The group law on the Jacobian of a curve of genus 2

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

Abstract

An explicit description is given of the group law on the Jacobian of a curve $\mathcal{C}$ of genus 2. The Kummer surface provides a useful intermediary stage; bilinear forms relating to the Kummer surface imply that the global group law may be given projectively by biquadratic forms defined over the same ring as the coefficients of $\mathcal{C}$. It is not assumed that $\mathcal{C}$ has a rational Weierstrass point, and the theory presented applies over an arbitrary ground field.

§0. Introduction

In [8] an explicit embedding in $\mathbf{P}^{15}$ is described of the Jacobian of a curve of genus 2 over an arbitrary ground field. The defining equations are 72 quadratic forms defined over the ground field ([8], Appendix A). It is the main aim of this paper to describe the biquadratic equations which define the group law on the Jacobian. Although these equations are too large to be written down, we shall give explicit bilinear forms (in Appendix B) relating to the Kummer surface from which the required biquadratic forms may be derived for any given specialisation. These forms, together with the defining equations of [8] will complete the explicit description of the Jacobian of a general curve of genus 2 as an Abelian variety. Considerable care will be taken to ensure that all maps and equations are defined over the ground field, and $\mathcal{C}$ will have the general sextic (rather than quintic) form. This has the drawback of increasing the sheer size of the algebra; however, in compensation, the results will have both a more general applicability and a more pleasing symmetry of structure. An example of this additional symmetry is given by the transformation $\breve{}$ in equation (12) of Section 3, which does not exist in the quintic situation (where the Weierstrass point at infinity is given an artificial special status). Before describing our forms, we shall first provide some motivation for our generalisations and give a few examples by way of illustration.

* The author thanks SERC for financial support.

A general curve of genus 2 can be written in the form: $Y^2 = \textit{sextic in } X$, and such a curve is reducible to the form $Y^2 = \textit{quintic in } X$ if and only if the original sextic has a rational root. In the general sextic case, a $\mathbf{P}^{15}$ embedding of the Jacobian variety is required, whereas in the quintic case, one can use a $\mathbf{P}^8$ embedding [9]. Our reasons for developing an explicit $\mathbf{P}^{15}$ theory fall into two categories: first, most of the examples likely to arise in the near future will not have a rational Weierstrass point (and so will require the $\mathbf{P}^{15}$ development); second, the $\mathbf{P}^{15}$ development gives rise to structures which are more natural in appearance (regardless of whether the curve is in quintic or sextic form), and which will provide a better base for the further development of an explicit theory in genus 2 (and higher).

Bost and Mestre in [2] have recently publicised curves of the form: $Y^2 = g(X)h(X)i(X)$, where $g(X)$, $h(X)$, $i(X)$ are quadratics. It is almost certain that most arithmetic progress in the near future will be on curves such as:

$$\mathcal{C} : Y^2 = (X^2 + 1)(2X^2 + 1)(X^2 + X + 1) \qquad (*)$$

where $g(X)$, $h(X)$, $i(X)$ are defined over $\mathbb{Q}$. Such a curve is only reducible (over $\mathbb{Q}$) to quintic form if one of the quadratic factors splits onto two linear factors (for example, $(*)$ is not reducible to quintic form). A curve such as $(*)$ is of particular interest since its Jacobian is isogenous to that of a related curve of the same form. For example, $(*)$ has Jacobian isogenous to that of: $\hat{\mathcal{C}} : Y^2 = -2X(X-1)(2X^2+2X-1)$. It is a highly unusual curve $\mathcal{C}$ for which both $\mathcal{C}$ and $\hat{\mathcal{C}}$ have a rational Weierstrass point, and so at least one of $\mathcal{C}$ or $\hat{\mathcal{C}}$ (and usually both) will be intractably in sextic form. We do not develop isogenies here (see [2] for a geometric development), but it is clear that a theory of the Jacobian which can handle the sextic situation is a prerequisite for their further arithmetic investigation.

The $\mathbf{P}^8$ and $\mathbf{P}^{15}$ embeddings of the Jacobian for genus 2 are somewhat analogous to, respectively, the embeddings: $(1, X, Y)$ in $\mathbf{P}^2$ and $(1, X, Y, X^2)$ in $\mathbf{P}^3$ of an elliptic curve. We observe that, for the $(1, X, Y, X^2)$ embedding, addition by a point of order 2 is a linear map, the group law is a biquadratic map, and its restriction to the projective x-coordinate of the image is a bilinear map. None of these are true for the $(1, X, Y)$ embedding. In genus 2, precisely the same types of maps occur in the $\mathbf{P}^{15}$ development (and do not in the $\mathbf{P}^8$ situation), and it is the main purpose of this article to describe them explicitly. The

more systematic and elegant theory which arises on $\mathbf{P}^{15}$ is also more likely to generalise in the future to higher genus, since the underlying linear algebra will merely require higher dimensional matrices (as opposed to $\mathbf{P}^8$, where the linear and quadratic maps are lost). By retaining the full set of 10 even and 6 odd functions, we preserve the elegant forms of the analytic theory [11], while still taking care to retain the arithmetic information of the original curve. As evidence of the value of retaining quadratic maps, we consider addition by a typical fixed divisor such as $D_0 = \{(0,1),(0,1)\}$ on the Jacobian of the curve in $(*)$. Let D be *any* divisor on the Jacobian and let $\kappa(D) = (k_1, k_2, k_3, k_4)$ be its image on the Kummer surface (where κ is defined by equation (6) in Section 2). Let $\kappa(D + D_0) = (k_1', k_2', k_3', k_4')$. Then it is immediate from specialising the quadratic and bilinear forms of Sections 2 and 3 that:

$$max\big(|k_1'|, |k_2'|, |k_3'|, |k_4'|\big) \leqslant 186502 max\big(|k_1|, |k_2|, |k_3|, |k_4|\big)^2.$$

An inequality of this type can clearly be derived for any curve of genus 2 and any D_0, and is highly reminiscent of the height on the projective x-coordinate of an elliptic curve. We also note that the duplication law of the Kummer surface (Corollary 3.8 and Appendix C) is very similar in appearance to that of the x-coordinate of an elliptic curve.

It also seems likely that the equations in the appendices will give a more efficient method of performing the group law in genus 2. There are two main contexts in the mathematics of computation where higher dimensional group laws arise: algebraic integration [7] and the factorisation of large integers [1]. In both cases, many applications of the group law are performed for a particular curve over $\mathbb{Z}$. We observe that most of the multiplications and additions in the large forms of the appendices need only be calculated once for any given curve. There is also the advantage (over direct manipulation of divisors) that all calculations are projective, and so no time consuming divisions are required. By way of illustration, if $\mathbf{k} = (k_1, k_2, k_3, k_4)$ is a point on the Kummer surface of the curve in $(*)$, and $(\delta_1, \delta_2, \delta_3, \delta_4) = 2\mathbf{k}$, then specialising the equations of Appendix C gives:

$$\begin{aligned}\delta_1 = {} & -296k_1^4 - 272k_1^3k_2 + 128k_1^3k_3 - 68k_1^3k_4 - 536k_1^2k_2^2 - 312k_1^2k_2k_3 - 64k_1^2k_2k_4 - 864k_1^2k_3^2 - \\ & 16k_1^2k_3k_4 + 16k_1^2k_4^2 - 192k_1k_2^3 - 208k_1k_2^2k_3 - 104k_1k_2^2k_4 - 480k_1k_2k_3^2 - 112k_1k_2k_3k_4 - \\ & 80k_1k_3^3 - 152k_1k_3^2k_4 + 4k_1k_4^3 - 144k_2^4 - 208k_2^3k_3 - 16k_2^3k_4 - 800k_2^2k_3^2 - 128k_2^2k_3k_4 - \\ & 560k_2k_3^3 - 144k_2k_3^2k_4 - 8k_2k_3k_4^2 - 880k_3^4 - 288k_3^3k_4 - 24k_3^2k_4^2\end{aligned}$$

