Periodical volume

Journal für die reine und angewandte Mathematik

- 411

in: Periodical

221 page(s)

Nutzungsbedingungen

DigiZeitschriften e.V. gewährt ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht kommerziellen Gebrauch bestimmt. Das Copyright bleibt bei den Herausgebern oder sonstigen Rechteinhabern. Als Nutzer sind Sie sind nicht dazu berechtigt, eine Lizenz zu übertragen, zu transferieren oder an Dritte weiter zu geben.

Die Nutzung stellt keine Übertragung des Eigentumsrechts an diesem Dokument dar und gilt vorbehaltlich der folgenden Einschränkungen:

Sie müssen auf sämtlichen Kopien dieses Dokuments alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten; und Sie dürfen dieses Dokument nicht in irgend einer Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen; es sei denn, es liegt Ihnen eine schriftliche Genehmigung von DigiZeitschriften e.V. und vom Herausgeber oder sonstigen Rechteinhaber vor.

Mit dem Gebrauch von DigiZeitschriften e.V. und der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use

DigiZeitschriften e.V. grants the non-exclusive, non-transferable, personal and restricted right of using this document. This document is intended for the personal, non-commercial use. The copyright belongs to the publisher or to other copyright holders. You do not have the right to transfer a licence or to give it to a third party.

Use does not represent a transfer of the copyright of this document, and the following restrictions apply:

You must abide by all notices of copyright or other legal protection for all copies taken from this document; and You may not change this document in any way, nor may you duplicate, exhibit, display, distribute or use this document for public or commercial reasons unless you have the written permission of DigiZeitschriften e.V. and the publisher or other copyright holders.

By using DigiZeitschriften e.V. and this document you agree to the conditions of use.

Kontakt / Contact

DigiZeitschriften e.V.
Papendiek 14
37073 Goettingen
Email: info@digizeitschriften.de

J. reine angew. Math. 411 (1990), 96—121

Journal für die reine und
angewandte Mathematik

© Walter de Gruyter
Berlin · New York 1990

Formal groups in genus two

By *David Grant**) at Boulder

0. Introduction

Despite the machinery of modern algebraic geometry, the study of elliptic curves is still greatly facilitated by explicit knowledge of their defining equations and group laws. The study of abelian surfaces, however, has proceeded largely without benefit of such formulas ([7] notwithstanding). Indeed, Cassels recently lamented: "I cannot even find in the literature an explicit set of equations for the Jacobian of a curve of genus 2 together with explicit expressions for the group operation in a form amenable to calculation [2]."

In this paper we fill that void, providing explicit equations for the Jacobian and its group law. In the case that the curve is defined over a ring complete under a non-archimedean valuation, these equations will allow us to find explicit parameters for the formal group on the kernel of reduction of the Jacobian modulo the maximal ideal of the ring.

The fastest way to find the equations defining the Jacobian and its group law is the nineteenth century approach, working over the complex numbers and using theta functions. It is hoped that the speed and clarity of this method will outweigh what is lost in generality, namely that the paper applies only to curves which contain a rational branch point and are defined over fields of characteristic $\neq 2$.

The equations defining the Jacobian of a curve without a rational branch point have recently been derived by E. V. Flynn [3].

All the necessary analytic theory is contained in a book by Baker [1]. Since this reference is apparently hard to find, in section one we reproduce all the requisite formulas which depend on hyperelliptic theta functions. These are applied in sections 2

*) Partially supported by NSF grant DMS 85-02804 A04.

and 3 to find the equations defining the Jacobian and its group law. The formal group calculations are carried out in section 4.

The proofs of Lemma 2. 6, Theorems 2. 11, 2. 13, and 3. 3 require the manipulation of some rather complex polynomial expressions. These were checked using the program MACSYMA on a Sun 3/50 workstation, which was paid for by a grant from the National Science Foundation.

1. Analytic theory

Let $\mathscr{C}$ be a curve of genus 2 defined over $\mathbb{C}$ by the equation

$$y^2 = x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5 .$$

The function x on $\mathscr{C}$ defines a $2-1$ cover of $\mathbb{P}^1$, branched over ∞ and 5 other points. We think of points on $\mathscr{C}$ as pairs (x, y) with the hyperelliptic involution on $\mathscr{C}$ mapping a point $P=(x, y)$ to $\bar{P}=(x, -y)$.

A basis for the differentials of the first kind on $\mathscr{C}$ is given by $\mu_1 = \frac{dx}{2y}$, $\mu_2 = \frac{x\,dx}{2y}$. There is a standard and canonical way to pick a basis $\{A_1, A_2, B_1, B_2\}$ for $H_1(\mathscr{C}, \mathbb{Z})$ satisfying $A_1 \cdot A_2 = B_1 \cdot B_2 = 0$, and $A_i \cdot B_j = \delta_{ij}$ (see [9], pp. 3. 75—3. 77).[1]

The period matrices ω, ω' and τ are defined by

$$\omega_{ij} = \int_{A_j} \mu_i, \quad \omega'_{ij} = \int_{B_j} \mu_i \quad (i, j = 1, 2), \text{ and } \tau = \omega^{-1}\omega'.$$

Standard calculations show that $\det\omega \neq 0$, and that $\tau \in \mathfrak{h}_2$, the Siegel upper-half space of dimension two.

Let L denote the lattice generated in $\mathbb{C}^2$ by the columns of ω and ω'. Algebraically, the Jacobian J of $\mathscr{C}$ can be described as the symmetric product $\mathscr{C}^{(2)}$ with the locus of unordered pairs $\{(P, \bar{P} \mid P \in \mathscr{C}\}$ blown down to the origin [8]. The Jacobian J will be identified with $\mathbb{C}^2/L$ via the map

$$(P_1, P_2) \xrightarrow{\Phi} \int_{\infty}^{P_1} + \int_{\infty}^{P_2} (\mu_1, \mu_2) \text{ modulo } L.$$

[1] Our formulas will differ slightly from Baker's [1] and Mumford's [9] because the former assumes that the curve is defined by $y^2 = 4x^5 + \ldots$ while the latter chooses dx/y and $x\,dx/y$ as a basis for the differentials of the first kind. Our choices seem to minimize the occurences of "2" in the resulting formulas.

The curve $\mathscr{C}$ can be embedded into J by

$$P \mapsto \Phi(P, \infty).$$

Its image will be denoted by Θ, the theta divisor of J.

Let a and b be column vectors in $\mathbb{Q}^2$. For $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ in $\mathbb{C}^2$, the 2-dimensional theta function with characteristic $\begin{bmatrix} a \\ b \end{bmatrix}$ is defined by

$$\theta\begin{bmatrix} a \\ b \end{bmatrix}(z) = \sum_{n \in \mathbb{Z}^2} e^{\pi i\, {}^t(n+a)\tau(n+a) + 2\pi i\, {}^t(n+a)(z+b)},$$

where n is written as a column vector and ${}^t v$ denotes the transpose of a column vector v.

For any $\begin{bmatrix} a \\ b \end{bmatrix}$ in $\mathbb{Q}^2$, $\theta\begin{bmatrix} a \\ b \end{bmatrix}(z)$ is analytic, and a simple calculation shows the following:

Lemma 1. 1. *Let p, q be column vectors in $\mathbb{Z}^2$. Then*

$$\theta\begin{bmatrix} a \\ b \end{bmatrix}(z + \tau p + q) = e^{-\pi i\, {}^t p\tau p - 2\pi i\, {}^t p(z+b) + 2\pi i\, {}^t a q}\,\theta\begin{bmatrix} a \\ b \end{bmatrix}(z).$$

A fundamental theorem of Riemann states that there are $a, b \in \frac{1}{2}\mathbb{Z}^2$ such that $\theta\begin{bmatrix} a \\ b \end{bmatrix}(z)$ is an odd function with a zero of order one precisely along the pullback of Θ to $\mathbb{C}^2$. A calculation [9], pp. 3. 80—3. 85, shows that with the standard choice of basis for $H_1(\mathscr{C}, \mathbb{Z})$, $a = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 \\ 1/2 \end{pmatrix}$.

The differentials of the second kind on $\mathscr{C}$,

$$\zeta_1 = \frac{(3x^3 + 2b_1x^2 + b_2x)\,dx}{2y} \quad \text{and} \quad \zeta_2 = \frac{x^2\,dx}{2y},$$

are used to form a matrix η of quasiperiods

$$\eta_{ij} = \int_{A_j} \zeta_i, \qquad (i, j = 1, 2).$$

Let $z=\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ be in $\mathbb{C}^2$. The 2-dimensional σ-function is defined by

$$(1.\,2) \qquad \sigma(z)=e^{-1/2\,{}^t z\eta\omega^{-1}z}\,\theta\begin{bmatrix}1/2\\1/2\\1\\1/2\end{bmatrix}(\omega^{-1}z).$$

This has a Taylor expansion [1], p. 96 (see also [4]),

$$(1.\,3) \qquad \sigma(z)=c\Big(z_1+\frac{1}{6}\,b_3 z_1^3-\frac{1}{3}\,z_2^3+(d^\circ\geqq 5)\Big),$$

where c is a nonzero constant related to the discriminant of $\mathscr{C}$ (see [4]), and $(d^\circ\geqq n)$ denotes a power series all of whose terms have total degree of at least n.

