_6 + 4a_{11}^2f_2f_6 + 4a_{11}a_{12}f_1f_6 + 4a_{12}^2f_0f_6 \tag{A.10}$$

$$a_0a_{13} = a_3a_5 \tag{A.11}$$

$$a_0a_{14} = 2a_4a_5 + a_5a_{15}f_1 + a_3a_{15}f_3 + a_5a_{10}f_5 \tag{A.12}$$

$$a_0a_{15} = a_5a_5 \tag{A.13}$$

$$a_2a_3 = a_0a_7 - 2a_5a_9f_0 - a_5a_8f_1 \tag{A.14}$$

$$a_2a_4 = a_0a_8 - a_2a_{10}f_5 + a_4a_9f_2 - a_3a_6f_6 + a_9a_{15}f_0f_3 + a_8a_{15}(f_1f_3 - f_2^2) + a_7a_{15}(f_1f_4 - f_2f_3) + a_6a_{15}f_1f_5 - a_9a_{13}f_0f_5 - 2a_8a_{13}f_2f_4 + 2a_7a_{13}(f_1f_6 - f_2f_5) - a_6a_{13}f_2f_6 + a_9a_{11}f_2f_4 + a_8a_{11}(-f_1f_6 + f_2f_5) - a_8a_{12}f_2f_4 + a_7a_{12}(f_1f_6 - f_2f_5) - a_6a_{12}f_2f_6 \tag{A.15}$$

$$a_2a_9 = a_0a_{15} + a_5a_{15}f_2 + a_4a_{15}f_3 + 2a_3a_{15}f_4 + 3a_4a_{13}f_5 + 3a_3a_{13}f_6 + a_3a_{12}f_6 + a_{15}^2f_1f_3 + a_{14}a_{15}f_1f_4 + a_{13}a_{15}(3f_1f_5 + 2f_2f_4) + 3a_{10}a_{15}f_3f_5 + a_{12}a_{15}f_1f_5 + a_{13}a_{14}(f_1f_6 + 2f_2f_5) + 2a_{11}a_{14}f_2f_6 + a_{12}a_{14}f_1f_6 + a_{10}a_{13}(2f_4f_6 + f_5^2) + 2a_{11}a_{13}f_3f_6 \tag{A.16}$$

$$2a_2a_8 = a_0a_{14} - a_5a_{15}f_1 - a_5a_{13}f_3 + a_5a_{10}f_5 + 2a_3a_{11}f_6 - 2a_{15}^2f_0f_3 - 4a_{14}a_{15}f_0f_4 + 2a_{13}a_{15}(-3f_0f_5 - f_1f_4) - 4a_{11}a_{15}f_0f_6 - 4a_{12}a_{15}f_0f_5 - 2a_{13}a_{14}f_1f_5 - 4a_{12}a_{14}f_0f_6 - 4a_{13}^2f_1f_6 - 2a_{12}a_{13}f_1f_6 \tag{A.17}$$

(A.18) $2a_2a_6 = a_0a_{11}+4a_5a_{14}f_0+3a_5a_{13}f_1+a_5a_{10}f_3-a_3a_{10}f_5+2a_5a_{11}f_2+a_5a_{12}f_1+a_{14}a_{15}(4f_0f_2-f_1^2)+6a_{13}a_{15}f_0f_3+a_{11}a_{15}(4f_0f_4+f_1f_3)+2a_{12}a_{15}f_0f_3+a_{10}a_{14}f_1f_5+2a_{13}^2(f_0f_5+f_1f_4)+2a_{12}a_{13}f_0f_5$

(A.19) $a_1a_6 = a_0a_{10}+3a_5a_{13}f_0+3a_4a_{13}f_1+2a_5a_{10}f_2+a_4a_{10}f_3+a_3a_{10}f_4+a_5a_{12}f_0+a_{13}a_{15}(2f_0f_2+f_1^2)+3a_{10}a_{15}f_1f_3+2a_{13}a_{14}f_0f_3+2a_{11}a_{14}f_0f_4+a_{10}a_{13}(3f_1f_5+2f_2f_4)+a_{11}a_{13}(f_0f_5+2f_1f_4)+a_{10}^2f_3f_5+a_{10}a_{11}f_2f_5+a_{10}a_{12}f_1f_5+a_{11}a_{12}f_0f_5$