$$\begin{aligned}
\delta_2 = {} & -13k_1^4 + 60k_1^3k_2 - 38k_1^3k_3 + 12k_1^3k_4 + 12k_1^2k_2^2 + 180k_1^2k_2k_3 + 86k_1^2k_2k_4 - 357k_1^2k_3^2 - \\
& 96k_1^2k_3k_4 + 4k_1^2k_4^2 - 8k_1k_2^3 + 192k_1k_2^2k_3 + 56k_1k_2^2k_4 + 264k_1k_2k_3^2 + 166k_1k_2k_3k_4 + \\
& 32k_1k_2k_4^2 + 20k_1k_3^3 - 84k_1k_3^2k_4 - 24k_1k_3k_4^2 - 24k_2^4 + 8k_2^3k_3 + 8k_2^3k_4 + 48k_2^2k_3^2 + 80k_2^2k_3k_4 + \\
& 15k_2^2k_4^2 + 120k_2k_3^3 + 140k_2k_3^2k_4 + 40k_2k_3k_4^2 + 4k_2k_4^3 - 44k_3^4 + 24k_3^3k_4 + 8k_3^2k_4^2 \\
\delta_3 = {} & -296k_1^4 - 244k_1^3k_2 - 40k_1^3k_3 - 120k_1^3k_4 - 412k_1^2k_2^2 - 288k_1^2k_2k_3 - 72k_1^2k_2k_4 - 672k_1^2k_3^2 - \\
& 92k_1^2k_3k_4 - 12k_1^2k_4^2 - 152k_1k_2^3 - 176k_1k_2^2k_3 - 80k_1k_2^2k_4 - 312k_1k_2k_3^2 - 88k_1k_2k_3k_4 - \\
& 4k_1k_2k_4^2 + 160k_1k_3^3 - 16k_1k_3^2k_4 - 120k_2^4 - 192k_2^3k_3 - 16k_2^3k_4 - 640k_2^2k_3^2 - 104k_2^2k_3k_4 - \\
& 352k_2k_3^3 - 64k_2k_3^2k_4 - 568k_3^4 - 104k_3^3k_4 + 20k_3^2k_4^2 + 4k_3k_4^3 \\
\delta_4 = {} & 1429k_1^4 + 1232k_1^3k_2 - 56k_1^3k_3 + 528k_1^3k_4 + 2340k_1^2k_2^2 + 1632k_1^2k_2k_3 + 360k_1^2k_2k_4 + 3456k_1^2k_3^2 + \\
& 336k_1^2k_3k_4 + 34k_1^2k_4^2 + 848k_1k_2^3 + 1248k_1k_2^2k_3 + 528k_1k_2^2k_4 + 1776k_1k_2k_3^2 + 504k_1k_2k_3k_4 + \\
& 16k_1k_2k_4^2 - 272k_1k_3^3 + 384k_1k_3^2k_4 + 32k_1k_3k_4^2 + 604k_2^4 + 992k_2^3k_3 + 96k_2^3k_4 + 3384k_2^2k_3^2 + \\
& 624k_2^2k_3k_4 + 16k_2^2k_4^2 + 1952k_2k_3^3 + 432k_2k_3^2k_4 + 16k_2k_3k_4^2 + 3436k_3^4 + 1008k_3^3k_4 + 52k_3^2k_4^2 + k_4^4
\end{aligned}$$

For example, $\kappa(D_0) = (4, 0, 0, -15)$ and $2(4, 0, 0, -15) = (-6896, -448, -3776, 31969)$. We can simplify the form of the above duplication law still further by a change of basis:

$$\mathbf{k} = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 1 & 1 & 0 \\ -6 & -9 & -6 & -1 \end{pmatrix} \mathbf{s},$$

in which the above duplication law can be rearranged as $2(s_1, s_2, s_3, s_4) = (\xi_1, \xi_2, \xi_3, \xi_4)$, where:

$$\begin{aligned}
\xi_1 = {} & -112z_1^2 - 328z_1z_2 - 208z_1z_3 - 4z_1z_4 - 240z_2^2 - 312z_2z_3 - 8z_2z_4 - 96z_3^2 - 4z_3z_4 \\
\xi_2 = {} & 48z_1^2 + 136z_1z_2 + 96z_1z_3 + 96z_2^2 + 144z_2z_3 + 48z_3^2 + 4z_3z_4 \\
\xi_3 = {} & -80z_1^2 - 232z_1z_2 - 152z_1z_3 - 4z_1z_4 - 168z_2^2 - 216z_2z_3 - 4z_2z_4 - 72z_3^2 - 4z_3z_4 \\
\xi_4 = {} & 476z_1^2 + 1392z_1z_2 + 888z_1z_3 + 24z_1z_4 + 1020z_2^2 + 1296z_2z_3 + 36z_2z_4 + 420z_3^2 + 24z_3z_4 + z_4^2
\end{aligned}$$

where:

$$z_1 = 3s_2s_3 + s_1s_4,\ z_2 = s_1s_3 + s_2s_4,\ z_3 = s_1s_2 + s_3s_4,\ z_4 = s_1^2 + 3s_2^2 + 3s_3^2 + s_4^2.$$

which requires fewer multiplications and additions. A further computational motivation is that the forms of Section 3 give a more efficient method of deriving terms of the formal group, which will have significance when it comes to using local techniques on the Jacobian to solve Diophantine problems on the original curve. The structure of the article is as follows.

Section 1 summarises the definitions and main results of [8]: the defining equations of the Jacobian, a pair of local parameters and the induced formal group. Section 2 concentrates on the Kummer surface. Quite apart from the usefulness of the Kummer surface as a stepping stone towards the Jacobian, we hope that some of the structure presented will be of independent interest. The Kummer surface in $\mathbf{P}^3$ is computationally easier to deal with than the Jacobian variety, while still retaining some of the essential structures, such as the notion of addition by a point of order 2, and a multiplication-by-m map. Finally, Section 3 discusses the bilinear and biquadratic forms which define the group law on the Jacobian; a fringe benefit is a more elementary derivation of the formal group than the development in [8]. The identities of Sections 2 and 3 are difficult to derive, but are comparatively easy to verify once found. We give a detailed derivation of the most straightforward of these (addition by a point of order 2 on the Kummer surface); however, finding the bilinear forms of Section 3 required a considerable period of programming in the symbolic algebra languages Reduce and Maple, and involved the manipulation of large files (up to 4 MBytes) of algebraic expressions. Therefore, it is not possible to present the full mechanical details of their derivation, although we do give a general description of the computational methodology.

Sections 2 and 3 describe collaborative work with J.W.S. Cassels. He also found the method of deriving the even-even terms of the bilinear forms using Lemma 2.1 which corroborated the values I had already more painfully obtained (using Methods 1 and 2 of Section 3).

§1. Preliminary Definitions

In this section, we summarise the relevant definitions and results of [8]. 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

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

with $f_0,\ldots,f_6$ in K, $f_6 \neq 0$, and the discriminant $\Delta(F) \neq 0$. Note that we do not assume the existence of a rational Weierstrass point, and so much of the analytic theory [13] is not directly applicable, although it still provides useful motivation.

We let $\mathrm{Pic}^0(\mathcal{C})$ denote the Picard group of $\mathcal{C}$; that is, the group of divisors of $\mathcal{C}$ of degree 0 modulo linear equivalence [14]. It is convenient (following [6]) to represent any element of $\mathrm{Pic}^0(\mathcal{C})$ by an unordered pair of points $\{(x_1, y_1), (x_2, y_2)\}$ on $\mathcal{C}$, where we also allow $+\infty$ and $-\infty$ (the 2 branches of the singularity of $\mathcal{C}$ at infinity) to appear in the unordered pair. This representation is unique except that we must identify all pairs of the form $\{(x, y), (x, -y)\}$ to give the canonical equivalence class, which we denote by $\mathcal{O}$. Generically, three such elements will sum to $\mathcal{O}$ if there is a function of the form $Y - (\text{cubic in } X)$ which meets $\mathcal{C}$ at all 6 component points. The Mordell–Weil group, $\mathrm{Pic}^0_K(\mathcal{C})$, is the subgroup invariant under Galois action. In our representation, it consists of pairs of points which are either both defined over K, or are conjugate over K and quadratic.

As a group, $\mathrm{Pic}^0(\mathcal{C})$ may be identified with the Jacobian of $\mathcal{C}$. We may give the Jacobian the structure of a smooth projective variety of dimension 2 by a classical blowing down of $\mathcal{O}$. Let Θ^+, Θ^- be the images of $\mathcal{C}$ in the Jacobian via the embeddings $P \mapsto P - (+\infty)$, $P \mapsto P - (-\infty)$, respectively. Then, by a theorem of Lefschetz, ([12], p.105), a basis of $\mathcal{L}\big(2(\Theta^+ + \Theta^-)\big)$ gives the desired projective embedding of the Jacobian. 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 vector space of dimension $\ell\big(2(\Theta^+ + \Theta^-)\big) = 4^2 = 16$. We reproduce the following basis from [8], p.427.