Let $\wp_{ij\cdots k}$ denote $-\dfrac{\partial}{\partial z_i}\dfrac{\partial}{\partial z_j}\cdots\dfrac{\partial}{\partial z_k}\log\sigma(z)$, and suppose $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}=\Phi((x_1, y_1), (x_2, y_2))$. Baker [1], p. 38, shows that:

$$(1.\,4) \qquad \wp_{11}(z)$$

$$=\frac{(x_1+x_2)\,(x_1x_2)^2+2b_1(x_1x_2)^2+b_2(x_1+x_2)x_1x_2+2b_3x_1x_2+b_4(x_1+x_2)+2b_5-2y_1y_2}{(x_1-x_2)^2},$$

$$\wp_{12}(z)=-x_1x_2,$$

$$\wp_{22}(z)=x_1+x_2,$$

$$\wp_{111}(z)=2\,\frac{y_2\,\psi(x_1, x_2)-y_1\,\psi(x_2, x_1)}{(x_1-x_2)^3}, \quad \text{where}$$

$$\psi(x_1, x_2)$$

$$=4b_5+b_4(3x_1+x_2)+2b_3x_1(x_1+x_2)+b_2x_1^2(x_1+3x_2)+4b_1x_1^3x_2+x_1^3\,x_2(3x_1+x_2),$$

$$\wp_{112}(z)=2\,\frac{y_1x_2^2-y_2x_1^2}{x_1-x_2},$$

$$\wp_{122}(z)=-2\,\frac{y_1x_2-y_2x_1}{x_1-x_2},$$

$$\wp_{222}(z)=2\,\frac{y_1-y_2}{x_1-x_2}.$$

Let $\mathfrak{p} = \mathfrak{p}_{11}\mathfrak{p}_{22} - \mathfrak{p}_{11}^2$. The expansion (1. 3) gives us:

$$
\begin{aligned}
(1.\ 5) \qquad & \frac{1}{c^2}\,\sigma(z)^2\,\mathfrak{p}_{11}(z) = 1 + (d^\circ \geqq 4),\\
& \frac{1}{c^2}\,\sigma(z)^2\,\mathfrak{p}_{12}(z) = -z_2^2 + (d^\circ \geqq 4),\\
& \frac{1}{c^2}\,\sigma(z)^2\,\mathfrak{p}_{22}(z) = 2z_1 z_2 + (d^\circ \geqq 4),\\
& \frac{1}{c^3}\,\sigma(z)^3\,\mathfrak{p}_{111}(z) = -2 + (d^\circ \geqq 2),\\
& \frac{1}{c^3}\,\sigma(z)^3\,\mathfrak{p}_{112}(z) = 2z_2^2 + (d^\circ \geqq 4),\\
& \frac{1}{c^3}\,\sigma(z)^3\,\mathfrak{p}_{122}(z) = -2z_1 z_2 + (d^\circ \geqq 4),\\
& \frac{1}{c^3}\,\sigma(z)^3\,\mathfrak{p}_{222}(z) = 2z_1^2 + (d^\circ \geqq 4),\\
& \frac{1}{c^3}\,\sigma(z)^3\,\mathfrak{p}(z) = 2z_2 + (d^\circ \geqq 3).
\end{aligned}
$$

For a divisor D on J, let $l(D)$ be the dimension of $\mathscr{L}(D)$, the space of functions f on J such that $(f) + D$ is an effective divisor.

Lemma 1. 1 shows that the even functions $\mathfrak{p}_{11}$, $\mathfrak{p}_{12}$, and $\mathfrak{p}_{22}$ are in $\mathscr{L}(2\Theta)$, and that the odd functions $\mathfrak{p}_{111}$, $\mathfrak{p}_{112}$, $\mathfrak{p}_{122}$, and $\mathfrak{p}_{222}$ are in $\mathscr{L}(3\Theta)$. Writing out the even function $\mathfrak{p}$ in terms of partial derivatives shows that it too lies in $\mathscr{L}(3\Theta)$. Similarly, its derivatives $\dfrac{\partial\mathfrak{p}}{\partial z_1} = \mathfrak{p}_{11}\mathfrak{p}_{122} + \mathfrak{p}_{111}\mathfrak{p}_{22} - 2\mathfrak{p}_{12}\mathfrak{p}_{112}$ and $\dfrac{\partial\mathfrak{p}}{\partial z_2} = \mathfrak{p}_{11}\mathfrak{p}_{222} + \mathfrak{p}_{112}\mathfrak{p}_{22} - 2\mathfrak{p}_{12}\mathfrak{p}_{122}$ are odd functions which lie in $\mathscr{L}(4\Theta)$.

Since Θ is an ample divisor with a self-intersection number of 2, the Riemann-Roch Theorem implies that $l(n\Theta) = n^2$ for $n \geqq 1$. It follows from (1. 5) that:

$$
\begin{aligned}
(1.\ 6) \qquad & \mathscr{L}(\Theta) = \mathbb{C},\\
& \mathscr{L}(2\Theta)/\mathscr{L}(\Theta) = \mathbb{C}\mathfrak{p}_{11} \oplus \mathbb{C}\mathfrak{p}_{12} \oplus \mathbb{C}\mathfrak{p}_{22},\\
& \mathscr{L}(3\Theta)/\mathscr{L}(2\Theta) = \mathbb{C}\mathfrak{p}_{111} \oplus \mathbb{C}\mathfrak{p}_{112} \oplus \mathbb{C}\mathfrak{p}_{122} \oplus \mathbb{C}\mathfrak{p}_{222} \oplus \mathbb{C}\mathfrak{p},\\
& \mathscr{L}(4\Theta)/\mathscr{L}(3\Theta) = \mathbb{C}\mathfrak{p}_{11}^2 \oplus \mathbb{C}\mathfrak{p}_{11}\mathfrak{p}_{12} \oplus \mathbb{C}\mathfrak{p}_{11}\mathfrak{p}_{22} \oplus \mathbb{C}\mathfrak{p}_{12}\mathfrak{p}_{22} \oplus \mathbb{C}\mathfrak{p}_{22}^2 \oplus \mathbb{C}\frac{\partial\mathfrak{p}}{\partial z_1} \oplus \mathbb{C}\frac{\partial\mathfrak{p}}{\partial z_2}, \text{ and}\\
& \mathscr{L}(5\Theta)/\mathscr{L}(4\Theta) = \mathfrak{p}_{22}\mathscr{L}(3\Theta) \oplus \mathbb{C}\mathfrak{p}\mathfrak{p}_{11} \oplus \mathbb{C}\mathfrak{p}\mathfrak{p}_{12} \oplus \mathbb{C}\mathfrak{p}_{111}\mathfrak{p}_{11} \oplus \mathbb{C}\mathfrak{p}_{111}\mathfrak{p}_{12}.
\end{aligned}
$$

A theorem of Lefschetz [6], p. 105, guarantees that the complete linear system $|3\Theta|$ defines a projective embedding i of J into $\mathbb{P}^8$:

$$(1.7) \quad i(z)=(\sigma^3, \sigma^3\wp_{11}, \sigma^3\wp_{12}, \sigma^3\wp_{22}, \sigma^3\wp_{111}, \sigma^3\wp_{112}, \sigma^3\wp_{122}, \sigma^3\wp_{222}, \sigma^3\wp)(z).$$

2. The equations defining the Jacobian

The equations defining J can be written down explicitly in terms of the coordinate functions determined by (1.7).

Let $S=\mathbb{C}[X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X]$, and $I(J)$ be the ideal of homogeneous polynomials in S which vanish on $i(J)$. Any set of generators of $I(J)$ provides a set of defining equations for J as a projective variety.

It is more convenient first to write down generators for the ideal defining the affine variety $i(J)\cap(X_0\neq 0)$ (Thm. 2.5). We will then find elements of the ideal which when homogenized with respect to X_0 define the projective closure of this variety. We do this by first making sure that the homogenized polynomials have the proper restriction to the subvariety cut out by $X_0=0$ (Thm. 2.11), and then by verifying that they satisfy the Jacobian criterion for non-singularity (Thm. 2.13).

Since $\sigma(z)=0$ precisely for those z in $\mathbb{C}^2/L$ which lie on Θ, we have

$$i(J)\cap(X_0\neq 0)=i(J-\Theta).$$

Let $U=J-\Theta$, $R=\mathbb{C}[X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X]$, and let $\mathcal{O}(U)$ denote the ring of regular functions on U. We have the isomorphism

$$R/I(U)\cong\mathcal{O}(U)=\mathbb{C}[\wp_{11}, \wp_{12}, \wp_{22}, \wp_{111}, \wp_{112}, \wp_{122}, \wp_{222}, \wp],$$

where $I(U)$ is the ideal of polynomials in R which vanish on $i(U)$.

We give $\mathcal{O}(U)$ the structure of a graded ring by identifying it with $\bigcup_n \mathscr{L}(n\Theta)$. Since Θ is a symmetric divisor, multiplication by -1 induces an involution on $\mathscr{L}(n\Theta)$ and on $\mathcal{O}(U)$. Let

$$\mathscr{L}(n\Theta)\cong\mathrm{Even}_n\oplus\mathrm{Odd}_n,$$

and

$$\mathcal{O}(U)\cong\mathrm{Even}\oplus\mathrm{Odd}$$

denote respectively the decomposition of $\mathscr{L}(n\Theta)$ and $\mathcal{O}(U)$ into positive and negative eigenspaces under this involution.

Proposition 2. 1. i) *For* $n \geqq 1$,

$$\dim(\mathrm{Even}_{2n}/\mathrm{Even}_{2n-1}) = 2n+1,$$
$$\dim(\mathrm{Odd}_{2n}/\mathrm{Odd}_{2n-1}) \;= 2n-2,$$
$$\dim(\mathrm{Even}_{2n+1}/\mathrm{Even}_{2n}) = 2n-1,$$
$$\dim(\mathrm{Odd}_{2n+1}/\mathrm{Odd}_{2n}) \;= 2n+2.$$

ii) *For* $n \geqq 2$,

$$\mathrm{Even}_{2n+2}/\mathrm{Even}_{2n+1} = (\mathbb{C}\mathfrak{p}_{11}^{n+1} \oplus \mathbb{C}\mathfrak{p}_{11}^{n}\mathfrak{p}_{12} \oplus \mathfrak{p}_{22}\,\mathrm{Even}_{2n})/\mathrm{Even}_{2n+1},$$
$$\mathrm{Odd}_{2n+2}/\mathrm{Odd}_{2n+1} \;= \mathfrak{p}(\mathrm{Odd}_{2n-1}/\mathrm{Odd}_{2n-2}),$$
$$\mathrm{Even}_{2n+3}/\mathrm{Even}_{2n+2} = \mathfrak{p}(\mathrm{Even}_{2n}/\mathrm{Even}_{2n-1}),$$
$$\mathrm{Odd}_{2n+3}/\mathrm{Odd}_{2n+2} \;= (\mathbb{C}\mathfrak{p}_{111}\mathfrak{p}_{11}^{n} \oplus \mathbb{C}\mathfrak{p}_{111}\mathfrak{p}_{12}\mathfrak{p}_{11}^{n-1} \oplus \mathfrak{p}_{22}\,\mathrm{Odd}_{2n+1})/\mathrm{Odd}_{2n+2}.$$

Proof. We proceed by induction. For $n=1$ and 2, i) follows from (1. 6). Now take $n \geqq 2$ and assume that i) holds for positive integers up to n.