(A.20) $2a_1a_7 = a_0a_{11}+a_3a_{15}f_1+2a_5a_{14}f_0-a_3a_{13}f_3-a_3a_{10}f_5-4a_{10}a_{14}f_0f_6-4a_{13}^2f_0f_5+2a_{10}a_{13}(-3f_1f_6-f_2f_5)-2a_{11}a_{13}f_1f_5-2a_{12}a_{13}f_0f_5-2a_{10}^2f_3f_6-4a_{10}a_{11}f_2f_6-4a_{10}a_{12}f_1f_6-4a_{11}a_{12}f_0f_6$

(A.21) $2a_1a_8 = a_0a_{12}-2a_5a_{15}f_0-2a_5a_{10}f_4-a_3a_{11}f_5-2a_4a_{12}f_3-4a_8a_9f_1+2a_6a_9f_3-4a_8^2f_2-2a_7a_8f_3-a_{15}^2f_1^2-2a_{14}a_{15}f_0f_3+2a_{13}a_{15}f_1f_3+a_{10}a_{15}(-8f_0f_6-f_1f_5+3f_3^2)-4a_{14}^2f_0f_4+2a_{13}a_{14}(-3f_0f_5+f_2f_3)+2a_{10}a_{14}(-f_1f_6+f_3f_4)-4a_{12}a_{14}f_0f_5+a_{10}a_{13}f_3f_5-12a_{12}a_{13}f_0f_6-4a_{12}^2f_0f_6$

(A.22) $2a_1a_9 = a_0a_{14}-a_5a_{15}f_1+a_3a_{15}f_3+2a_3a_{14}f_4+3a_3a_{13}f_5+4a_3a_{11}f_6+a_3a_{12}f_5+a_{11}a_{15}f_1f_5+a_{10}a_{14}(4f_2f_6+f_3f_5)+2a_{13}^2(f_1f_6+f_2f_5)+6a_{10}a_{13}f_3f_6+2a_{12}a_{13}f_1f_6+a_{10}a_{11}(4f_4f_6-f_5^2)+2a_{10}a_{12}f_3f_6$

(A.23) $a_4a_4 = a_0a_{13}+a_5a_{13}f_2+a_5a_{10}f_4+a_3a_{10}f_6+a_9^2f_0+a_{13}a_{15}f_1f_3+a_{10}a_{15}f_2f_4+a_{11}a_{15}f_1f_4+a_{10}a_{14}(f_1f_6+f_2f_5)+a_{11}a_{14}f_1f_5+a_{10}a_{13}(2f_2f_6+f_3f_5)+a_{10}^2f_4f_6+a_{10}a_{11}f_3f_6+a_{10}a_{12}f_2f_6+a_{11}a_{12}f_1f_6$

(A.24) $a_0a_{12} = 2a_0a_{13}+4a_5a_{15}f_0+2a_5a_{14}f_1+4a_5a_{13}f_2+4a_5a_{10}f_4+4a_4a_{10}f_5+4a_3a_{10}f_6+2a_5a_{11}f_3+a_{15}^2(4f_0f_2-f_1^2)+4a_{14}a_{15}f_0f_3+2a_{13}a_{15}(4f_0f_4+f_1f_3)+a_{10}a_{15}(4f_2f_4-f_3^2)+4a_{11}a_{15}f_1f_4+4a_{12}a_{15}f_0f_4+4a_{13}a_{14}f_0f_5+4a_{10}a_{14}(f_1f_6+f_2f_5)+4a_{12}a_{14}f_0f_5+4a_{13}^2(f_0f_6+2f_1f_5)+4a_{10}a_{13}(2f_2f_6+f_3f_5)+4a_{12}a_{13}(2f_0f_6+f_1f_5)+a_{10}^2(4f_4f_6+f_5^2)+4a_{10}a_{11}f_3f_6+4a_{10}a_{12}f_2f_6+4a_{11}a_{12}f_1f_6+4a_{12}^2f_0f_6$

(A.25) $a_2a_{15} = a_5a_9-a_8a_{15}f_3-2a_7a_{15}f_4-2a_6a_{15}f_5-2a_6a_{14}f_6-a_8a_{13}f_5$

(A.26) $a_2a_{14} = 2a_5a_8 + a_9a_{15}f_1 + 2a_8a_{15}f_2 + a_7a_{15}f_3 - a_7a_{13}f_5 - 2a_6a_{13}f_6$