Definition 1.1. Let the map $J : \mathrm{Pic}^0(\mathcal{C}) \to \mathbf{P}^{15}$ take $D = \{(x_1, y_1), (x_2, y_2)\} \in \mathrm{Pic}^0(\mathcal{C})$ 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 $\mathcal{O}$:

$$a_{15} = 1,\ a_{14} = x_1 + x_2,\ a_{13} = x_1x_2,\ a_{12} = {x_1}^2 + {x_2}^2,\ a_{11} = x_1x_2(x_1 + x_2),\ a_{10} = (x_1x_2)^2.$$

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 $(1,0,\ldots,0)$. Note that the Mordell-Weil group $\mathrm{Pic}^0_K(\mathcal{C})$ is mapped into $\mathbf{P}^{15}(K)$. The following result from [8] gives $J(\mathcal{C})$ the structure of a variety.

Theorem 1.2. *The 72 quadratic forms over $\mathbb{Z}[f_0,\ldots,f_6]$ given in Appendix A of [8] are a set of defining equations for the projective variety given by the embedding of Definition 1.1.* □

The forms of Theorem 1.2 have been chosen so as to be homogeneous with respect to the following weights on X, Y and $f_1, \ldots, f_6$.

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*:

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

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

We also introduce the notion of *localised* coordinates: $s_i = a_i/a_0$ for $i = 1, \ldots, 15$. Each s_i has induced weights: $wt_j(s_i) = wt_j(a_i) - wt_j(a_0)$ for $j = 1, 2$. Each of the quadratic forms of Theorem 1.2 may be divided by a_0^2 and expressed in terms of $s_0, \ldots, s_{15}$. A process of recursive substitution (as described in [8], p.429) then allows each s_i to be written as formal power series over $\mathbb{Z}[f_0, \ldots, f_6]$ in the pair of local parameters s_1, s_2. For example

$$s_{10} = s_1^4 - 2f_0 s_1^2 s_2^4 - 2f_4 s_1^6 + \ldots \tag{2}$$

In order to classify the various forms and power series in the coming sections without being overwhelmed by algebra, it is useful to introduce a notion of initial part.

Definition 1.4. Let $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots \in J(\mathcal{C})$ with projective coordinates $a_i, b_i, c_i, \ldots$ and local coordinates $s_i, t_i, u_i \ldots$ respectively. Let σ be a form in $a_i, b_i, c_i \ldots$ or a power series in $s_i, t_i, u_i \ldots$ defined over $\mathbb{Z}[f_0, \ldots f_6]$. Then the *initial part* of σ is σ modulo $f_0, \ldots f_6$. We say $\sigma_1 \approx \sigma_2$ if σ_1 and σ_2 have the same initial part.

For example, the defining equation $(A.27)$ in [8]:

$$a_2 a_{13} = a_5 a_7 - 2f_0 a_9 a_{15} - f_1 a_8 a_{15} \tag{3}$$

has initial part: $a_2 a_{13} - a_5 a_7$. Alternatively, we may write: $a_2 a_{13} \approx a_5 a_7$. Similarly, the local power series expansion in (2) above can be shortened to: $s_{10} \approx s_1^4$. We observe

that any power series expansion of s_i in terms of the local parameters s_1, s_2 must be uniquely determined by its initial part (since if there were two with the same initial part, their difference would give a non-trivial relationship between the local parameters). The local power series expansions of the local coordinates $s_0 \dots s_{15}$ in terms of s_1, s_2 have the following initial parts ([8], p.432).

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

Note that the notion of initial part given in Definition 1.4 relies on the curve $\mathcal{C}$ having non-specialised coefficients $f_0, \dots f_6$. However, since all of the forms and power series to be discussed will have a non-trivial initial part, we may describe an equivalent definition by first defining a variant of wt_1. Namely, let WT_1 agree with wt_1 on the $a_i, b_i, c_i, \dots$ and $s_i, t_i, u_i, \dots$, but $WT_1(f_i) = 0$. The defining equations (1.1) and the local power series are not homogeneous in WT_1, and it is equivalent to Definition 1.4 to define the initial part to be the terms of lowest WT_1. For power series entirely in terms of local parameters $(s_1, s_2, t_1, t_2, \dots)$ such as (4), this is also equivalent to 'polynomial of lowest degree in the local parameters'. The large expressions required to describe the group law in Sections 2 and 3 will, for simplicity, be abbreviated to initial parts in the main body of the text, with the complete equations given in the appendices.

We conclude the section with the result from [8] (p. 433) that the formal group induced by the local parameters s_1, s_2 is defined over the same ring as the coefficients of $\mathcal{C}$.

Theorem 1.5. *Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in J(\mathcal{C})$ be such that $\mathbf{c} = \mathbf{a} + \mathbf{b}$. Further, let $s_1 = a_1/a_0, s_2 = a_2/a_0, t_1 = b_1/b_0, t_2 = b_2/b_0, u_1 = c_1/c_0, u_2 = c_2/c_0$ (the local parameters of $\mathbf{a}, \mathbf{b}, \mathbf{c}$, respectively). Then there is a formal group law $\mathcal{F} = \begin{pmatrix} \mathcal{F}_1 \\ \mathcal{F}_2 \end{pmatrix}$ where $\mathcal{F}_1, \mathcal{F}_2$ are power series in s_1, s_2, t_1, t_2 defined over $R = \mathbb{Z}[f_0, \dots, f_6]$. If $f_0, \dots, f_6$ all lie in a (non-Archimedean) valuation ring, and $\mathbf{a}, \mathbf{b}$ both lie in the following neighbourhood of the origin:*

$$\mathcal{N} = \{\mathbf{a} \in J(\mathcal{C}) : |s_i| < 1,\ \textit{for } 1 \leqslant i \leqslant 15\} \tag{5}$$

then $\mathcal{F}_1, \mathcal{F}_2$ converge, and $u_1 = \mathcal{F}_1(s_1, s_2, t_1, t_2)$, $u_2 = \mathcal{F}_2(s_1, s_2, t_1, t_2)$ □

§2. The Kummer Surface

The 16 functions of Definition 1.1 may be divided into 10 even functions: $a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}$, and 6 odd functions: $a_1, a_2, a_6, a_7, a_8, a_9$. Note that, if $\mathbf{a} = J\big(\{(x_1, y_1), (x_2, y_2)\}\big)$, then negation: $-\mathbf{a} = J\big(\{(x_1, -y_1), (x_2, -y_2)\}\big)$, leaves the 10 even functions unchanged and negates the 6 odd functions, so that

$$-\mathbf{a} = (a_0, -a_1, -a_2, a_3, a_4, a_5, -a_6 - a_7, -a_8, -a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15})$$

Of the 10 even functions, there are 4 functions: $a_5, a_{13}, a_{14}, a_{15}$ which give a basis for $\mathcal{L}\big((\Theta^+ + \Theta^-)\big)$. These provide a basis in $\mathbf{P}^3$ for the Kummer surface. For convenience, we introduce the labelling: $k_1 = a_{15}, k_2 = a_{14}, k_3 = a_{13}, k_4 = a_5$, so that:

$$k_1 = 1, k_2 = x_1 + x_2, k_3 = x_1 x_2, k_4 = (F_0(x_1, x_2) - 2y_1 y_2)/(x_1 - x_2)^2 \tag{6}$$

where $F_0(x_1, x_2)$ is as defined in 1.1. We let $\mathcal{K}(\mathcal{C})$ represent the image of the map κ on $J(\mathcal{C})$ which takes $(a_0, \ldots, a_{15})$ to (k_1, k_2, k_3, k_4). The map κ identifies $\pm$. Points of order 2 are injected into $\mathcal{K}(\mathcal{C})$; all other points $\mathbf{k} = \kappa(\mathbf{a})$ in $\mathcal{K}(\mathcal{C})$ have precisely $\pm\mathbf{a}$ as preimages. The functions in (6) satisfy the homogeneous quartic:

$$R(k_1, k_2, k_3)k_4^2 + S(k_1, k_2, k_3)k_4 + T(k_1, k_2, k_3) = 0 \tag{7}$$

where R, S, T are forms of degree $2, 3, 4$, respectively, defined over $\mathbb{Z}[f_0, \ldots, f_6]$. These are given explicitly in Appendix A. The initial part of this equation is: $(k_2^2 - 2k_1k_3)k_4^2$. It is clearly desirable to work as much as possible on the simpler Kummer surface in $\mathbf{P}^3$ rather than the Jacobian variety in $\mathbf{P}^{15}$. Therefore we now consider what structure is preserved by the map κ into the Kummer surface.