From (1. 6) we have the following inclusions:

$$(2.\,2)\quad \mathrm{Even}_{2n+2}/\mathrm{Even}_{2n+1} \supseteqq (\mathbb{C}\mathfrak{p}_{11}^{n+1} \oplus \mathbb{C}\mathfrak{p}_{11}^{n}\mathfrak{p}_{12} \oplus \mathfrak{p}_{22}\,\mathrm{Even}_{2n})/\mathrm{Even}_{2n+1},$$
$$\mathrm{Odd}_{2n+2}/\mathrm{Odd}_{2n+1} \;\supseteqq \mathfrak{p}(\mathrm{Odd}_{2n-1}/\mathrm{Odd}_{2n-2}),$$
$$\mathrm{Even}_{2n+3}/\mathrm{Even}_{2n+2} \supseteqq \mathfrak{p}(\mathrm{Even}_{2n}/\mathrm{Even}_{2n-1}),$$
$$\mathrm{Odd}_{2n+3}/\mathrm{Odd}_{2n+2} \;\supseteqq (\mathbb{C}\mathfrak{p}_{111}\mathfrak{p}_{11}^{n} \oplus \mathbb{C}\mathfrak{p}_{111}\mathfrak{p}_{12}\mathfrak{p}_{11}^{n-1} \oplus \mathfrak{p}_{22}\,\mathrm{Odd}_{2n+1})/\mathrm{Odd}_{2n+2}.$$

It follows from the inductive hypothesis and (1. 5) that the right-hand sides of (2. 2) have dimensions of $2n+3$, $2n$, $2n+1$, and $2n+4$, respectively. By the Riemann-Roch Theorem, the dimensions of $\mathscr{L}((2n+2)\Theta)/\mathscr{L}((2n+1)\Theta)$ and $\mathscr{L}((2n+3)\Theta)/\mathscr{L}((2n+2)\Theta)$ are $4n+3$ and $4n+5$, respectively. So the containments (2. 2) are in fact equalities. Hence ii) holds for n, and i) holds for $n+1$.

Corollary 2. 3.

1) $\mathrm{Even} \cong \mathbb{C}[\mathfrak{p}_{11}, \mathfrak{p}_{12}, \mathfrak{p}_{22}, \mathfrak{p}]$

$$\cong \mathbb{C}[\mathfrak{p}_{11}, \mathfrak{p}_{22}] \oplus \mathfrak{p}\,\mathbb{C}[\mathfrak{p}_{11}, \mathfrak{p}_{22}] \oplus \mathfrak{p}_{12}\,\mathbb{C}[\mathfrak{p}_{11}, \mathfrak{p}_{22}] \oplus \mathfrak{p}\,\mathfrak{p}_{12}\,\mathbb{C}[\mathfrak{p}_{11}, \mathfrak{p}_{22}].$$

2) $I(U) \cong \mathrm{Even}[\mathrm{Odd}_3, \mathrm{Odd}_4] = \mathrm{Even}[\mathfrak{p}_{111}, \mathfrak{p}_{112}, \mathfrak{p}_{122}, \mathfrak{p}_{222}]$.

Lemma 2. 4. *If* $e_1\,\mathfrak{p}_{122} + e_2\,\mathfrak{p}_{222} = 0$, *for some* e_1 *and* $e_2 \in$ Even, *then*

$$e_1 = \mathfrak{p}_{222}\,o_1 \quad and \quad e_2 = \mathfrak{p}_{122}\,o_2$$

for some o_1 *and* $o_2 \in$ Odd.

Proof. It suffices to show that the divisors of zeroes $(\wp_{122})_0$ and $(\wp_{222})_0$ have no component in common. So suppose

$$0=\wp_{122}(z)=-2\frac{y_1x_2-y_2x_1}{x_1-x_2}=\wp_{222}(z)=2\frac{y_1-y_2}{x_1-x_2}.$$

If $x_1=x_2$, then for $z\notin L$, $y_1=y_2$, and

$$\wp_{222}(z)=2\frac{y_1^2-y_2^2}{(x_1-x_2)(y_1+y_2)}=\frac{5x_1^4+4b_1x_1^3+3b_2x_1^2+2b_3x_1+b_4}{2y_1}.$$

So $((x_1-x_2)^2)_0$ and $(\wp_{222})_0$ have no components in common. So except for finitely many points, the above implies:

$$y_2x_1-y_1x_2=y_1-y_2=0, \quad \text{and} \quad x_1\neq x_2,$$

which only holds for finitely many points. Hence $(\wp_{222})_0$ and $(\wp_{122})_0$ have no component in common.

Theorem 2. 5. *Let*

$$\begin{aligned}
f_1 &= X^2+X_{11}^2X_{12}-b_1X_{11}^2X_{22}+b_2X_{11}X_{12}X_{22}-b_3X_{11}X_{22}^2+b_4X_{12}X_{22}^2\\
&\quad -b_5X_{22}^3+2b_1XX_{11}-2b_2XX_{12}+2b_3XX_{22}+(b_3-b_1b_2)X_{11}X_{12}\\
&\quad +(b_2^2-b_1b_3)X_{11}X_{22}+(b_1b_4-b_2b_3-b_5)X_{12}X_{22}-b_1b_5X_{22}^2\\
&\quad +2(b_1b_3-b_2^2)X+(b_1b_4-b_5)X_{11}+b_2(b_2^2-b_1b_3)X_{12}\\
&\quad +(b_3b_4-b_2b_5)X_{22}+b_1b_3b_4-b_2^2b_4-b_3b_5,\\
f_2 &= 2X-X_{11}X_{22}+X_{12}^2-b_2X_{12}+b_4,\\
f_3 &= X_{112}-X_{222}X_{12}+X_{122}X_{22},\\
f_4 &= X_{111}+X_{222}X_{11}+X_{122}X_{12}-2X_{112}X_{22}-2b_1X_{112}+b_2X_{122},\\
f_5 &= X_{122}^2-X_{11}X_{22}^2+2XX_{22}+X_{11}X_{12}-b_1X_{11}X_{22}-b_2X_{12}X_{22}+2b_1X\\
&\quad -b_1b_2X_{12}+b_4X_{22}+b_1b_4-b_5,\\
f_6 &= X_{222}^2-X_{22}^3-X_{12}X_{22}-b_1X_{22}^2-X_{11}-b_2X_{22}-b_3,\\
f_7 &= X_{122}X_{222}-X_{12}X_{22}^2+X-b_2X_{12}-b_1X_{12}X_{22}.
\end{aligned}$$

Then $I(U)=(f_1,f_2,f_3,f_4,f_5,f_6,f_7)$, *so* f_1-f_7 *are defining polynomials for* U.

Remarks. 1) It is easy to show that $f_1\in(f_5,f_6,f_7)$, so in fact f_2-f_7 suffice to define U.

2) Hence using f_2, f_3, f_4, and f_6 to eliminate respectively X, X_{112}, X_{111}, and X_{11}, we get an isomorphic embedding of U into $\mathbb{A}^4$ by $z \mapsto (\wp_{12}, \wp_{22}, \wp_{122}, \wp_{222})(z)$. This is a special case of a general phenomenon for hyperelliptic curves (see [9], p. 3. 20).

3) There is also a nice embedding of U into $\mathbb{A}^5$ given by

$$z \mapsto (\wp_{22}, \wp_{222}, \wp_{2222}, \wp_{22222}, \wp_{222222})(z)$$

(see [9], p. 3. 175).

Proof. The result follows from the next three lemmas.

Lemma 2. 6. *When* $X_{11} = \wp_{11}$, $X_{12} = \wp_{12}$, $X_{22} = \wp_{22}$, $X_{111} = \frac{1}{2}\wp_{111}$, $X_{112} = \frac{1}{2}\wp_{112}$, $X_{122} = \frac{1}{2}\wp_{122}$, $X_{222} = \frac{1}{2}\wp_{222}$, *and* $X = \frac{1}{2}(\wp + b_2\wp_{12} - b_4)$, *the polynomials* f_1, f_2, f_3, f_4, f_5, f_6, *and* f_7 *are identically zero.*

Proof. These can all be established from (1. 4) by direct computation. Note that f_2 is just the definition of $\wp$. Also, f_1, f_5, f_6, and f_7 can be found in [1], p. 41.

Lemma 2. 7. $\quad \text{Even} \cong \mathbb{C}[X_{11}, X_{12}, X_{22}, X]/(f_1, f_2)$.

Proof. By the previous lemma, f_1 and f_2 express $\wp_{12}^2$ and $\wp^2$ as elements of

$$\mathbb{C}[\wp_{11}, \wp_{22}] \oplus \wp\,\mathbb{C}[\wp_{11}, \wp_{22}] \oplus \wp_{12}\,\mathbb{C}[\wp_{11}, \wp_{22}] \oplus \wp\wp_{12}\,\mathbb{C}[\wp_{11}, \wp_{22}].$$

Therefore by Corollary 2. 3,

$$\text{Even} \cong \mathbb{C}[\wp_{11}, X_{12}, \wp_{22}, X]/(f_1(\wp_{11}, X_{12}, \wp_{22}, X), f_2(\wp_{11}, X_{12}, \wp_{22}, X)).$$

Furthermore, $\mathbb{C}[\wp_{11}, \wp_{22}] \cong \mathbb{C}[X_{11}, X_{22}]$, because by Corollary 2. 3,

$$2 = \dim(J) = \text{tr.deg.}(K(J)) = \text{tr.deg.}(\mathbb{C}(\wp_{11}, \wp_{22})).$$

Lemma 2. 8. *For* $3 \leqq i \leqq 7$, *let*

$$g_i(X_{111}, X_{112}, X_{122}, X_{222}) = f_i(\wp_{11}, \wp_{12}, \wp_{22}, X_{111}, X_{112}, X_{122}, X_{222}, \frac{1}{2}(\wp + b_2\wp_{12} - b_4)).$$

Then,

$$I(U) = \text{Even}[X_{111}, X_{112}, X_{122}, X_{222}]/(g_3, g_4, g_5, g_6, g_7).$$

Proof. For $i = 3, 4$, let

$$h_i(X_{111}, X_{112}) = g_i(X_{111}, X_{112}, \frac{1}{2}\wp_{122}, \frac{1}{2}\wp_{222}).$$

From Corollary 2.3 we have,

$$(2.9)\qquad \begin{aligned} I(U) &= \mathrm{Even}[X_{111}, X_{112}, \mathfrak{p}_{122}, \mathfrak{p}_{222}]/(h_3, h_4) \\ &= \mathrm{Even}[\mathfrak{p}_{122}, \mathfrak{p}_{222}] \\ &= \mathrm{Even} \oplus \mathfrak{p}_{122}\,\mathrm{Even} + \mathfrak{p}_{222}\,\mathrm{Even}, \end{aligned}$$

where the last sum is not direct.

Let $T = \mathrm{Even}[X_{122}, X_{222}]/(g_5, g_6, g_7)$. From Lemma 2.6 we have a well-defined projection

$$\pi : T \longrightarrow \mathrm{Even}[\mathfrak{p}_{122}, \mathfrak{p}_{222}]$$

by sending $X_{112} \longrightarrow \frac{1}{2}\mathfrak{p}_{112}$ and $X_{222} \longrightarrow \frac{1}{2}\mathfrak{p}_{222}$.

The polynomials g_5, g_6 and g_7 can be used to kill off all quadratic terms in X_{112} and X_{122}, so every element of T can be represented as $e_0 + e_1 X_{122} + e_2 X_{222}$ for some $e_0, e_1, e_2 \in \mathrm{Even}$.