(A.27) $a_2a_{13} = a_5a_7 - 2a_9a_{15}f_0 - a_8a_{15}f_1$

(A.28) $a_2a_{10} = a_3a_7 - 2a_9a_{13}f_0 - a_8a_{13}f_1$

(A.29) $a_2a_{11} = 2a_3a_8 + a_9a_{13}f_1 + 2a_8a_{13}f_2 + a_7a_{13}f_3 - a_7a_{10}f_5 - 2a_6a_{10}f_6$

(A.30) $a_2a_{12} = 2a_5a_7 + 2a_7a_{15}f_2 + a_6a_{15}f_3 + a_9a_{14}f_1 + 2a_9a_{13}f_2 + 3a_8a_{13}f_3 + 4a_7a_{13}f_4 + 3a_6a_{13}f_5 + a_8a_{10}f_5 + 2a_6a_{11}f_6$

(A.31) $a_1a_{10} = a_3a_6 - a_7a_{13}f_1 - 2a_9a_{10}f_1 - 2a_8a_{10}f_2 - a_7a_{10}f_3 - 2a_9a_{11}f_0$

(A.32) $a_1a_{11} = 2a_3a_7 - 2a_9a_{13}f_0 - a_8a_{13}f_1 + a_8a_{10}f_3 + 2a_7a_{10}f_4 + a_6a_{10}f_5$

(A.33) $a_1a_{13} = a_3a_8 - a_7a_{10}f_5 - 2a_6a_{10}f_6$

(A.34) $a_1a_{15} = a_5a_8 - a_7a_{13}f_5 - 2a_6a_{13}f_6$

(A.35) $a_1a_{14} = 2a_5a_7 - 2a_9a_{15}f_0 - a_8a_{15}f_1 + a_8a_{13}f_3 + 2a_7a_{13}f_4 + a_6a_{13}f_5$

(A.36) $a_1a_{12} = 2a_3a_8 + a_7a_{15}f_1 + 2a_9a_{14}f_0 + 3a_9a_{13}f_1 + 4a_8a_{13}f_2 + 3a_7a_{13}f_3 + 2a_6a_{13}f_4 + a_9a_{10}f_3 + 2a_8a_{10}f_4 + a_6a_{11}f_5$

(A.37) $a_5a_8 = a_4a_9 - a_8a_{15}f_2 - a_7a_{15}f_3 - a_6a_{15}f_4 - a_6a_{14}f_5 - a_8a_{13}f_4 - a_6a_{13}f_6 - a_6a_{12}f_6$

(A.38) $a_5a_7 = a_4a_8 + a_9a_{15}f_0 + a_8a_{15}f_1 - a_7a_{13}f_4 - a_6a_{13}f_5 - a_6a_{11}f_6$

(A.39) $a_5a_6 = a_4a_7 + a_7a_{15}f_1 + a_9a_{14}f_0 + a_9a_{13}f_1 + a_8a_{13}f_2 + a_7a_{13}f_3 - a_6a_{10}f_6$

(A.40) $a_3a_7 = a_4a_6 - a_9a_{13}f_0 - a_7a_{13}f_2 - a_9a_{10}f_2 - a_8a_{10}f_3 - a_7a_{10}f_4 - a_9a_{11}f_1 - a_9a_{12}f_0$

(A.41) $a_3a_8 = a_4a_7 - a_9a_{14}f_0 - a_9a_{13}f_1 - a_8a_{13}f_2 + a_7a_{10}f_5 + a_6a_{10}f_6$

(A.42) $a_3a_9 = a_4a_8 - a_9a_{15}f_0 + a_8a_{13}f_3 + a_7a_{13}f_4 + a_6a_{13}f_5 + a_8a_{10}f_5 + a_6a_{11}f_6$

(A.43) $a_5a_{15} = a_9^2 - a_{15}^2f_2 - a_{14}a_{15}f_3 - a_{10}a_{15}f_6 - a_{14}^2f_4 - a_{13}a_{14}f_5 - a_{12}a_{14}f_5 - 2a_{12}a_{13}f_6 - a_{12}^2f_6$

(A.44) $a_5a_{14} = 2a_8a_9 + a_{15}^2f_1 - a_{13}a_{15}f_3 - 2a_{13}a_{14}f_4 - 2a_{10}a_{14}f_6 - 3a_{13}^2f_5 - 2a_{12}a_{13}f_5 - 2a_{11}a_{12}f_6$