First, if $\mathbf{a}, \mathbf{b} \in J(\mathcal{C})$ and $\mathbf{b}$ is of order 2, then $\mathbf{a} + \mathbf{b} = \mathbf{a} - \mathbf{b}$, so that $\kappa(\mathbf{a} + \mathbf{b}) = \kappa(\mathbf{a} - \mathbf{b}) = \kappa(-\mathbf{a} + \mathbf{b}) = \kappa(-\mathbf{a} - \mathbf{b})$. Therefore, in general, $\kappa(\mathbf{a} + \mathbf{b})$ depends only on $\kappa(\mathbf{a}), \kappa(\mathbf{b})$, and it is unambiguous to define $\kappa(\mathbf{a}) + \kappa(\mathbf{b}) = \kappa(\mathbf{a} + \mathbf{b})$, which constitutes 'addition by a point of order 2' on the Kummer surface. Note that, over the algebraic

closure, the divisors of order 2 are simply pairs of distinct roots of the sextic in (1); that is, $\{(x_3,0),(x_4,0)\}$. Let us assume for the moment that $\mathbf{b}$ is a rational point of order 2 on $J(\mathcal{C})$. A typical such $\mathbf{b}$ may be represented by a rational quadratic factor of the sextic in $\mathcal{C}$. We temporarily assume that our curve has the form

$$\mathcal{C}^g : Y^2 = g(X)h(X) = (g_2X^2 + g_1X + g_0)(h_4X^4 + h_3X^3 + h_2X^2 + h_1X + h_0) \qquad (8)$$

and take $\mathbf{b} = \mathbf{b}^g = J(\{(x_3,0),(x_4,0)\})$, where x_3, x_4 are the roots of the quadratic $g_2X^2 + g_1X + g_0$. Having fixed $\mathbf{b}^g$, we have an involution on the Jacobian $W^g : \mathbf{a} \to \mathbf{a} + \mathbf{b}^g$, which induces an involution on the Kummer surface:

$$W^g : \mathcal{K}(\mathcal{C}^g) \to \mathcal{K}(\mathcal{C}^g) : \mathbf{k} \mapsto \mathbf{k} + \kappa(\mathbf{b}^g). \qquad (9)$$

We wish to express W^g as a linear map. Here, the expressions are small enough that we can derive the map with the following 'pen and paper' computation.

Let $\kappa = \mathcal{K}\big(\{(x_1,y_1),(x_2,y_2)\}\big)$. To find $\mathbf{k}' = \mathbf{k} + \kappa(\mathbf{b}^g)$, we first construct the function $Y = \Upsilon(X)$, a cubic in X, which passes through $(x_1,y_1),(x_2,y_2),(x_3,0),(x_4,0)$. This is given by:

$$Y = \Upsilon(X) = g(X)L(X)$$

where $L(X) = AX + B$, with

$$A = \big(\frac{y_1}{g(x_1)} - \frac{y_2}{g(x_2)}\big)/(x_1 - x_2),\ B = \big(\frac{x_1y_2}{g(x_2)} - \frac{x_2y_1}{g(x_1)}\big)/(x_1 - x_2).$$

Substituting $Y = \Upsilon(X)$ into $\mathcal{C}^g$ gives:

$$\big(g(X)\big)^2(AX + B)^2 = g(X)h(X).$$

On dividing out by $g(X)$ and multiplying through by $g(x_1)g(x_2)(x_1 - x_2)^2$, and replacing each occurrence of y_i^2 by $g(x_i)h(x_i)$, $i = 1,2$, this can be rearranged to give:

$$\tau_1(X,x_1,x_2) - 2y_1y_2(X - x_1)(X - x_2)g(x) = 0$$

where $\tau_1(X,x_1,x_2)$ is the polynomial

$$g(X)g(x_1)h(x_2)(X - x_2)^2 - g(x_1)g(x_2)h(X)(x_1 - x_2)^2 + g(x_2)g(X)h(x_1)(X - x_1)^2.$$

We observe that τ_1 is invariant under $X \leftrightarrow x_1$ and $X \leftrightarrow x_2$, and so has $(X - x_1)$, $(X - x_2)$ as factors. We can now write:

$$\tau_1(X, x_1, x_2) = (X - x_1)(X - x_2)\tau_2(X, x_1, x_2)$$

where τ_2 is defined over $\mathbb{Z}[g_0, g_1, g_2, h_0, h_1, h_2, h_3, h_4]$, is quadratic in X and cubic in each of x_1, x_2. It follows that the roots of the quadratic

$$\tau_2(X, x_1, x_2) - 2y_1y_2g(X) = 0$$

are the x-coordinates of the divisor on $J(\mathcal{C})$ corresponding to $\mathbf{a} + \mathbf{b}^g$. The function $\tau_2(X, x_1, x_2) - 2y_1y_2g(X)$ has a zero of order 2 at $(x_1, y_1) = (x_2, y_2)$ and so the quadratic in X:

$$\big(\tau_2(X, x_1, x_2) - 2y_1y_2g(X)\big)/(x_1 - x_2)^2 = PX^2 - QX + R$$

has a pole only at $\mathcal{O}$, and is of degree one at infinity. Taking $\mathbf{k}' = (k_1', k_2', k_3', k_4') = \mathbf{k} + \kappa(\mathbf{b}^g)$, we see that $(k_1', k_2', k_3') = (P, Q, R)$ as projective triples, and that $P, Q, R \in \mathcal{L}(\Theta^+ + \Theta^-)$. Since k_1, k_2, k_3, k_4 gives a basis for $\mathcal{L}(\Theta^+ + \Theta^-)$, we can easily write (k_1', k_2', k_3') as a $\mathbb{Z}[g_0, g_1, g_2, h_0, h_1, h_2, h_3, h_4]$-linear map on $\mathbf{k}$. This map may be extended to k_4' by expressing k_4' as rational function in k_1', k_2', k_3' and rewriting this expression as a linear combination of k_1, k_2, k_3, k_4. We may summarise the above by the following Lemma.

Lemma 2.1. *Let $\mathcal{C}$ be as in* (8)*, and W^g be the 'addition by a point of order 2' involution given in* (9)*. Then there is a matrix $(W_{ij}^g) \in M_4(\mathbb{Z}[g_0, g_1, g_2, h_0, h_1, h_2, h_3, h_4])$ such that for any $\mathbf{k} = \begin{pmatrix} k1 \\ k2 \\ k3 \\ k4 \end{pmatrix} \in \mathcal{K}(\mathcal{C})$, $W^g(\mathbf{k}) = (W_{ij}^g)\mathbf{k}$.* □

The matrix (W_{ij}^g) is written out explicitly in Appendix A. We note that, since (W_{ij}^g) represents an involution in $\mathbf{P}^3$, its square gives a scalar multiple of the identity. This property can be used as an alternative means of extending the linear map from (k_1', k_2', k_3') to (k_1', k_2', k_3', k_4'). In fact, $(W_{ij}^g)^2 = R \cdot I$, where R is the resultant of $g_2X^2 + g_1X + g_0$ and $h_4X^4 + h_3X^3 + h_2X^2 + h_1X + h_0$.