Suppose that

$$\pi(e_0 + e_1 X_{122} + e_2 X_{222}) = e_0 + e_1 \mathfrak{p}_{122} + e_2 \mathfrak{p}_{222} = 0.$$

Isolating odd and even parts gives:

$$e_0 = e_1 \mathfrak{p}_{122} + e_2 \mathfrak{p}_{222} = 0.$$

So by Lemma 2.4 and (2.9),

$$(2.10)\qquad e_1 = \mathfrak{p}_{222}\, o_1 = \mathfrak{p}_{222}(e_3 \mathfrak{p}_{122} + e_4 \mathfrak{p}_{222})$$

for some $o_1 \in \mathrm{Odd}$, and $e_3, e_4 \in \mathrm{Even}$.

Write $\mathfrak{p}_{122}^2 = e_5$, $\mathfrak{p}_{222}^2 = e_6$, and $\mathfrak{p}_{122}\mathfrak{p}_{222} = e_7$, where $e_5, e_6, e_7 \in \mathrm{Even}$. Then,

$$0 = e_1 \mathfrak{p}_{122} + e_2 \mathfrak{p}_{222} = \mathfrak{p}_{222}(e_3 e_5 + e_4 e_7 + e_2).$$

So working in T,

$$\begin{aligned} e_1 X_{122} + e_2 X_{222} &= e_1 X_{122} - (e_3 e_5 + e_4 e_7) X_{222} \\ &= e_1 X_{122} - e_3 X_{122}^2 X_{222} - e_4 X_{122} X_{222}^2 \\ &= X_{122}(e_1 - e_3 e_7 - e_4 e_6). \end{aligned}$$

From (2.10) we see $e_1 = e_3 e_7 + e_4 e_6$, so π is injective.

Recall that $i(J)\cap(X_0=0)=i(\Theta)=i(\Phi(\mathscr{C}))$. For a polynomial $g\in R$ we let $g^h\in S$ denote g homogenized with respect to X_0. If $g_1,\dots,g_t$ are a set of polynomials, we let $Z(g_1,\dots,g_t)$ denote their common zeroes.

Theorem 2. 11. *Let f_2 and f_6 be as in 2. 5, and*:

$$\begin{aligned} f_8 &= X_{111}^2-X_{11}^3-b_3X_{11}^2-b_4X_{11}X_{12}+3b_5X_{11}X_{22}+2b_5X \\ &\quad +(4b_1b_5-b_2b_4)X_{11}-3b_2b_5X_{12}+(4b_3b_5-b_4^2)X_{22} \\ &\quad +4b_1b_3b_5+b_4b_5-b_1b_4^2-b_2^2b_5, \\ f_9 &= -X_{111}X_{112}+b_1X_{111}X_{122}-b_2X_{112}X_{122}+b_3X_{112}X_{222}-b_4X_{122}X_{222} \\ &\quad +b_5X_{222}^2-X^2-b_1XX_{11}+b_2XX_{12}-b_3XX_{22}-b_3X_{11}X_{12} \\ &\quad +b_1b_3X_{11}X_{22}-(b_5+b_1b_4)X_{12}X_{22}+2b_1b_5X_{22}^2-2(b_1b_3+b_4)X \\ &\quad -2b_5X_{11}+(2b_2b_4+b_1b_2b_3+b_1b_5-b_3^2-b_1^2b_4)X_{12}+2b_5(b_1^2-b_2)X_{22} \\ &\quad +b_1b_2b_5-b_1b_3b_4-2b_3b_5, \\ f_{10} &= X_{122}^2-X_{111}X_{122}+X_{11}X-b_3X_{11}X_{22}+2b_4X_{12}X_{22}-3b_5X_{22}^2+2b_3X \\ &\quad +(b_1b_4-b_2b_3-b_5)X_{12}-2b_1b_5X_{22}+b_3b_4-b_2b_5, \\ f_{11} &= X_{111}X_{222}-X_{112}X_{122}-2XX_{12}+X_{11}^2-2b_1X_{11}X_{12}+3b_2X_{11}X_{22} \\ &\quad -2b_3X_{12}X_{22}+b_4X_{22}^2-5b_2X+b_3X_{11}+(3b_2^2-2b_1b_3)X_{12} \\ &\quad +(b_1b_4-b_5)X_{22}-2b_2b_4, \\ f_{12} &= X_{122}^2-X_{112}X_{222}+X_{22}X+2X_{11}X_{12}-b_1X_{11}X_{22}+2b_1X \\ &\quad +(b_3-b_1b_2)X_{12}+b_1b_4-b_5. \end{aligned}$$

Then f_8-f_{12} are in $I(U)$, and $Z(f_2^h, f_6^h, f_8^h, f_9^h, f_{10}^h, f_{11}^h, f_{12}^h, X_0)$ is isomorphic to $\mathscr{C}$.

Proof. It is straightforward to show that f_8-f_{12} are in the ideal generated by f_2-f_7.

To establish the remainder of the theorem, note that $Z(f_6^h, X_0)=Z(X_{22}, X_0)$ and $Z(f_8^h, X_0)=Z(X_{11}, X_0)$. Hence $Z(f_2^h, f_6^h, f_8^h, X_0)=Z(X_{11}, X_{12}, X_{22}, X_0)$. Therefore,

$$Z(f_2^h, f_6^h, f_8^h, f_9^h, f_{10}^h, f_{11}^h, f_{12}^h, X_0)$$

is isomorphic to the variety in $\mathbb{P}^4$ defined by:

$$\begin{gathered} X_{112}^2-X_{111}X_{122}, \\ X_{111}X_{222}-X_{112}X_{122}, \\ X_{122}^2-X_{112}X_{222}, \quad \text{and} \end{gathered} \tag{2. 12}$$

$$-X_{111}X_{112}+b_1X_{111}X_{122}-b_2X_{112}X_{122}+b_3X_{112}X_{222}-b_4X_{122}X_{222}+b_5X_{222}^2-X^2.$$

The complete linear system $|6\infty|$ determines an embedding of $\mathscr{C}$ into $\mathbb{P}^4$ via

$$P \mapsto (1,\ -x,\ x^2,\ -x^3,\ y)\,(P),$$

and it is easy to identify the image of $\mathscr{C}$ with the zeroes of the polynomials (2. 12) in $\mathbb{C}[X_{222}, X_{122}, X_{112}, X_{111}, X]$.

Theorem 2. 13. *Suppose $\mathscr{C}$ is a non-singular curve of genus two defined by*

$$y^2 = f(x),$$

where

$$f(x) = x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5,$$

and the b_i lie in any field F of characteristic $\neq 2$. Let $f_2 - f_7$ be as in 2. 5, $f_8 - f_{12}$ as in 2. 11 and:

$$f_{13} = X_{111} X_{12} - X_{112} X_{11} - b_4 X_{122} + 2 b_5 X_{222},$$

$$f_{14} = 2 X_{122} X_{11} - X_{112} X_{12} - X_{111} X_{22} - b_2 X_{112} + 2 b_3 X_{122} - b_4 X_{222}.$$

Then f_{13} and f_{14} are in $I(U)$, and the Jacobian matrix of $f_i^h = 0$, $2 \leqq i \leqq 14$, has maximal rank at every point of $Z(\{f_i^h | 2 \leqq i \leqq 14\})$.

The proof is rather computational, and so will be postponed momentarily in favor of the following corollaries.

Corollary 2. 14. *For $\mathscr{C}$ defined over $\mathbb{C}$, the equations*

$$f_i^h = 0, \qquad 2 \leqq i \leqq 14,$$

are a set of defining equations for $i(J)$.

Proof. By 2. 5 and 2. 11, $i(J) = Z(\{f_i^h | 2 \leqq i \leqq 14\})$; we need only show that the ideal $\mathfrak{a} = (\{f_i^h | 2 \leqq i \leqq 14\})$ is radical, or equivalently, that the scheme $Y = \operatorname{Proj}(S/\mathfrak{a})$ is reduced. It suffices to show that for every $y \in Y$, the local ring $\mathcal{O}_{Y,y}$ is reduced. But by Theorem 2. 13, $\mathcal{O}_{Y,y}$ is a regular local ring, and hence has no nilpotents.

Corollary 2. 15. *Suppose $\mathscr{C}$ is a non-singular curve of genus two defined by*

$$y^2 = x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5,$$

where the b_i lie in any field F of characteristic $\neq 2$. Then $f_i^h = 0$, $2 \leqq i \leqq 14$, are a set of defining equations for the Jacobian of $\mathscr{C}$.

Proof. By the Lefschetz principle, Corollary 2.14 holds for any field of characteristic zero. Now let F be any field of characteristic $p \neq 2$. We will give $\mathscr{C}$ the structure of a non-singular projective curve by glueing together the two affine patches

$$U: y^2 = x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5 = f(x),$$
$$V: s^2 = t + b_1 t^2 + b_2 t^3 + b_3 t^4 + b_4 t^5 + b_5 t^6$$

along the identification $t = 1/x$, $s = y/x^3$. We will let W be the affine open set where $r = \dfrac{y}{(x-1)^3}$, and $q = \dfrac{1}{x-1}$ are regular.

Let $x_i, y_i, t_i, s_i, q_i, r_i$ be the corresponding coordinate functions on copies

$$U_i,\ V_i,\ W_i; \qquad i = 1, 2.$$

Let π denote the natural projection of $\mathscr{C} \times \mathscr{C}$ onto the symmetric product $\mathscr{C}^{(2)}$. Then the open cover $\mathbf{U} = \pi(U_1 \times U_2)$, $\mathbf{V} = \pi(V_1 \times V_2)$, $\mathbf{W} = \pi(W_1 \times W_2)$ gives $\mathscr{C}^{(2)}$ the structure of a non-singular projective variety.