(A.45) $a_5a_{13} = a_8^2 - a_{15}^2f_0 - a_{13}^2f_4 - 2a_{10}a_{13}f_6 - a_{11}a_{13}f_5 - a_{10}a_{12}f_6$

(A.46) $a_5a_{10} = a_7^2 - 2a_{13}a_{15}f_0 - a_{10}a_{15}f_2 - a_{11}a_{15}f_1 - a_{12}a_{15}f_0 - a_{10}^2f_6$

(A.47) $a_5a_{11} = 2a_7a_8 - 2a_{14}a_{15}f_0 - a_{13}a_{15}f_1 + a_{10}a_{15}f_3 - a_{10}a_{13}f_5 - 2a_{10}a_{11}f_6$

(A.48) $a_5a_{12} = 2a_7a_9 + a_{14}a_{15}f_1 + 2a_{13}a_{15}f_2 + a_{11}a_{15}f_3 - a_{10}a_{14}f_5 - 2a_{10}a_{13}f_6 - 2a_{10}a_{12}f_6$

(A.49) $a_4a_{15} = a_8a_9 - a_{13}a_{15}f_3 - a_{11}a_{15}f_4 - a_{10}a_{14}f_6 - 2a_{13}^2f_5 - a_{12}a_{13}f_5 - a_{11}a_{12}f_6$

(A.50) $a_4a_{14} = a_7a_9 + a_8^2 - a_{15}^2f_0 + a_{13}a_{15}f_2 - a_{10}a_{15}f_4 - 3a_{10}a_{13}f_6 - 2a_{11}a_{13}f_5 - 2a_{10}a_{12}f_6$

(A.51) $a_4a_{13} = a_7a_8 - a_{14}a_{15}f_0 - a_{13}a_{15}f_1 - a_{10}a_{13}f_5 - a_{10}a_{11}f_6$

(A.52) $a_3a_{10} = a_6^2 - a_{10}a_{15}f_0 - a_{11}a_{13}f_1 - 2a_{12}a_{13}f_0 - a_{10}^2f_4 - a_{10}a_{11}f_3 - a_{11}^2f_2 - a_{11}a_{12}f_1 - a_{12}^2f_0$

(A.53) $a_3a_{11} = 2a_6a_7 - 2a_{11}a_{15}f_0 - 2a_{12}a_{14}f_0 - 3a_{13}^2f_1 - a_{10}a_{13}f_3 - 2a_{11}a_{13}f_2 - 2a_{12}a_{13}f_1 + a_{10}^2f_5$

(A.54) $a_3a_{13} = a_7^2 - 2a_{13}a_{15}f_0 - a_{12}a_{15}f_0 - a_{13}a_{14}f_1 - a_{13}^2f_2 - a_{10}^2f_6$

(A.55) $a_3a_{15} = a_8^2 - a_{15}^2f_0 - a_{10}a_{15}f_4 - a_{10}a_{14}f_5 - 2a_{10}a_{13}f_6 - a_{10}a_{12}f_6$

(A.56) $a_3a_{14} = 2a_7a_8 - 2a_{14}a_{15}f_0 - a_{13}a_{15}f_1 + a_{10}a_{15}f_3 - a_{10}a_{13}f_5 - 2a_{10}a_{11}f_6$

(A.57) $a_3a_{12} = 2a_6a_8 - 2a_{13}a_{15}f_0 - a_{11}a_{15}f_1 - 2a_{12}a_{15}f_0 + a_{10}a_{14}f_3 + 2a_{10}a_{13}f_4 + a_{10}a_{11}f_5$

(A.58) $a_4a_{10} = a_6a_7 - a_{11}a_{15}f_0 - a_{10}a_{14}f_2 - a_{12}a_{14}f_0 - 2a_{13}^2f_1 - a_{10}a_{13}f_3 - a_{12}a_{13}f_1$

(A.59) $a_4a_{11} = a_6a_8 + a_7^2 - 3a_{13}a_{15}f_0 - a_{10}a_{15}f_2 - 2a_{12}a_{15}f_0 - 2a_{13}a_{14}f_1 + a_{10}a_{13}f_4 - a_{10}^2f_6$

(A.60) $a_4a_{12} = a_6a_9 + a_7a_8 - a_{14}a_{15}f_0 + 2a_{10}a_{15}f_3 + a_{11}a_{15}f_2 + a_{11}a_{13}f_4 - a_{10}a_{11}f_6$