A second useful piece of structure on the Kummer surface is motivated by a set of identities of theta functions given in [11]. For any $\mathbf{a} \in J(\mathcal{C})$, let $\big(k_1(\mathbf{a}), k_2(\mathbf{a}), k_3(\mathbf{a}), k_4(\mathbf{a})\big)$

represent the image $\kappa(\mathbf{a})$ on the Kummer surface. Then, the identities of [11] (p.179) imply that, for $i, j \in \{1, \ldots, 4\}$, the functions

$$k_i(\mathbf{a}+\mathbf{b})k_j(\mathbf{a}-\mathbf{b}) + k_i(\mathbf{a}-\mathbf{b})k_j(\mathbf{a}+\mathbf{b}) \tag{10}$$

are given projectively by biquadratic forms in the variables $\big(k_1(\mathbf{a}), \ldots, k_4(\mathbf{a})\big)$, $\big(k_1(\mathbf{b}), \ldots, k_4(\mathbf{b})\big)$ over the algebraic closure. We observe that in the case when $\mathcal{C}$ has the form $\mathcal{C}^g$ and $\mathbf{b} = \mathbf{b}^g$ is of order 2, then the forms in (10) are projectively equal to $2k_i\big(W^g(\mathbf{a})\big)k_j\big(W^g(\mathbf{a})\big)$. By Lemma 2.1, this is a quadratic form in $\big(k_1(\mathbf{a}), \ldots, k_4(\mathbf{a})\big)$, over the ground field of $\mathcal{C}^g$. If we formally regard the coefficient of each $k_i(\mathbf{a})k_j(\mathbf{a})$ as a quadratic form in $k_1(\mathbf{b}^g), \ldots, k_4(\mathbf{b}^g)$, we can equate coefficients and derive biquadratic forms $\psi_{ij}\big(\kappa(\mathbf{a}), \kappa(\mathbf{b})\big)$ which are projectively equal to (10) for arbitrary $\mathbf{a}, \mathbf{b} \in J(\mathcal{C})$. We can do this (infer the general form of ψ_{ij} for arbitrary $\mathbf{b}$ on a general curve $\mathcal{C}$ from the special case $\mathbf{b}^g$ on $\mathcal{C}^g$) because the 10 products $k_i(\mathbf{b}^g)k_j(\mathbf{b}^g)$ are linearly independent over $\mathbb{Q}(f_0, \ldots, f_6)$. The above discussion may be summarised by the following lemma.

Lemma 2.2. *For $\mathbf{a}, \mathbf{b} \in J(\mathcal{C})$, let $\kappa(\mathbf{a}) = \big(k_1(\mathbf{a}), \ldots, k_4(\mathbf{a})\big)$, $\kappa(\mathbf{b}) = \big(k_1(\mathbf{b}), \ldots, k_4(\mathbf{b})\big) \in \mathcal{K}(\mathcal{C})$. Then, for $i, j \in \{1, \ldots, 4\}$, there exist biquadratic forms ψ_{ij} defined over $\mathbb{Z}[f_0, \ldots, f_6]$ such that the 4×4 matrix $\Big(\psi_{ij}\big(\kappa(\mathbf{a}), \kappa(\mathbf{b})\big)\Big)$ is projectively equal to $\Big(k_i(\mathbf{a}+\mathbf{b})k_j(\mathbf{a}-\mathbf{b}) + k_i(\mathbf{a}-\mathbf{b})k_j(\mathbf{a}+\mathbf{b})\Big)$.* □

It will be seen that the forms ψ_{ij} are easily derivable from the bilinear forms of the next section, and so we have not given them explicitly.

Finally, since $(\pm m\mathbf{a}) = m(\pm\mathbf{a})$, it follows that the multiplication-by-m map may legitimately be defined on the Kummer surface by: $m\kappa(\mathbf{a}) = \kappa(m\mathbf{a})$. In particular, the duplication map may be given by quartic forms defined over $\mathbb{Z}[f_0, \ldots, f_6]$. As with the forms of Lemma 2.2, these will be explicitly derived from the bilinear forms of the next section.

§3. The Group Law

In this section we shall present a 4×4 matrix of bilinear forms on the Jacobian which will provide both a description of the group law and an explicit derivation of the forms

mentioned at the end of Section 2. We first describe an isomorphism between the Kummer surface and the 10 even coordinates of the Jacobian embedding.

Lemma 3.1. *Let* $\mathbf{a} \in J(\mathcal{C})$ *and let* $\mathcal{E}(\mathcal{C})$ *represent the image of* $J(\mathcal{C})$ *under the restriction map to the 10 even functions:*

$$(a_0, \ldots, a_{15}) \mapsto (a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}).$$

Then $\mathcal{K}(\mathcal{C}) \cong \mathcal{E}(\mathcal{C})$ *under the following isomorphism (for* $\mathbf{k} = (k_1, k_2, k_3, k_4) \in \mathcal{K}(\mathcal{C})$*):*

$$\begin{aligned}\rho : \mathcal{K}(\mathcal{C}) &\mapsto \mathcal{E}(\mathcal{C}) \\ : \mathbf{k} &\mapsto (\rho_0(\mathbf{k}), \rho_3(\mathbf{k}), \rho_4(\mathbf{k}), \rho_5(\mathbf{k}), \rho_{10}(\mathbf{k}), \rho_{11}(\mathbf{k}), \rho_{12}(\mathbf{k}), \rho_{13}(\mathbf{k}), \rho_{14}(\mathbf{k}), \rho_{15}(\mathbf{k}))\end{aligned}$$

where:

$$\rho_0(\mathbf{k}) = k_4^2,\ \rho_3(\mathbf{k}) = k_3k_4,\ \rho_4(\mathbf{k}) = \frac{1}{2}(k_2k_4 - f_1k_1^2 - f_3k_1k_3 - f_5k_3^2),\ \rho_5(\mathbf{k}) = k_1k_4$$

$\rho_{10}(\mathbf{k}) = k_3^2, \rho_{11}(\mathbf{k}) = k_2k_3, \rho_{12}(\mathbf{k}) = k_2^2 - 2k_1k_3, \rho_{13}(\mathbf{k}) = k_1k_3, \rho_{14}(\mathbf{k}) = k_1k_2, \rho_{15}(\mathbf{k}) = k_1^2.$

Further, if $\mathbf{e} = (a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15})$ *is in* $\mathcal{E}(\mathcal{C})$*, then for* $j \in \{1, \ldots, 4\}$*, the map:*

$$\theta^i : \mathcal{E}(\mathcal{C}) \mapsto \mathcal{K}(\mathcal{C}) : \mathbf{e} \mapsto \left(\theta_1^i(\mathbf{e}), \theta_2^i(\mathbf{e}), \theta_3^i(\mathbf{e}), \theta_4^i(\mathbf{e})\right)$$

gives the inverse of ρ*, where the matrix* $(\theta_j^i\big((\mathbf{e})\big)$ *is given by:*

$$\begin{pmatrix} a_{15} & a_{14} & a_{13} & a_5 \\ a_{14} & a_{12} + 2a_{13} & a_{11} & 2a_4 + f_1a_{15} + f_3a_{13} + f_5a_{10} \\ a_{13} & a_{11} & a_{10} & a_3 \\ a_5 & 2a_4 + f_1a_{15} + f_3a_{13} + f_5a_{10} & a_3 & a_0 \end{pmatrix}.$$

The linear maps on $\mathcal{E}(\mathcal{C})$ *which give the inverse of* ρ *are precisely the* $\mathbb{Z}[f_0, \ldots, f_6]$*-linear combinations of the rows* $\theta^1, \ldots, \theta^4$*.* □

We also observe that, for any pair of odd functions a_i, a_j (not necessarily distinct), there exists a defining equation on $J(\mathcal{C})$ ([8], Appendix A) of the form:

$$a_ia_j = E_{ij}(a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}). \tag{11}$$

where each E_{ij} (for $i, j \in \{1, 2, 6, 7, 8, 9\}$) is a quadratic form in the 10 even functions. Therefore, given $(a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15})$ in $\mathcal{E}(\mathcal{C})$, the square of any odd

function, a_i^2, is uniquely determined by E_{ii}, and so a_i is determined up to a choice of sign. Having fixed one of the non-zero odd functions, a_1 say, the equations E_{1j} (for $j = 2, 6, 7, 8, 9$) uniquely determine the remaining odd functions. This gives a natural route from a point $\mathbf{k} \in \mathbf{P}^3$ on the Kummer surface to its two preimages $\pm\mathbf{a} \in \mathbf{P}^{15}$ on the Jacobian variety. Namely, $\mathcal{K}(\mathcal{C}) \to \mathcal{E}(\mathcal{C})$ (by ρ), which then has two extensions to $J(\mathcal{C})$ via (11).

We shall now give the main result of the section. It will not be possible to give the details of the derivation, but we shall follow the statement by a sketch of the main computational techniques.