Let Y denote the algebraic set defined by $f_2^h - f_{14}^h$ in $P^8(F)$. Keeping the notation of (1.4),

$$(2.16) \qquad (X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X)$$
$$= \Bigg(1, \frac{(x_1+x_2)(x_1x_2)^2 + 2b_1(x_1x_2)^2 + b_2(x_1+x_2)x_1x_2 + 2b_3x_1x_2 + b_4(x_1+x_2) + 2b_5 - 2y_1y_2}{(x_1-x_2)^2},$$
$$-x_1x_2,\ x_1+x_2,\ \frac{y_2\psi(x_1,x_2) - y_1\psi(x_2,x_1)}{(x_1-x_2)^3},\ \frac{y_1x_2^2 - y_2x_1^2}{x_1-x_2},\ \frac{y_2x_1 - y_1x_2}{x_1-x_2},\ \frac{y_1-y_2}{x_1-x_2},$$
$$\frac{2(x_1x_2)^3 + b_1(x_1+x_2)(x_1x_2)^2 + 2b_2(x_1x_2)^2 + b_3(x_1+x_2)x_1x_2 + 2b_4x_1x_2 + b_5(x_1+x_2) - y_1y_2(x_1+x_2)}{(x_1-x_2)^2}\Bigg)$$

defines a continuous map from $\mathbf{U} \cap (x_1 \neq x_2)$ into Y. (This is seen most easily by lifting $\mathscr{C}$ to a curve over a field of characteristic zero, and applying Lemma 2.6 and Theorems 2.11 and 2.13.) We will show that (2.16) extends to a surjective morphism from $\mathscr{C}^{(2)}$ onto Y. Therefore Y is connected, so by 2.13, it is smooth, hence reduced and irreducible, and therefore a non-singular projective variety. Further, (2.16) defines a birational transformation from $\mathscr{C}^{(2)}$ to Y, via the identification of function fields:

$$K(\mathscr{C}^{(2)}) = F(x_1+x_2, x_1x_2, y_1+y_2, y_1y_2) = F(X_{22}, X_{12}, X_{11}, X_{222}) = K(Y).$$

Let i denote the hyperelliptic involution of $\mathscr{C}$, and D the divisor of $\mathscr{C}^{(2)}$ which is the image of the composite

$$\mathscr{C} \xrightarrow{1 \times i} \mathscr{C} \times \mathscr{C} \xrightarrow{\pi} \mathscr{C}^{(2)}.$$

When we extend (2. 16) to a surjective morphism

$$\phi : \mathscr{C}^{(2)} \longrightarrow Y,$$

we will verify that the divisor D is mapped to a single point. This shows that Y is the Jacobian of $\mathscr{C}$. Indeed then ϕ factors as

$$\begin{tikzcd}
\mathscr{C}^{(2)} \arrow[rr, "\phi"] \arrow[dr, "\psi"'] & & Y \\
& J \arrow[ur, "\tau"'] &
\end{tikzcd}$$

where ψ^{-1} is the monoidal transformation blowing up a point on J to the exceptional curve D on $\mathscr{C}^{(2)}$. Then J is the Jacobian of $\mathscr{C}$, and τ must be an isomorphism since an abelian surface is a relative minimal model.

We will show in detail how (2. 16) extends to $\mathbf{U}$, verifying that $\mathbf{U} \cap D$ collapses to a point. We will then quickly sketch the way it extends to $\mathbf{V}$ and maps $\mathbf{V} \cap D$ to a point. This simultaneously proves the same for $\mathbf{W}$ by considering the isomorphic curve $y^2 = f(x+1)$. Finally, we will verify that ϕ is surjective.

Over any field of characteristic $p \neq 2$, the coordinate ring on the affine set of Y defined by $X_0 = 1$ is generated by X_{12}, X_{22}, X_{122}, and X_{222}. Therefore we can extend (2. 16) to $\mathbf{U} \cap (y_1 \neq -y_2)$ via the identifications:

$$\frac{y_1 - y_2}{x_1 - x_2} = \left(\frac{f(x_1) - f(x_2)}{x_1 - x_2} \right) \frac{1}{y_1 + y_2}, \quad \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2} = \left(\frac{x_1 f(x_2) - x_2 f(x_1)}{x_1 - x_2} + y_1 y_2 \right) \frac{1}{y_1 + y_2}.$$

Hence (2. 16) extends to $T_0 = \mathbf{U} \cap ((x_1 \neq x_2) \cup (y_1 \neq -y_2))$, which is the complement of D in $\mathbf{U}$.

Multiplying (2. 16) by $(x_1 - x_2)^3$ shows that the morphism extends to

$$T_1 = \mathbf{U} \cap (y_2 \psi(x_1, x_2) \neq y_1 \psi(x_2, x_1)),$$

and that $T_1 \cap D$ gets mapped to $O = (0, 0, 0, 0, 1, 0, 0, 0, 0)$. Let

$$g(x_1, x_2) = \frac{y_2^2 \psi(x_1, x_2)^2 - y_1^2 \psi(x_2, x_1)^2}{(x_1 - x_2)^3}.$$

It can be verified that $g(x_1, x_2)$ is a polynomial in x_1 and x_2. Then multiplying (2. 16) by $y_2 \psi(x_1, x_2) + y_1 \psi(x_2, x_1)$ shows that the morphism extends to

$$T_2 = \mathbf{U} \cap (g(x_1, x_2) \neq 0),$$

and that $T_2 \cap D$ gets mapped to O. We now want to show that $\mathbf{U} = T_0 \cup T_1 \cup T_2$. Note that if $x_1 = x_2$, $y_1 = -y_2$, then $y_2 \phi(x_1, x_2) - y_1 \phi(x_2, x_1) = 8 y_2^3$, so we need only check that $x_1 = x_2$, $y_1 = y_2 = 0$ implies that $g(x_1, x_2) \neq 0$. Assume on the contrary that $f(x)$ and $g(x, x)$ have a common zero x_0. A linear substitution for x in $y^2 = f(x)$ just induces a linear transformation of the coordinate functions on Y in (2. 16), so we can assume that $x_0 = 0$. In that case $b_5 = 0$, $b_4 \neq 0$, and $g(0, 0) = -b_4^3$. Therefore $\mathbf{U} = T_0 \cap T_1 \cap T_2$.

In terms of the coordinate functions on $\mathbf{V}$, (2. 16) can be written as:

$$(2.\ 17) \qquad (X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X)$$

$$= \Bigg(1, \frac{(t_1+t_2) + 2b_1 t_1 t_2 + b_2(t_1+t_2) t_1 t_2 + 2b_3 (t_1 t_2)^2 + b_4 (t_1+t_2)(t_1 t_2)^2 + 2b_5 (t_1 t_2)^3 - 2 s_1 s_2}{t_1 t_2 (t_1 - t_2)^2},$$

$$-\frac{1}{t_1 t_2}, \frac{t_1+t_2}{t_1 t_2}, \frac{s_2 t_1 \chi(t_1, t_2) - s_1 t_2 \chi(t_2, t_1)}{(t_1 t_2)^2 (t_2 - t_1)^3}, \frac{s_2 t_1^5 - s_1 t_2^5}{(t_1 t_2)^2 (t_2 - t_1)}, \frac{s_1 t_2^4 - s_2 t_1^4}{(t_1 t_2)^2 (t_2 - t_1)}, \frac{s_2 t_1^3 - s_1 t_2^3}{(t_1 t_2)^2 (t_2 - t_1)},$$

$$\frac{2(t_1 t_2) + b_1 (t_1+t_2)(t_1 t_2) + 2b_2 (t_1 t_2)^2 + b_3 (t_1+t_2)(t_1 t_2)^2 + 2b_4 (t_1 t_2)^3 + b_5 (t_1+t_2)(t_1 t_2)^3 - s_1 s_2 (t_1+t_2)}{(t_1 t_2)^2 (t_1 - t_2)^2}\Bigg),$$

where $\chi(t_1, t_2) = t_1^4 t_2^2 \psi\left(\frac{1}{t_1}, \frac{1}{t_2}\right)$ is regular on $\mathbf{V}$.

The map (2. 17) is already defined on the overlap $\mathbf{V} \cap \mathbf{U} = \mathbf{V} \cap (t_1 t_2 \neq 0)$. Multiplying (2. 17) by $t_1 t_2 (s_2 t_1 \chi(t_1, t_2) + s_1 t_2 \chi(t_2, t_1))$ clears all denominators (since t_i divides s_i^2; $i = 1, 2$), and the resulting simplified expression for X_{111} is a polynomial in t_1 and t_2 which is congruent to $1 \bmod (t_1 t_2)$. Hence (2. 17) extends to all of $\mathbf{V}$, and $\mathbf{V} \cap D$ maps to O.

We have constructed a morphism $\phi : \mathscr{C}^{(2)} \to Y$ which collapses D to O. To show ϕ is surjective, we will construct maps

$$\lambda : Y \cap (X_0 \neq 0) \to \mathbf{U},$$

$$\mu : Y \cap (X_0 = 0) \cap (X_{111} \neq 0) \to \mathbf{V},$$

such that $\phi\lambda$ and $\phi\mu$ are the identity. The equations $X_0 = X_{111} = 0$ define the points $(0, 0, 0, 0, 0, 0, 0, 1, \pm\sqrt{b_5})$ on Y, which are the image under ϕ of

$$(q_1 = -1,\ r_1 = \pm\sqrt{b_5};\ q_2 = r_2 = 0) \text{ on } \mathbf{W}.$$

To construct λ, we take $X_0 = 1$, and let x_1 and x_2 be the roots of

$$\Xi^2 - X_{22}\Xi - X_{12} = 0,$$

and then set $y_i = x_i X_{222} + X_{122}$ for $i = 1, 2$. Then all symmetric polynomials in x_i, y_i are polynomials in X_{12}, X_{22}, X_{122}, and X_{222}, so we get a morphism. Lifting to characteristic zero shows that $\phi\lambda$ is the identity.

When $X_0 = 0$ and $X_{111} \neq 0$, we define μ by setting $t_1 = 1/X_{111}$, $s_1 = X/X_{111}$, $t_2 = s_2 = 0$. It is straightforward to verify that $\phi\mu$ is the identity.

Proof of Theorem 2. 13.

Case I: $X_0 \neq 0$. It is straightforward to verify that $f_8 - f_{14}$ are in the ideal of $F[X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X]$ generated by $f_2 - f_7$. Note that f_2, f_3, and f_4 can be used to eliminate X, X_{112}, and X_{111} from $f_5 - f_7$, giving us an isomorphic variety in $\mathbb{A}^5$ defined by:

$$j_1 = X_{122}^2 - X_{12}^2 X_{22} + X_{11} X_{12} - b_1 X_{12}^2 - b_5,$$

$$j_2 = X_{222}^2 - X_{22}^3 - X_{12} X_{22} - b_1 X_{22}^2 - b_2 X_{22} - X_{11} - b_3, \quad \text{and}$$

$$j_3 = 2 X_{122} X_{222} - 2 X_{22}^2 X_{12} + X_{11} X_{22} - X_{12}^2 - 2 b_1 X_{22} X_{12} - b_2 X_{12} - b_4.$$

The Jacobian matrix M of j_1, j_2, and j_3, with successive columns corresponding to derivatives with respect to $X_{11}, X_{12}, X_{22}, X_{122}$, and X_{222}, is given by:

$$M = \begin{bmatrix} X_{12} & -2b_1 X_{12} - 2X_{12} X_{22} + X_{11} & -X_{12}^2 & 2X_{122} & 0 \\ -1 & -X_{22} & -b_2 - 2b_1 X_{22} - X_{12} - 3X_{22}^2 & 0 & 2X_{222} \\ X_{22} & -b_2 - 2b_1 X_{22} - 2X_{12} - 2X_{22}^2 & -2b_1 X_{12} + X_{11} - 4X_{12} X_{22} & 2X_{222} & 2X_{122} \end{bmatrix}.$$

We want to show that M has rank 3. If it does not, then the determinant of each 3×3 minor M_{ijk} consisting of columns i, j, and k is zero, and so in particular:

$$(2.\,18) \qquad |M_{145}| = 4 X_{22} X_{122} X_{222} - 4 X_{12} X_{222}^2 + 4 X_{122}^2 = 0.$$

Define x_1, x_2 so that $Z = x_1$, $Z = x_2$ are the roots of

$$Z^2 - X_{22} Z - X_{12} = 0.$$

Then $X_{22} = x_1 + x_2$, $X_{12} = -x_1 x_2$, and (2. 18) implies

$$(2.\,19) \qquad (X_{122} + x_1 X_{222})(X_{122} + x_2 X_{222}) = 0.$$

We can quickly rule out the possibility that $x_1 = x_2$. For then $X_{22} = 2x_1$, $X_{12} = -x_1^2$, and (2. 19) implies $X_{122} = -x_1 X_{222}$. Hence from j_1, j_2 and j_3,

$$0 = x_1^2 X_{222}^2 + 2 x_1 X_{122} X_{222} + X_{122}^2 = f(x_1),$$

and

$$0 = X_{122} X_{222} + x_1 X_{222}^2 = \frac{1}{2}(f'(x_1)),$$

which violates the assumption that $\mathscr{C}$ is non-singular.