(A.61) $a_6a_{14} = 2a_7a_{13} - a_8a_{11} + a_7a_{12}$

(A.62) $a_9a_{11} = -a_7a_{14} + 2a_8a_{13} + a_8a_{12}$

(A.63) $a_9a_{13} = -a_7a_{15} + a_8a_{14}$

(A.64) $a_8a_{13} = -a_6a_{15} + a_7a_{14}$

(A.65) $a_7a_{13} = -a_9a_{10} + a_8a_{11}$

(A.66) $a_6a_{13} = -a_8a_{10} + a_7a_{11}$

(A.67) $a_{14}a_{14} = 2a_{13}a_{15} + a_{12}a_{15}$

(A.68) $a_{13}a_{13} = a_{10}a_{15}$

(A.69) $a_{11}a_{11} = 2a_{10}a_{13} + a_{10}a_{12}$

(A.70) $a_{12}a_{13} = -2a_{10}a_{15} + a_{11}a_{14}$

(A.71) $a_{11}a_{15} = a_{13}a_{14}$

(A.72) $a_{10}a_{14} = a_{11}a_{13}$.

Appendix B. Local Power Series Expansions

The following are the local power series expansions of $s_1, \ldots, s_{15}$ up to terms quadratic in the f_i's.

(B.1) $s_1 = s_1$

(B.2) $s_2 = s_2$

(B.3) $s_3 = s_1^2 - f_0 s_2^4 - f_4 s_1^4 + 2f_0 f_2 s_2^6 + 2f_0 f_4 s_1^2 s_2^4 + 4f_0 f_5 s_1^3 s_2^3 + (18f_0 f_6 + f_1 f_5) s_1^4 s_2^2 + 8f_1 f_6 s_1^5 s_2 + (4f_2 f_6 - f_3 f_5 + 2f_4^2) s_1^6$

(B.4) $s_4 = s_1 s_2 + f_0 f_3 s_2^6 + 4f_0 f_4 s_1 s_2^5 + (9f_0 f_5 + f_1 f_4) s_1^2 s_2^4 + (20f_0 f_6 + 3f_1 f_5) s_1^3 s_2^3 + (9f_1 f_6 + f_2 f_5) s_1^4 s_2^2 + 4f_2 f_6 s_1^5 s_2 + f_3 f_6 s_1^6$

(B.5) $s_5 = s_2^2 - f_2 s_2^4 - f_6 s_1^4 + (4f_0 f_4 - f_1 f_3 + 2f_2^2) s_2^6 + 8f_0 f_5 s_1 s_2^5 + (18f_0 f_6 + f_1 f_5) s_1^2 s_2^4 + 4f_1 f_6 s_1^3 s_2^3 + 2f_2 f_6 s_1^4 s_2^2 + 2f_4 f_6 s_1^6$

(B.6) $s_6 = s_1^3 + 3f_0 s_1 s_2^4 + 3f_1 s_1^2 s_2^3 + 2f_2 s_1^3 s_2^2 + f_3 s_1^4 s_2 - f_4 s_1^5 + f_0 f_1 s_2^7 + (f_1^2 - 4f_0 f_2) s_1 s_2^6 + (6f_0 f_3 - 3f_1 f_2) s_1^2 s_2^5 + (10f_0 f_4 + 3f_1 f_3 - 2f_2^2) s_1^3 s_2^4 + (18f_0 f_5 + f_1 f_4) s_1^4 s_2^3 + (30f_0 f_6 + 7f_1 f_5 - 2f_2 f_4) s_1^5 s_2^2 + (13f_1 f_6 + 2f_2 f_5 - 2f_3 f_4) s_1^6 s_2 + (6f_2 f_6 - f_3 f_5 + 2f_4^2) s_1^7$

$$s_7 = s_2(s_1^2 + f_0 s_2^4 + f_1 s_1 s_2^3 - f_4 s_1^4 - 2f_0 f_2 s_2^6 + (2f_0 f_3 - 2f_1 f_2) s_1 s_2^5 + 6f_0 f_4 s_1^2 s_2^4 + 10 f_0 f_5 s_1^3 s_2^3 + (22 f_0 f_6 + 2f_1 f_5) s_1^4 s_2^2 + 8 f_1 f_6 s_1^5 s_2 + (4f_2 f_6 - f_3 f_5 + 2f_4^2) s_1^6) \tag{B.7}$$