Theorem 3.2. *Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in J(\mathcal{C})$ be such that $\mathbf{c} = \mathbf{a} + \mathbf{b}$. Then there exists a 4×4 matrix of bilinear forms $\big(\phi_{ij}(\mathbf{a}, \mathbf{b})\big)$ defined over $\mathbb{Z}[f_0, \ldots, f_6]$ which is projectively equal to the matrix $\big(k_i(\mathbf{a} - \mathbf{b})k_j(\mathbf{a} + \mathbf{b})\big)$. For each fixed $i \in \{1, \ldots, 4\}$, we have: $\kappa(\mathbf{c}) = \big(\phi_{i1}(\mathbf{a}, \mathbf{b}), \phi_{i2}(\mathbf{a}, \mathbf{b}), \phi_{i3}(\mathbf{a}, \mathbf{b}), \phi_{i4}(\mathbf{a}, \mathbf{b})\big)$.* □

Much of the structure of the bilinear forms $\big(\phi_{ij}(\mathbf{a}, \mathbf{b})\big)$ is more clearly summarised by the behaviour of their initial parts; we list only the initial parts here, with the entire forms in a file (available by anonymous ftp) named in Appendix B.

$$\phi_{11}(\mathbf{a}, \mathbf{b}) \approx a_0 b_{15} - 2a_5 b_5 + a_{15} b_0$$

$$\phi_{12}(\mathbf{a}, \mathbf{b}) \approx a_0 b_{14} + 2a_1 b_9 - 2a_2 b_8 - 2a_4 b_5 - 2a_5 b_4 - 2a_8 b_2 + 2a_9 b_1 + a_{14} b_0$$

$$\phi_{13}(\mathbf{a}, \mathbf{b}) \approx b_{13} a_0 + a_{13} b_0 - 2a_7 b_2 - 4a_4 b_4 + a_5 b_3 + a_3 b_5 - 2b_7 a_2 + 2b_8 a_1 + 2a_8 b_1$$

$$\phi_{14}(\mathbf{a}, \mathbf{b}) \approx -2a_2 b_2 + b_0 a_5 + a_0 b_5$$

$$\phi_{21}(\mathbf{a}, \mathbf{b}) \approx a_0 b_{14} - 2a_1 b_9 + 2a_2 b_8 - 2a_4 b_5 - 2a_5 b_4 + 2a_8 b_2 - 2a_9 b_1 + a_{14} b_0$$

$$\phi_{22}(\mathbf{a}, \mathbf{b}) \approx 2b_{13} a_0 + b_0 a_{12} + a_0 b_{12} + 2a_{13} b_0 - 4a_5 b_3 - 4a_3 b_5$$

$$\phi_{23}(\mathbf{a}, \mathbf{b}) \approx -2a_3 b_4 - 2a_4 b_3 + 2a_1 b_7 - 2a_2 b_6 + a_0 b_{11} - 2a_6 b_2 + 2a_7 b_1 + a_{11} b_0$$

$$\phi_{24}(\mathbf{a}, \mathbf{b}) \approx 2b_0 a_4 + 2a_0 b_4 - 2a_1 b_2 - 2b_1 a_2$$

$$\phi_{31}(\mathbf{a}, \mathbf{b}) \approx a_{13} b_0 - 2a_8 b_1 + 2a_7 b_2 + a_5 b_3 - 4a_4 b_4 + a_3 b_5 + 2b_7 a_2 - 2b_8 a_1 + b_{13} a_0$$

$$\phi_{32}(\mathbf{a}, \mathbf{b}) \approx -2a_3 b_4 - 2a_4 b_3 - 2a_1 b_7 + 2a_2 b_6 + a_0 b_{11} + 2a_6 b_2 - 2a_7 b_1 + a_{11} b_0$$

$$\phi_{33}(\mathbf{a}, \mathbf{b}) \approx a_0 b_{10} - 2a_3 b_3 + a_{10} b_0$$

$$\phi_{34}(\mathbf{a}, \mathbf{b}) \approx a_0 b_3 - 2a_1 b_1 + b_0 a_3$$

$$\phi_{41}(\mathbf{a},\mathbf{b}) \approx b_0a_5 + 2a_2b_2 + a_0b_5$$
$$\phi_{42}(\mathbf{a},\mathbf{b}) \approx 2a_0b_4 + 2b_1a_2 + 2a_1b_2 + 2b_0a_4$$
$$\phi_{43}(\mathbf{a},\mathbf{b}) \approx a_0b_3 + 2a_1b_1 + b_0a_3$$
$$\phi_{44}(\mathbf{a},\mathbf{b}) \approx a_0b_0$$

Remark 3.3. The bilinear forms satisfy the following properties.

(i). Each $\phi_{ij}(\mathbf{a},\mathbf{b})$ is invariant under $(\mathbf{a},\mathbf{b}) \to (-\mathbf{a},-\mathbf{b})$ (since both $k_i(\mathbf{a}-\mathbf{b})$ and $k_j(\mathbf{a}+\mathbf{b})$ are invariant). Therefore, each bilinear form contains only *even·even* terms and *odd·odd* terms. That is, if the monomial a_mb_n occurs then the coordinates a_m, b_n must either be both even or both odd. Similarly, invariance under $(\mathbf{a},\mathbf{b}) \to (\mathbf{b},\mathbf{a})$ gives that the forms are symmetric $\mathbf{a}$ and $\mathbf{b}$.

(ii). At duplication (that is, $\mathbf{b}=\mathbf{a}$), each $k_i(\mathbf{a}-\mathbf{b}) = k_i(\mathcal{O}) = 0$ for $i = 1,2,3$. Therefore, the first three rows of $\big(\phi_{ij}(\mathbf{a},\mathbf{a})\big)$ are all zero. This vanishing is not a transparent cancellation of terms, but is a statement that each such entry lies in the ideal generated by the defining equations of the Jacobian variety. For example, note that the initial part of $\phi_{34}(\mathbf{a},\mathbf{a})$ above is: $2(a_0a_3 - a_1^2)$, which is twice the initial part of the defining equation $(A.1)$ in Appendix A of [8]. The fourth row is the only non-degenerate row at $\mathbf{b}=\mathbf{a}$, and so it is the only row which can be specialised to give the duplication map on the Jacobian.

(iii). At $\mathbf{b} = \mathcal{O} = (1,0,0,\ldots,0)$ all terms b_ib_j vanish except b_0^2. Therefore, we expect each row of coefficients of b_0^2 to lie in the span of the θ^i of Lemma 3.1. In fact, the bilinear forms ϕ_{ij} have been chosen so that the coefficient of b_0^2 is simply θ_j^i. By symmetry, the same comment applies with the roles of $\mathbf{a}$ and $\mathbf{b}$ swapped.

(iv). There are two transformations which permute the ϕ_{ij}. The obvious one is to negate either $\mathbf{a}$ or $\mathbf{b}$ ($\mathbf{b}$, say). This interchanges each ϕ_{ij} with ϕ_{ji} and negates the odd coordinates of $\mathbf{b}$. Therefore, any ϕ_{ji} may be derived from ϕ_{ij} by leaving the *even·even* terms unchanged and negating the *odd·odd* terms. In particular, the ϕ_{ii} along the leading diagonal have only *even·even* terms.

A more subtle transformation is on $\mathcal{C}$ itself; namely $\breve{}\ : X \mapsto 1/X, \mapsto Y/X^3$ which transforms $\mathcal{C}$ to a curve of the same form:

$$\breve{\mathcal{C}} : Y^2 = F(X) = f_0X^6 + f_1X^5 + f_2X^4 + f_3X^3 + f_4X^2 + f_5X + f_6 \qquad (12)$$

where each f_i is replaced by f_{6-i}. There is an induced biregular map from $J(\mathcal{C})$ to $J(\breve{\mathcal{C}})$: $(a_0,\ldots,a_{15}) \rightarrow (a_0,-a_2,-a_1,a_5,a_4,a_3,-a_9,-a_8,-a_7,-a_6,a_{15},a_{14},a_{12},a_{13},a_{11},a_{10})$, and from $\mathcal{K}(\mathcal{C})$ to $\mathcal{K}(\breve{\mathcal{C}})$: $(k_1,k_2,k_3,k_4) \rightarrow (k_3,k_2,k_1,k_4)$. Therefore, replacing each of $a_0,\ldots,a_{15}$ by $a_0,-a_2,-a_1,a_5,a_4,a_3,-a_9,-a_8,-a_7,-a_6,a_{15},a_{14},a_{12},a_{13},a_{11},a_{10}$, respectively, and each of f_i by f_{6-i}, induces the permutation: $\phi_{11} \leftrightarrow \phi_{33}$, $\phi_{12} \leftrightarrow \phi_{32}$, $\phi_{13} \leftrightarrow \phi_{31}$, $\phi_{14} \leftrightarrow \phi_{34}$, $\phi_{21} \leftrightarrow \phi_{23}$, $\phi_{41} \leftrightarrow \phi_{43}$, with ϕ_{22}, ϕ_{24}, ϕ_{42}, ϕ_{44} invariant.