So let us now assume that $x_1 \neq x_2$. For $i=1, 2$ we define

$$y_i = x_i X_{222} + X_{122},$$

which gives us

$$X_{222} = \frac{y_1 - y_2}{x_1 - x_2} \quad \text{and} \quad X_{122} = -\frac{x_2 y_1 - x_1 y_2}{x_1 - x_2}.$$

Using these values and j_1, j_2 and j_3 we get

$$\begin{aligned} f(x_i) &= x_i^2 X_{222}^2 + 2 x_i X_{222} X_{122} + X_{122}^2 \\ &= y_i^2 \quad (i=1, 2). \end{aligned}$$

Also (2. 19) now reads

$$y_1 y_2 = 0. \tag{2. 20}$$

From j_2 we can solve

$$X_{11} = \frac{(x_1+x_2) x_1^2 x_2^2 + 2 b_1 x_1^2 x_2^2 + b_2 (x_1+x_2) x_1 x_2 + 2 b_3 x_1 x_2 + b_4 (x_1+x_2) + 2 b_5 - 2 y_1 y_2}{(x_1 - x_2)^2}$$

and so $|M_{124}| = 0$ can be rewritten as:

$$0 = \frac{2 y_2 (f'(x_1)(x_2 - x_1) + 4 f(x_1)) - 2 y_1 (f'(x_2)(x_1 - x_2) + 4 f(x_2))}{(x_2 - x_1)^3}. \tag{2. 21}$$

From (2. 20), $y_1 y_2 = 0$, so without loss of generality, say $y_1 = 0$. Then $f(x_1) = 0$, and (2. 21) implies $y_2 f'(x_1) = 0$. But $f'(x_1) = 0$ violates the non-singularity of $\mathscr{C}$, so we conclude $y_1 = y_2 = 0$.

Finally we can rewrite $|M_{123}| = 0$ as

$$0 = \frac{(2 y_1 y_2 + (x_1 - x_2) f'(x_1) - 2 f(x_1))(2 y_1 y_2 + (x_2 - x_1) f'(x_2) - 2 f(x_2))}{(x_1 - x_2)^4},$$

so $y_1 = y_2 = 0$ implies that $f'(x_1) = 0$ or $f'(x_2) = 0$, either of which violates the non-singularity of $\mathscr{C}$. So M has rank 3, as desired.

Case II: $X_0 = 0$. When $X_0 = 0$, $f_6^h = 0$ implies $X_{22} = 0$, $f_8^h = 0$ implies $X_{11} = 0$, and therefore $f_2^h = 0$ implies $X_{12} = 0$. Hence the Jacobian matrix N of $\{f_i^h \mid 2 \leqq i \leqq 14\}$, with successive columns denoting derivatives with respect to X_{11}, X_{12}, X_{22}, X, X_{111}, X_{112}, X_{122}, X_{222}, and X_0, is given by:

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2X \\
0 & -X_{222} & X_{122} & 0 & 0 & 0 & 0 & 0 & X_{112} \\
X_{222} & X_{122} & -2X_{112} & 0 & 0 & 0 & 0 & 0 & \begin{pmatrix} X_{111} \\ +b_2X_{122} \\ -2b_1X_{112} \end{pmatrix} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X_{122}^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X_{222}^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X_{122}X_{222} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X_{111}^2 \\
-b_1X & b_2X & -b_3X & -2X & \begin{pmatrix} -X_{112} \\ +b_1X_{122} \\ \end{pmatrix} & \begin{pmatrix} -X_{111} \\ -b_2X_{122} \\ +b_3X_{222} \end{pmatrix} & \begin{pmatrix} b_1X_{111} \\ -b_2X_{112} \\ -b_4X_{222} \end{pmatrix} & \begin{pmatrix} 2b_5X_{222} \\ -b_4X_{122} \\ +b_3X_{112} \end{pmatrix} & -2(b_4+b_1b_3)X \\
X & 0 & 0 & 0 & -X_{122} & 2X_{112} & -X_{111} & 0 & 2b_3X \\
0 & -2X & 0 & 0 & X_{222} & -X_{122} & -X_{112} & X_{111} & -5b_2X \\
0 & 0 & X & 0 & 0 & -X_{222} & 2X_{122} & -X_{112} & 2b_1X \\
-X_{112} & X_{111} & 0 & 0 & 0 & 0 & 0 & 0 & \begin{pmatrix} 2b_5X_{222} \\ -b_4X_{122} \end{pmatrix} \\
2X_{122} & -X_{112} & -X_{111} & 0 & 0 & 0 & 0 & 0 & \begin{pmatrix} -b_2X_{112} \\ +2b_3X_{122} \\ -b_4X_{222} \end{pmatrix}
\end{bmatrix}$$

Our goal is to show that N has rank 6. We let N_{ij} denote its entry in the i^{th}-row and j^{th}-column.

It follows from (2. 12) that if $X_{222}=0$, then $X_{122}=X_{112}=X=0$ also, so $X_{111}\neq 0$. Therefore N_{59} and N_{79} are never both zero, and the submatrix

$$[N_{ij}]_{(i=2,3,12,13)(j=1,2,3)}$$

always has rank $\geqq 2$. So it suffices to show that the submatrix $[N_{ij}]_{(8\leqq i\leqq 11)(4\leqq j\leqq 8)}$ always has rank $\geqq 3$. But as in the proof of 2. 11, this submatrix is just the Jacobian matrix of the embedding of $\mathscr{C}$ into $\mathbb{P}^4$ determined by the complete linear system $|6\infty|$, which is non-singular in characteristic $\neq 2$.

3. The group law

Let $\mathscr{C}$ be defined over $\mathbb{C}$. The "group law" on its Jacobian J is the morphism

$$s: J\times J \longrightarrow J,$$

defined by

$$s(u,v)=u+v.$$

Recall that $U=J-\Theta$. It follows readily from the results in the previous section that $K(J)=K(U)=\mathbb{C}(\wp_{11},\wp_{12},\wp_{22},\wp_{111})$, so s is determined by $\varphi(s(u,v))$ for

$$\varphi=\wp_{11},\wp_{12},\wp_{22},\wp_{111},$$

and $u, v, u+v\in U$.

It follows immediately from 1. 1 and (1. 2) that

$$q(u,v)=-c^2\,\frac{\sigma(u+v)\,\sigma(u-v)}{\sigma^2(u)\,\sigma^2(v)} \tag{3. 1}$$

is a function on $J\times J$. The heart of the group law is the classical formula [1], p. 100:

$$q(u,v)=\wp_{11}(u)-\wp_{11}(v)+\wp_{12}(u)\,\wp_{22}(v)-\wp_{12}(v)\,\wp_{22}(u). \tag{3. 2}$$

Theorem 3. 3 (Group law). 1) *For $i, j=1,2$; $u, v, u+v\in U$,*

$$\wp_{ij}(u+v)=-\wp_{ij}(u)-\wp_{ij}(v)+\frac{1}{4}\left(\frac{q_i(u,v)}{q(u,v)}\right)\left(\frac{q_j(u,v)}{q(u,v)}\right)-\frac{1}{4}\,\frac{q_{ij}(u,v)}{q(u,v)}$$

where

$$\begin{aligned} q_1(u,v) = {} & \mathfrak{p}_{111}(u) - \mathfrak{p}_{111}(v) + \mathfrak{p}_{112}(u)\,\mathfrak{p}_{22}(v) - \mathfrak{p}_{112}(v)\,\mathfrak{p}_{22}(u) \\ & + \mathfrak{p}_{122}(v)\,\mathfrak{p}_{12}(u) - \mathfrak{p}_{122}(u)\,\mathfrak{p}_{12}(v), \end{aligned}$$

$$\begin{aligned} q_2(u,v) = {} & \mathfrak{p}_{112}(u) - \mathfrak{p}_{112}(v) + \mathfrak{p}_{122}(u)\,\mathfrak{p}_{22}(v) - \mathfrak{p}_{122}(v)\,\mathfrak{p}_{22}(u) \\ & + \mathfrak{p}_{222}(v)\,\mathfrak{p}_{12}(u) - \mathfrak{p}_{222}(u)\,\mathfrak{p}_{12}(v), \end{aligned}$$

$$\begin{aligned} q_{11}(u,v) = {} & 4b_3\,q(u,v) + 4b_4(\mathfrak{p}_{12}(u) - \mathfrak{p}_{12}(v)) + 4(\mathfrak{p}(u)\,\mathfrak{p}_{12}(v) - \mathfrak{p}(v)\,\mathfrak{p}_{12}(u)) \\ & - 8b_5(\mathfrak{p}_{22}(u) - \mathfrak{p}_{22}(v)) + 2(\mathfrak{p}_{112}(u)\,\mathfrak{p}_{122}(v) - \mathfrak{p}_{112}(v)\,\mathfrak{p}_{122}(u)), \end{aligned}$$

$$\begin{aligned} q_{12}(u,v) = {} & 4b_3(\mathfrak{p}_{12}(u) - \mathfrak{p}_{12}(v)) + 2b_2(\mathfrak{p}_{12}(u)\,\mathfrak{p}_{22}(v) - \mathfrak{p}_{12}(v)\,\mathfrak{p}_{22}(u)) \\ & - 4(\mathfrak{p}_{11}(u)\,\mathfrak{p}_{12}(v) - \mathfrak{p}_{11}(v)\,\mathfrak{p}_{12}(u)) + 2(\mathfrak{p}(u)\,\mathfrak{p}_{22}(v) - \mathfrak{p}(v)\,\mathfrak{p}_{22}(u)) \\ & - 2b_4(\mathfrak{p}_{22}(u) - \mathfrak{p}_{22}(v)) + \mathfrak{p}_{222}(v)\,\mathfrak{p}_{112}(u) - \mathfrak{p}_{222}(u)\,\mathfrak{p}_{112}(v), \end{aligned}$$

$$\begin{aligned} q_{22}(u,v) = {} & 8b_1(\mathfrak{p}_{12}(u)\,\mathfrak{p}_{22}(v) - \mathfrak{p}_{12}(v)\,\mathfrak{p}_{22}(u)) + 4b_2(\mathfrak{p}_{12}(u) - \mathfrak{p}_{12}(v)) \\ & - 4(\mathfrak{p}(u) - \mathfrak{p}(v)) - 8(\mathfrak{p}_{11}(u)\,\mathfrak{p}_{22}(v) - \mathfrak{p}_{11}(v)\,\mathfrak{p}_{22}(u)) \\ & + 2(\mathfrak{p}_{122}(u)\,\mathfrak{p}_{222}(v) - \mathfrak{p}_{122}(v)\,\mathfrak{p}_{222}(u)). \end{aligned}$$