$$s_8 = s_1(s_2^2 - f_2 s_2^4 + f_5 s_1^3 s_2 + f_6 s_1^4 + (4f_0 f_4 - f_1 f_3 + 2f_2^2) s_2^6 + 8 f_0 f_5 s_1 s_2^5 + (22 f_0 f_6 + 2 f_1 f_5) s_1^2 s_2^4 + 10 f_1 f_6 s_1^3 s_2^3 + 6 f_2 f_6 s_1^4 s_2^2 + (2f_3 f_6 - 2f_4 f_5) s_1^5 s_2 - 2 f_4 f_6 s_1^6) \tag{B.8}$$

$$s_9 = s_2^3 - f_2 s_2^5 + f_3 s_1 s_2^4 + 2 f_4 s_1^2 s_2^3 + 3 f_5 s_1^3 s_2^2 + 3 f_6 s_1^4 s_2 + (6 f_0 f_4 - f_1 f_3 + 2 f_2^2) s_2^7 + (13 f_0 f_5 + 2 f_1 f_4 - 2 f_2 f_3) s_1 s_2^6 + (30 f_0 f_6 + 7 f_1 f_5 - 2 f_2 f_4) s_1^2 s_2^5 + (18 f_1 f_6 + f_2 f_5) s_1^3 s_2^4 + (10 f_2 f_6 + 3 f_3 f_5 - 2 f_4^2) s_1^4 s_2^3 + (6 f_3 f_6 - 3 f_4 f_5) s_1^5 s_2^2 + (f_5^2 - 4 f_4 f_6) s_1^6 s_2 + f_5 f_6 s_1^7 \tag{B.9}$$

$$s_{10} = s_1^4 - 2 f_0 s_1^2 s_2^4 - 2 f_4 s_1^6 + f_0^2 s_2^8 + 4 f_0 f_2 s_1^2 s_2^6 + 6 f_0 f_4 s_1^4 s_2^4 + 8 f_0 f_5 s_1^5 s_2^3 + (36 f_0 f_6 + 2 f_1 f_5) s_1^6 s_2^2 + 16 f_1 f_6 s_1^7 s_2 + (8 f_2 f_6 - 2 f_3 f_5 + 5 f_4^2) s_1^8 \tag{B.10}$$

$$s_{11} = 2 s_1^3 s_2 - 2 f_0 s_1 s_2^5 + f_1 s_1^2 s_2^4 + f_3 s_1^4 s_2^2 - 2 f_4 s_1^5 s_2 + f_5 s_1^6 - f_0 f_1 s_2^8 + 4 f_0 f_2 s_1 s_2^7 - 2 f_1 f_2 s_1^2 s_2^6 + 12 f_0 f_4 s_1^3 s_2^5 + (23 f_0 f_5 + f_1 f_4 - f_2 f_3) s_1^4 s_2^4 + (76 f_0 f_6 + 8 f_1 f_5) s_1^5 s_2^3 + (32 f_1 f_6 + 2 f_2 f_5 - 2 f_3 f_4) s_1^6 s_2^2 + (16 f_2 f_6 - 2 f_3 f_5 + 4 f_4^2) s_1^7 s_2 + (f_3 f_6 - 3 f_4 f_5) s_1^8 \tag{B.11}$$

$$s_{12} = 2 s_1^2 s_2^2 + 2 f_0 s_2^6 + 4 f_1 s_1 s_2^5 + 2 f_2 s_1^2 s_2^4 + 4 f_3 s_1^3 s_2^3 + 2 f_4 s_1^4 s_2^2 + 4 f_5 s_1^5 s_2 + 2 f_6 s_1^6 + (f_1^2 - 6 f_0 f_2) s_2^8 + (4 f_0 f_3 - 8 f_1 f_2) s_1 s_2^7 + (20 f_0 f_4 + 4 f_1 f_3 - 4 f_2^2) s_1^2 s_2^6 + (40 f_0 f_5 + 8 f_1 f_4 - 4 f_2 f_3) s_1^3 s_2^5 + (86 f_0 f_6 + 22 f_1 f_5 - 2 f_2 f_4 + f_3^2) s_1^4 s_2^4 + (40 f_1 f_6 + 8 f_2 f_5 - 4 f_3 f_4) s_1^5 s_2^3 + (20 f_2 f_6 + 4 f_3 f_5 - 4 f_4^2) s_1^6 s_2^2 + (4 f_3 f_6 - 8 f_4 f_5) s_1^7 s_2 + (f_5^2 - 6 f_4 f_6) s_1^8 \tag{B.12}$$