(v). Each ϕ_{ij} is homogeneous with respect to both wt_1 and wt_2.

There follows a brief sketch of the three methods used to derive the bilinear forms.

Method 1. *Direct Algebraic Manipulation.*

We write $\mathbf{a} = J(\{(x_1,y_1),(x_2,y_2)\})$, $\mathbf{b} = J(\{(x_3,y_3),(x_4,y_4)\})$, $\mathbf{c} = J(\{(x_5,y_5),(x_6,y_6)\})$, with $\mathbf{c} = \mathbf{a}+\mathbf{b}$. One can then follow through the 'naive' technique for adding divisors modulo linear equivalence ([3],[6]). Namely, one finds the function $Y-(\alpha X^3+\beta X^2+\gamma X+\delta)$ which meets $\mathcal{C}$ at $(x_1,y_1),\ldots,(x_4,y_4)$, and expresses each of $\alpha,\beta,\gamma,\delta$ as rational functions in $x_1,y_1,\ldots,x_4,y_4$ over $\mathbb{Z}[f_0,\ldots,f_6]$. It is then possible similarly to express x_5+x_6, x_5x_6, y_5+y_6, y_5y_6 and so $k_1(\mathbf{a}+\mathbf{b}),\ldots,k_4(\mathbf{a}+\mathbf{b})$. The same procedure can be applied to $\mathbf{a}-\mathbf{b}$, and so we eventually obtain: $k_i(\mathbf{a}+\mathbf{b})k_j(\mathbf{a}-\mathbf{b})$ for each $i,j \in \{1,\ldots,4\}$ as rational functions in $x_1,y_1,\ldots,x_4,y_4$ over $\mathbb{Z}[f_0,\ldots,f_6]$. These are rather large and required 4 MBytes of storage on an IBM mainframe. These 16 expressions have unwanted common poles and zeroes (for example, at $x_2=x_3, y_2=-y_3$), and so we divide these out to obtain 16 rational functions in $x_1,\ldots,x_4,y_1,\ldots y_4$ which are projectively equal to $\big(k_i(\mathbf{a}+\mathbf{b})k_j(\mathbf{a}-\mathbf{b})\big)$, and which have poles only at: $x_1=x_2, y_1=-y_2$ and $x_3=x_4, y_3=-y_4$, and which are of degree at most 2 in each X_i $(1 \leqslant i \leqslant 4)$. Such functions lie in $\mathcal{L}\big(2(\Theta^+ + \Theta^-)\big) \otimes \mathcal{L}\big(2(\Theta^+ + \Theta^-)\big)$, and so can be represented as a linear combination of the monomials a_ib_j; that is, as a bilinear map in $\mathbf{a}$ and $\mathbf{b}$. Finding this representation is a lengthy computation which involves a careful ordering of the monomials a_ib_j and using these to reduce the current largest pole in each of the 16 rational functions. The methodology is along the lines described in [8] for finding the defining equations of Theorem 1.2, but with expressions several orders of magnitude larger. The remarks in 3.3 above can all be used as devices for reducing the amount of computation. In particular, homogeneity with respect to wt_1 and wt_2 places a severe restriction on the allowable coef-

ficients of any given monomial $a_i b_j$. In fact, for reassurance, the bilinear forms were also derived from first principles without use of these computational aids, so that the remarks in 3.3 could then be used as an independent verification.

Method 2. *Formal Power Series.*

In this method, one derives the local power series expansion of each desired form, and equates coefficients to determine each form globally. We first give a few technical definitions and lemmas.

Definition 3.4. Let $\sigma(\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots)$ be a form over $\mathbb{Z}[f_0, \ldots, f_6]$, homogeneous in each of $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots \in J(\mathcal{C})$, and let $(s_1, s_2), (t_1, t_2), (u_1, u_2), \ldots$ be the local parameters for $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$, respectively. The *localisation* of σ, denoted σ^ℓ, is the power series in $s_1, s_2, t_1, t_2, u_1, u_1, \ldots$ over $\mathbb{Z}[f_0, \ldots, f_6]$ obtained by replacing each $a_i, b_j, c_k \ldots$ with the local power series expansion for $s_i, t_j, u_k, \ldots$ in the local parameters.

Note that, if $\sigma(\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots)$ is homogeneous of degrees $l, m, n \ldots$ respectively, then $\sigma^\ell(s_1, s_2, t_1, t_2, u_1, u_2, \ldots)$ converges to $\sigma(\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots)/(a_0^l b_0^m c_0^n)$ when $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots \in \mathcal{N}$, where $\mathcal{N}$ is the neighbourhood defined in (5). If $\big(\sigma_{ij}\big)$ is a projective array of such forms, all homogenous of the same degrees in each of $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$, then $\big(\sigma_{ij}^\ell\big) = \big(\sigma_{ij}\big)$ under the same conditions. That is, $\big(\sigma_{ij}^\ell\big)$ gives the local expansion of $\big(\sigma_{ij}\big)$ in $\mathcal{N} \times \mathcal{N} \times \ldots \times \mathcal{N}$.

The usefulness of localisations as a computational tool is that there is no non-trivial relationship satisfied by the local parameters; the defining equations of the Jacobian, when localised, are transparent identities in the ring of power series. It follows that a sufficient condition for a set of forms in $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots \in J(\mathcal{C})$ to be linearly independent is that they have linearly independent local power series expansions. An application of this idea is given in the following lemma.

Lemma 3.5. *Let $\mathbf{a} \in J(\mathcal{C})$. The set of 16 functions linear in $\mathbf{a}$:*

$$S_{\mathbf{a}} = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12} - 2a_{13}, a_{13}, a_{14}, a_{15}\}$$

have localisations, $S_{\mathbf{a}}^\ell$, whose polynomials of lowest degree are linearly independent. The same applies to the localisations $T_{\mathbf{a}}^\ell$ of the following set of 64 functions quadratic in $\mathbf{a}$:

$$T_{\mathbf{a}} = \{a_0^2, a_0a_2, a_0a_1, a_0a_5, a_0a_4, a_0a_3, a_0a_9, a_0a_8, a_0a_7, a_0a_6, a_0a_{15}, a_0a_{14},$$
$$a_0a_{13}, a_0a_{11}, a_0a_{10}, a_2a_{15}, a_2a_{14}, a_2a_{13}, a_2a_{11}, a_2a_{10}, a_1a_{10}, a_5a_{15}, a_4a_{15}, a_3a_{15},$$
$$a_4a_{13}, a_3a_{13}, a_3a_{11}, a_3a_{10}, a_9a_{15}, a_8a_{15}, a_9a_{13}, a_8a_{13}, a_9a_{10}, a_8a_{10}, a_7a_{10}, a_6a_{10},$$
$$a_{15}^2, a_{14}a_{15}, a_{13}a_{15}, a_{11}a_{15}, a_{10}a_{15}, a_{10}a_{14}, a_{10}a_{13}, a_{10}a_{11}, a_{10}^2, a_{12}a_{15} - 2a_{13}a_{15},$$
$$a_{12}a_{14} - 2a_{11}a_{15},\ a_{12}a_{13} - 2a_{10}a_{15},\ a_{11}a_{12} - 2a_{10}a_{14},\ a_{10}a_{12} - 2a_{10}a_{13},$$
$$a_{12}^2 - 4a_{12}a_{13} + a_{10}a_{13},\ a_5a_{12} - 2a_3a_{15},\ a_4a_{12} - 2a_4a_{13},\ a_3a_{12} - 2a_3a_{13},$$
$$a_9a_{14} - 2a_8a_{15},\ 2a_9a_{13} - a_8a_{14},\ a_9a_{12} - a_8a_{14},\ a_9a_{11} - 2a_8a_{13},\ a_9a_{11} - a_8a_{12},$$
$$2a_9a_{10} - a_8a_{11},\ a_8a_{11} - a_7a_{12},\ 2a_8a_{10} - a_7a_{11},\ a_7a_{11} - a_6a_{12},\ 2a_7a_{10} - a_6a_{11}\}$$