2) $$\begin{aligned} \mathfrak{p}_{111}(u+v) = {} & -\frac{1}{2}\,\mathfrak{p}_{111}(u) - \frac{1}{2}\,\mathfrak{p}_{111}(v) + \frac{3}{8}\,\frac{q_1(u,v)\,q_{11}(u,v)}{q(u,v)^2} - \frac{1}{8}\,\frac{q_{111}(u,v)}{q(u,v)} \\ & - \frac{1}{4}\left(\frac{q_1(u,v)}{q(u,v)}\right)^3 + \frac{3}{2}\,(\mathfrak{p}_{11}(u) + \mathfrak{p}_{11}(v))\,\frac{q_1(u,v)}{q(u,v)}, \end{aligned}$$

where

$$\begin{aligned} q_{111}(u,v) = {} & 4b_3\,q_1(u,v) + 4(\mathfrak{p}_{111}(u)\,\mathfrak{p}_{22}(u)\,\mathfrak{p}_{12}(v) - \mathfrak{p}_{111}(v)\,\mathfrak{p}_{22}(v)\,\mathfrak{p}_{12}(u)) \\ & + \mathfrak{p}_{122}(v)\,(2\mathfrak{p}_{12}(u)\,(6\mathfrak{p}_{11}(u) - 2\mathfrak{p}_{11}(v) + 4b_3) - 4b_4\,\mathfrak{p}_{22}(u)) \\ & - \mathfrak{p}_{122}(u)\,(2\mathfrak{p}_{12}(v)\,(6\mathfrak{p}_{11}(v) - 2\mathfrak{p}_{11}(u) + 4b_3) - 4b_4\,\mathfrak{p}_{22}(v)) \\ & + \mathfrak{p}_{112}(u)\,(\mathfrak{p}_{12}(v)\,(12\mathfrak{p}_{12}(v) - 8\mathfrak{p}_{12}(u) + 4b_2) + 4b_4) \\ & - \mathfrak{p}_{112}(v)\,(\mathfrak{p}_{12}(u)\,(12\mathfrak{p}_{12}(u) - 8\mathfrak{p}_{12}(v) + 4b_2) + 4b_4). \end{aligned}$$

Proof. Let $D_i = \dfrac{\partial}{\partial u_i} + \dfrac{\partial}{\partial v_i}$, $i = 1, 2$. Applying $D_i D_j$ to the logarithm of (3. 1) yields:

$$\frac{D_i D_j\,q(u,v)}{q(u,v)} - \left(\frac{D_i\,q(u,v)}{q(u,v)}\right)\left(\frac{D_j\,q(u,v)}{q(u,v)}\right) = -4\,\mathfrak{p}_{ij}(u+v) + 2\,\mathfrak{p}_{ij}(u) + 2\,\mathfrak{p}_{ij}(v).$$

So defining

$$q_i(u, v) = D_i\, q(u, v),$$
$$q_{ij}(u, v) = D_i D_j\, q(u, v) - 6(\mathfrak{p}_{ij}(u) + \mathfrak{p}_{ij}(v))\, q(u, v),$$

and

$$q_{111}(u, v) = D_1\, q_{11}(u, v),$$

reduces the theorem to the evaluation of the $q_{ij}(u, v)$ and $q_{111}(u, v)$. By differentiating f_5, f_6, and f_8, we can easily derive the following equations (see also [1], p. 48):

$$(3.4)\qquad \begin{aligned} \mathfrak{p}_{1111} &= 6\mathfrak{p}_{11}^2 + 4b_3\mathfrak{p}_{11} + 4b_4\mathfrak{p}_{12} - 12b_5\mathfrak{p}_{22} - 8b_1b_5 + 2b_2b_4, \\ \mathfrak{p}_{1112} &= 6\mathfrak{p}_{11}\mathfrak{p}_{12} + 4b_3\mathfrak{p}_{12} - 2b_4\mathfrak{p}_{22} - 4b_5, \\ \mathfrak{p}_{1122} &= 6\mathfrak{p}_{11}\mathfrak{p}_{22} - 4\mathfrak{p} + 2b_2\mathfrak{p}_{12}, \\ \mathfrak{p}_{1222} &= 6\mathfrak{p}_{12}\mathfrak{p}_{22} - 2\mathfrak{p}_{11} + 4b_1\mathfrak{p}_{12}, \\ \mathfrak{p}_{2222} &= 6\mathfrak{p}_{22}^2 + 4\mathfrak{p}_{12} + 4b_1\mathfrak{p}_{22} + 2b_2. \end{aligned}$$

The evaluation of the $q_{ij}(u, v)$ follows from (3.2) after repeated application of (3.4). The formula for $\mathfrak{p}_{111}(u+v)$ is obtained by applying $\frac{1}{2}D_1$ to the formula for $\mathfrak{p}_{11}(u+v)$ and using (3.4).

Remark. A formula for $\mathfrak{p}(u+v)$ can be obtained from the above by calculating $\mathfrak{p}_{11}(u+v)\,\mathfrak{p}_{22}(u+v) - \mathfrak{p}_{12}^2(u+v)$. Formulas for $\mathfrak{p}_{ijk}(u+v)$ can be obtained by applying $\frac{1}{2}D_i$ to the formulas for $\mathfrak{p}_{jk}(u+v)$ and then using (3.4) to remove all terms of the form $\mathfrak{p}_{ijkl}$.

4. Formal groups

In this section $\mathscr{C}$ will be defined by

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5,$$

where the b_i lie in a ring R of characteristic $\neq 2$, complete under a non-archimedean valuation. Let K be the quotient field of R.

By 2.15, $f_2 - f_{14}$ are defining equations for the Jacobian J, and by the Lefschetz principle, 3.3 still gives its group law, when the following substitutions are made:

$$(4.1)\qquad \begin{aligned} \mathfrak{p}_{ij} &= X_{ij} && i, j = 1, 2, \\ \mathfrak{p}_{ijk} &= 2X_{ijk}, && i, j, k = 1, 2, \quad \text{and} \\ \mathfrak{p} &= 2X - b_2X_{12} + b_4. \end{aligned}$$

Let $\mathfrak{n}$ be the maximal ideal of $\mathcal{O}_{O,J}$, the local ring of J at the origin O. Let $\hat{\mathcal{O}}_{O,J}$ denote the completion of $\mathcal{O}_{O,J}$ in the $\mathfrak{n}$-adic topology, and let $\hat{\mathfrak{n}}$ be $\mathfrak{n}\hat{\mathcal{O}}_{O,J}$. We chose our embedding $\Phi : \mathscr{C} \mapsto J$ so that the origin on J is the image of the point at ∞ on $\mathscr{C}$. Hence $O \in \Theta$, and from 2. 14 we see that its coordinates are

$$X_0 = X_{11} = X_{12} = X_{22} = X = X_{112} = X_{122} = X_{222} = 0; \; X_{111} = 1.$$

Hence, $\dfrac{X_0}{X_{111}}, \dfrac{X_{ij}}{X_{111}}, \dfrac{X_{ijk}}{X_{111}}$ lie in $\hat{\mathfrak{n}}$, and so can be expanded as formal power series in any two local parameters of $\hat{\mathfrak{n}}$ over K. For notational convenience, we set $X_0 = 1$.

Theorem 4. 2. *The functions* $t_1 = -\dfrac{X_{11}}{X_{111}}$, $t_2 = -\dfrac{X}{X_{111}}$ *are local parameters of* $\hat{\mathfrak{n}}$. *The power series expansions for* $\dfrac{1}{X_{111}}, \dfrac{X_{ij}}{X_{111}}, \dfrac{X_{ijk}}{X_{111}}$, $i, j, k = 1, 2$, *in terms of* t_1 *and* t_2 *all have coefficients in* R.

Proof. Dividing f_8 by X_{111}^3 shows that $\dfrac{1}{X_{111}} \in \mathfrak{n}^3$. It is then clear after dividing f_6 by X_{111}^3 that $\dfrac{X_{22}}{X_{111}}$ is in $\mathfrak{n}^2$. Hence when we divide f_2 by X_{111}^2 it follows that $\dfrac{X_{12}}{X_{111}} \in \mathfrak{n}^2$. Finally, the successive division of f_{10}, f_{11} and f_9 by X_{111}^2 shows in turn that $\dfrac{X_{122}}{X_{111}}, \dfrac{X_{222}}{X_{111}}$, and $\dfrac{X_{112}}{X_{111}}$ all lie in $\mathfrak{n}^2$. So t_1 and t_2 must form a basis for $\mathfrak{n}/\mathfrak{n}^2$.

Therefore we can write:

$$\frac{1}{X_{111}} = \sum_{i,j \geqq 0} \alpha_{ij} t_1^i t_2^j,$$

$$\frac{X_{22}}{X_{111}} = \sum_{i,j \geqq 0} \beta_{ij} t_1^i t_2^j,$$

$$\frac{X_{12}}{X_{111}} = \sum_{i,j \geqq 0} \gamma_{ij} t_1^i t_2^j,$$

with $\alpha_{ij}, \beta_{ij}, \gamma_{ij} \in K$. In fact we will show that the expansions are of the form:

(4. 3)
$$\frac{1}{X_{111}} = t_1^3 \Big(-1 + \sum_{\substack{i \geqq 3 \\ i+j>3}} \alpha_{ij} t_1^{i-3} t_2^j\Big),$$

$$\frac{X_{22}}{X_{111}} = t_1 \Big(-2 t_1 t_2 + \sum_{\substack{i>1 \\ i+j>3}} \beta_{ij} t_1^{i-1} t_2^j\Big),$$

$$\frac{X_{12}}{X_{111}} = t_1 \Big(t_2^2 + \sum_{\substack{i \geqq 1 \\ i+j>3}} \gamma_{ij} t_1^{i-1} t_2^j\Big).$$

Assume inductively that α_{ij}, β_{ij}, γ_{ij} are in R, and that $\alpha_{0j}=\alpha_{1j}=\alpha_{2j}=\beta_{0j}=\gamma_{0j}=0$ for $i+j<m$. This holds for $m=1$ since expansions of functions in $\hat{\mathfrak{n}}$ in terms of generators have no constant term.