$$s_{13} = s_1^2 s_2^2 - f_0 s_2^6 - f_2 s_1^2 s_2^4 - f_4 s_1^4 s_2^2 - f_6 s_1^6 + 3 f_0 f_2 s_2^8 + (6 f_0 f_4 - f_1 f_3 + 2 f_2^2) s_1^2 s_2^6 + 12 f_0 f_5 s_1^3 s_2^5 + (37 f_0 f_6 + 2 f_1 f_5 + f_2 f_4) s_1^4 s_2^4 + 12 f_1 f_6 s_1^5 s_2^3 + (6 f_2 f_6 - f_3 f_5 + 2 f_4^2) s_1^6 s_2^2 + 3 f_4 f_6 s_1^8 \tag{B.13}$$

$$s_{14} = 2 s_1 s_2^3 + f_1 s_2^6 - 2 f_2 s_1 s_2^5 + f_3 s_1^2 s_2^4 + f_5 s_1^4 s_2^2 - 2 f_6 s_1^5 s_2 + (f_0 f_3 - 3 f_1 f_2) s_2^8 + (16 f_0 f_4 - 2 f_1 f_3 + 4 f_2^2) s_1 s_2^7 + (32 f_0 f_5 + 2 f_1 f_4 - 2 f_2 f_3) s_1^2 s_2^6 + (76 f_0 f_6 + 8 f_1 f_5) s_1^3 s_2^5 + (23 f_1 f_6 + f_2 f_5 - f_3 f_4) s_1^4 s_2^4 + 12 f_2 f_6 s_1^5 s_2^3 - 2 f_4 f_5 s_1^6 s_2^2 + 4 f_4 f_6 s_1^7 s_2 - f_5 f_6 s_1^8 \tag{B.14}$$

$$s_{15} = s_2^4 - 2 f_2 s_2^6 - 2 f_6 s_1^4 s_2^2 + (8 f_0 f_4 - 2 f_1 f_3 + 5 f_2^2) s_2^8 + 16 f_0 f_5 s_1 s_2^7 + (36 f_0 f_6 + 2 f_1 f_5) s_1^2 s_2^6 + 8 f_1 f_6 s_1^3 s_2^5 + 6 f_2 f_6 s_1^4 s_2^4 + 4 f_4 f_6 s_1^6 s_2^2 + f_6^2 s_1^8. \tag{B.15}$$

REFERENCES

[1] Cassels, J. W. S. *The Mordell-Weil Group of Curves of Genus 2.* Arithmetic and Geometry papers dedicated to I. R. Shafarevich on the occassion of his sixtieth birthday, Vol. **1.** Arithmetic, 29-60, Birkhäuser, Boston (1983).

[2] Cassels, J. W. S. *Arithmetic of curves of genus 2.* Number Theory and Applications (Proceedings of a NATO conference in Banff, 1988), Ed. R.A. Mollin, D. Reidel Publishing Co., Netherlands (to appear).

[3] Flynn, E. V. *Curves of Genus 2*, Ph. D. Dissertation, University of Cambridge, 1989.

[4] Grant, D. *Formal Groups in Genus 2.* J. Reine Angew. Math. (to appear).

[5] Lang, S. *Diophantine Geometry*, Springer-Verlag, New York (1963).

[6] Lang, S. *Introduction to Algebraic and Abelian Functions*, 2nd edition, G. T. M. **89**, Springer-Verlag, New York (1982).

[7] Mattuck, A. *Abelian Varieties over p-adic Ground Fields*, Ann. of Math. (2), **62** (1955), 92-119.

[8] Montgomery, P. L. *Speeding up the Pollard and Elliptic Curve Method of Factorization.* Mathematics of Computation, **48**, no.177 (Jan. 1987), 243-264.

[9] Mumford, D. *On the Equations Defining Abelian Varieties I.* Invent. Math. **1** (1966), 287-354.

[10] Mumford, D. *Tata Lectures on Theta.* Progress in Mathematics, I, **28** and II, **43**, Birkhäuser, Boston (1983).

[11] Serre, J. P. *Lie Algebras and Lie Groups.* Benjamin, Reading (1965).

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