Take $m>1$. When $i+j=m$, α_{ij} is determined by equating coefficients of $t_1^i t_2^j$ when the right-hand side of f_8 divided by X_{111}^3. This gives α_{ij} as a polynomial over R in α_{kl}, β_{kl}, and γ_{kl}, with $k+l<m$. From the inductive hypothesis, this simultaneously verifies that $\alpha_{ij}=0$ unless $i\geqq 3$. It is also easy to check that $\alpha_{30}=-1$.

Once having determined α_{ij}, $i+j=m$, each β_{ij} is found by dividing f_2 by X_{111}^2 and equating coefficients of $t_1^{i+1}t_2^j$. This gives $\beta_{ij}=\alpha_{i+1,j-1}$ plus a polynomial over R in γ_{kl}, α_{kl}, with $k+l<m$, and simultaneously that $\beta_{0j}=0$. It is easy to check that $\beta_{21}=-2$.

Finally, once α_{ij}, β_{ij}, $i+j=m$, are determined, γ_{ij} is found by dividing f_1 by X_{111}^3 and equating coefficients of $t_1^{i+2}t_2^j$. This gives γ_{ij} as a polynomial over R in α_{kl} and β_{kl} with $k+l\leqq m$, and γ_{kl} with $k+l<m$. Again, it follows that $\gamma_{0j}=0$ and $\gamma_{12}=1$.

The remainder of the theorem follows by dividing f_9-f_{11} by X_{111}^2. The division yields:

(4. 4)
$$\frac{X_{112}}{X_{111}}=-t_2^2+\sum_{i+j\geqq 4}\delta_{ij}t_1^i t_2^j,$$
$$\frac{X_{122}}{X_{111}}=t_1 t_2+\sum_{i+j\geqq 4}\varepsilon_{ij}t_1^i t_2^j,$$
$$\frac{X_{222}}{X_{111}}=-t_1^2+\sum_{i+j\geqq 4}\zeta_{ij}t_1^i t_2^j,$$

where δ_{ij}, ε_{ij}, ζ_{ij} are in R by (4. 3).

Corollary 4. 5. *Let $\mathfrak{m}$ be the maximal ideal of R and J_0 the kernel of reduction of J modulo $\mathfrak{m}$. There is a bijection*

$$\phi: J_0 \longrightarrow \mathfrak{m}\times\mathfrak{m},$$

given by

$$z \xmapsto{\phi} (t_1(z), t_2(z)).$$

Proof. Since t_1 and t_2 lie in $\mathfrak{n}$, for any z in J_0, $t_1(z)$ and $t_2(z)$ are in $\mathfrak{m}$. The map is injective since t_1 and t_2 generate $\hat{\mathfrak{n}}$, and surjective since (4. 3) and (4. 4) are convergent for $t_1(z)$, $t_2(z)$ in $\mathfrak{m}$.

Theorem 4. 6. *The bijection ϕ induces a formal group structure on $\mathfrak{m}\times\mathfrak{m}$ via*

$$t_i(u+v)=F_i(t_1(u), t_2(u), t_1(v), t_2(v)),\qquad i=1, 2,$$

where the F_i are formal power series with coefficients in R.

Proof. Since an abelian variety over K is an analytic group, it follows that

$$t_1(u+v)=\frac{-X_{11}(u+v)}{X_{111}(u+v)}=t_1(u)+t_1(v)+(d^\circ \geqq 2),$$

$$t_2(u+v)=\frac{-X(u+v)}{X_{111}(u+v)}=t_2(u)+t_2(v)+(d^\circ \geqq 2)$$

are power series with coefficients in K [10]. It remains to be shown that the coefficients of the power series lie in R.

Let

$$r(u,v)=X_{11}(u)-X_{11}(v)+X_{12}(u)\,X_{22}(v)-X_{12}(v)\,X_{22}(u).$$

Then it follows from 3. 3 and (4. 1) that $X_{111}(u+v)\,r(u,v)^3$ is a polynomial in $X(u)$, $X(v)$, $X_{ij}(u)$, $X_{ij}(v)$, $X_{ijk}(u)$, and $X_{ijk}(v)$ with coefficients in R. Further, if we set

$$d(u,v)=X_{111}(u+v)\,r(u,v)^3\,(X_{111}(u)\,X_{111}(v))^{-4},$$

then by 3. 3 and 4. 2, $d(u,v)\in R[[t_1(u),t_2(u),t_1(v),t_2(v)]]$.

For $i=1,2$, let $n_i(u,v)=t_i(u+v)\,d(u,v)$. Then the group law shows that

$$n_i(u,v)\in R[[t_1(u),t_2(u),t_1(v),t_2(v)]].$$

If $|\ |_v$ is the absolute value on R, we define the content of a polynomial

$$f=\sum_{(i_1,\dots,i_n)} a_{i_i\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}\in R[x_1,\dots,x_n]$$

by

$$\operatorname{content}(f)=\sup_{(i_1,\dots,i_n)}\{|a_{i_i\cdots i_n}|_v\}.$$

The following is a version of Gauss's lemma [5], p. 55:

Lemma 4. 7. *Let R be a ring complete under a non-archimedean absolute value $|\ |_v$, and K its field of fractions. Suppose $f=gh$, with $f,g\in R[[x_1,\dots,x_m]]$, and $h\in K[[x_1,\dots,x_m]]$.*

Let $\bar g$ be the polynomial of least degree in g. Then

$$\operatorname{content}(\bar g)=1\Rightarrow h\in R[[x_1,\dots,x_n]].$$

Thus to establish Theorem 4. 6, it suffices to show that content$(\bar{d})=1$, where $\bar{d}$ is the polynomial of least degree contained in d. But if $\bar{n}_1$ is the polynomial of least degree contained in n_1, then

$$\bar{n}_1(u,v)=\bar{d}(u,v)\,(t_1(u)+t_1(v)),$$

so it is enough to show that content$(\bar{n}_1)=1$. By 3. 3 and (4. 1),

$$\begin{aligned}
&n_1(u,v)\,r(u,v)^{-1}\,X_{111}(u)\,X_{111}(v)\\
&\qquad=-X_{11}(u+v)\,r(u,v)^2\,(X_{111}(u)\,X_{111}(v))^{-3}\\
&\qquad=\left(\frac{X_{11}(u)}{X_{111}(u)}\,\frac{1}{X_{111}(v)}+\frac{X_{11}(v)}{X_{111}(v)}\,\frac{1}{X_{111}(u)}\right)\left(\frac{r(u,v)}{X_{111}(u)\,X_{111}(v)}\right)^2\\
&\qquad\quad+\left(\frac{r_{11}(u,v)}{X_{111}(u)\,X_{111}(v)}\right)\left(\frac{r(u,v)}{X_{111}(u)\,X_{111}(v)}\right)\frac{1}{X_{111}(u)\,X_{111}(v)}\\
&\qquad\quad-\left(\frac{r_1(u,v)}{X_{111}(u)\,X_{111}(v)}\right)^2\frac{1}{X_{111}(u)\,X_{111}(v)},
\end{aligned}$$

where

$$\begin{aligned}
r_1(u,v)&=X_{111}(u)-X_{111}(v)+X_{112}(u)\,X_{22}(v)-X_{112}(v)\,X_{22}(u)\\
&\quad+X_{122}(v)\,X_{12}(u)-X_{122}(u)\,X_{12}(v),
\end{aligned}$$

and

$$\begin{aligned}
r_{11}(u,v)&=b_3\,r(u,v)+2(X(u)\,X_{12}(v)-X(v)\,X_{12}(u))-2b_5(X_{22}(u)-X_{22}(v))\\
&\quad+2(X_{112}(u)\,X_{122}(v)-X_{112}(v)\,X_{122}(u)).
\end{aligned}$$

The lead terms follow from (4. 3) and (4. 4):

$$\frac{r(u,v)}{X_{111}(u)\,X_{111}(v)}=t_1(u)\,t_1(v)\,(t_1^2(v)-t_1^2(u))+(d^\circ\geqq 5),$$

$$\frac{r_1(u,v)}{X_{111}(u)\,X_{111}(v)}=(t_1^3(u)-t_1^3(v))+(d^\circ\geqq 4),$$

$$\frac{r_{11}(u,v)}{X_{111}(u)\,X_{111}(v)}=(d^\circ\geqq 4).$$

Hence,

$$\begin{aligned}
&n_1(u,v)\,r(u,v)^{-1}\,X_{111}(u)\,X_{111}(v)\\
&\qquad=(t_1(u)\,t_1^3(v)+t_1(v)\,t_1^3(u))\,(t_1(u)\,t_1(v)\,(t_1^2(v)-t_1^2(u)))^2\\
&\qquad\quad-(t_1^3(u)-t_1^3(v))^2\,t_1^3(u)\,t_1^3(v)+(d^\circ\geqq 14)\\
&\qquad=-t_1^5(u)\,t_1^5(v)\,(t_1(u)-t_1(v))^2+(d^\circ\geqq 14).
\end{aligned}$$

So,

$$\bar{n}_1(u, v) = t_1^6(u)\, t_1^6(v)\, (t_1(u) - t_1(v))^3\, (t_1(u) + t_1(v)),$$

and $\operatorname{content}(\bar{n}_1) = 1$.

References

[1] *H. F. Baker*, An Introduction to the Theory of Multiply Periodic Functions, Cambridge 1907.

[2] *J. W. S. Cassels*, The Mordell-Weil group of curves of genus 2, in Arithmetic and Geometry, Prog. in Math. **35**, Boston 1983.

[3] *E. V. Flynn*, The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field, Proc. Camb. Phil. Soc., to appear.

[4] *D. Grant*, On a generalization of Jacobi's derivative formula to dimension two, J. reine angew. Math. **392** (1988), 125—136.

[5] *S. Lang*, Diophantine Geometry, New York 1983.

[6] *S. Lang*, Introduction to Algebraic and Abelian Functions, 2nd ed., Grad. Texts in Math. **89**, New York 1982.

[7] *D. Mumford*, On the equations defining abelian varieties I., Invent. Math. **1** (1966), 287—354.

[8] *D. Mumford*, Curves and Their Jacobians, Ann Arbor 1976.

[9] *D. Mumford*, Tata Lectures on Theta, I, II, Prog. in Math. **28, 43**, Boston 1983, 1984.

[10] *J.-P. Serre*, Lie Algebras and Lie Groups, Reading 1965.

Department of Mathematics, University of Colorado at Boulder, Campus Box 426, Boulder, Colorado 80309, USA

Eingegangen 18. April 1988, in revidierter Fassung 11. Dezember 1989