A change of basis on $T_{\mathbf{a}}$ gives the set of quadratic monomials:

$$U_{\mathbf{a}} = \{a_0^2, a_0a_2, a_0a_1, a_0a_5, a_0a_4, a_0a_3, a_0a_9, a_0a_8, a_0a_7, a_0a_6, a_0a_{15}, a_0a_{14},$$
$$a_0a_{13}, a_0a_{11}, a_0a_{10}, a_2a_{15}, a_2a_{14}, a_2a_{13}, a_2a_{11}, a_2a_{10}, a_1a_{10}, a_5a_{15}, a_4a_{15}, a_3a_{15},$$
$$a_4a_{13}, a_3a_{13}, a_3a_{11}, a_3a_{10}, a_9a_{15}, a_8a_{15}, a_9a_{13}, a_8a_{13}, a_9a_{10}, a_8a_{10}, a_7a_{10}, a_6a_{10},$$
$$a_{15}^2, a_{14}a_{15}, a_{13}a_{15}, a_{11}a_{15}, a_{10}a_{15}, a_{10}a_{14}, a_{10}a_{13}, a_{10}a_{11}, a_{10}^2,$$
$$a_{12}a_{15}, a_{12}a_{14}, a_{12}a_{13}, a_{11}a_{12}, a_{10}a_{12}, a_{12}^2, a_5a_{12}, a_4a_{12}, a_3a_{12},$$
$$a_9a_{14}, a_8a_{14}, a_9a_{12}, a_9a_{11}, a_8a_{12}, a_8a_{11}, a_7a_{12}, a_7a_{11}, a_6a_{12}, a_6a_{11}\}$$

whose localisations $U_{\mathbf{a}}^{\ell}$ are linearly independent. The sets $T_{\mathbf{a}}$ and $U_{\mathbf{a}}$ each span $\mathcal{L}\big(4(\Theta^+ + \Theta^-)\big)$.

Proof. Since the 64 functions in either $T_{\mathbf{a}}$ or $U_{\mathbf{a}}$ have linearly independent localisations, it follows that they are themselves linearly independent functions on $\mathcal{C}^{(2)}$. Therefore, either set gives a basis for $\mathcal{L}\big(4(\Theta^+ + \Theta^-)\big)$, which has dimension $8^2 = 64$. Alternatively, one can write out an explicit basis for $\mathcal{L}\big(4(\Theta^+ + \Theta^-)\big)$ in terms of x_1, y_1, x_2, y_2 and verify that it is spanned by either $T_{\mathbf{a}}$ or $U_{\mathbf{a}}$. The sets $T_{\mathbf{a}}$ and $U_{\mathbf{a}}$ have been arranged so that the first 3 rows give 36 independent functions with poles at $\mathcal{O}$ ($9 - i$ functions with a pole of order i at $\mathcal{O}$, for $1 \leqslant i \leqslant 8$); the remaining rows give the 28 independent regular functions: $(x_1x_2)^i(x_1 + x_2)^j(y_1y_2)^k(y_1 + y_2)^l$, for $i + j + 3k + 3l \leqslant 4$. □

We shall only be concerned with the cases when $\sigma(\mathbf{a}, \mathbf{b})$ is a bilinear or biquadratic form. A biquadratic form in $\mathbf{a}, \mathbf{b} \in J(\mathcal{C})$ is unique modulo the ideal generated by the

72 defining equations of the Jacobian, satisfied by each of $\mathbf{a}$ and $\mathbf{b}$. We shall remove this ambiguity by fixing a representative of any biquadratic form; namely, we express any such form uniquely as a linear combination of monomials $a_i a_j b_m b_n$, where $a_i a_j \in U_{\mathbf{a}}$ and $b_m b_n \in U_{\mathbf{b}}$.

Lemma 3.6. *Any bilinear form $\sigma(\mathbf{a}, \mathbf{b})$, $\mathbf{a}, \mathbf{b} \in J(\mathcal{C})$, is uniquely determined by its localisation σ^ℓ up to terms $s_1^i s_2^j t_1^m t_2^n$ of degree: $i + j \leqslant 6, m + n \leqslant 6$. Any biquadratic form is uniquely determined by its localisation up to terms of degree $i + j \leqslant 12, m + n \leqslant 12$.*

Proof. The independent polynomials of lowest degree of the localisations in $S_{\mathbf{a}}^\ell$ have degree $\leqslant 6$. Similarly, those of $T_{\mathbf{a}}^\ell$ have degree $\leqslant 12$. □

The members of $S_{\mathbf{a}}^\ell$ modulo degree 7 form a $\mathbb{Z}[f_0, \ldots, f_6]$-basis for: $\mathbb{Q}(f_0, \ldots, f_6)[S_{\mathbf{a}}^\ell] \cap \mathbb{Z}[f_0, \ldots, f_6][s_1, s_2, t_1, t_2]$ modulo degree 7. Similarly for $U_{\mathbf{a}}^\ell$ modulo degree 13. This may be combined with Lemma 3.6 to give the following equivalence between the integrality of a form and of its localisation.

Lemma 3.7. *Let $\sigma(\mathbf{a}, \mathbf{b})$ be a bilinear or biquadratic form over $\mathbb{Q}(f_0, \ldots, f_6)$. Then σ is defined over $\mathbb{Z}[f_0, \ldots, f_6]$ if and only if its localisation σ^ℓ is defined over $\mathbb{Z}[f_0, \ldots, f_6]$.* □

Given the above lemmas, we can use local power series to derive the $\phi_{ij}(\mathbf{a}, \mathbf{b})$ in two stages. First, we express the coefficients of the function $Y - (\alpha X^3 + \beta X^2 + \gamma X + \delta)$ in terms of $\mathbf{a}$, $\mathbf{b}$. Specifically, $(1, \alpha, \beta, \gamma, \delta)$ are projectively equal to ([8], p.431):

$$a_{10}b_{15} + b_{10}a_{15} - a_{14}b_{11} + a_{13}(b_{12} + b_{13}) + b_{13}(a_{12} + a_{13})$$

$$a_7 b_{15} + b_7 a_{15} + a_{13}b_9 + b_{13}a_9 - a_{14}b_8 - b_{14}a_8$$

$$-a_6 b_{15} - b_6 a_{15} + a_8(b_{12} + b_{13}) + b_8(a_{12} + a_{13}) - a_{11}b_9 - b_{11}a_9$$

$$a_6 b_{14} + b_6 a_{14} - a_7(b_{12} + b_{13}) - b_7(a_{12} + a_{13}) + a_9 b_{10} + b_9 a_{10}$$

$$-a_6 b_{13} - b_6 a_{13} + a_7 b_{11} + b_7 a_{11} - a_8 b_{10} - b_8 a_{10}$$

respectively. We can now express all of the rational functions in x_1, y_1, x_2, y_2 in method 1 as considerably simpler functions in $\mathbf{a}$, $\mathbf{b}$. That is, we express each desired $\phi_{ij}(\mathbf{a}, \mathbf{b})$ as:

$$\phi_{ij}(\mathbf{a}, \mathbf{b}) = \mathcal{N}_{ij}(\mathbf{a}, \mathbf{b}) / \mathcal{D}_{ij}(\mathbf{a}, \mathbf{b})$$

where $\mathcal{N}_{ij}, \mathcal{D}_{ij}$ are known homogeneous forms over $\mathbb{Z}[f_0, \ldots, f_6]$, with $\mathcal{N}_{ij}$ of degree 1 greater than $\mathcal{D}_{ij}$ in each of $\mathbf{a}$ and $\mathbf{b}$. Then $\phi_{ij}^{\ell} = \mathcal{N}_{ij}^{\ell}/\mathcal{D}_{ij}^{\ell}$, and so we may write out $\mathcal{N}_{ij}^{\ell}, \mathcal{D}_{ij}^{\ell}$ to derive ϕ_{ij}^{ℓ} to any required degree in s_1, s_2, t_1, t_2. We may then use Lemma 3.6 (the bilinear case) to determine the coefficients of ϕ_{ij}. As a further verification, after deriving ϕ_{ij}, we can check that $\phi_{ij} \cdot \mathcal{D}_{ij} - \mathcal{N}_{ij}$ lies in the ideal generated by the defining equations satisfied by $\mathbf{a}$ and $\mathbf{b}$.

Method 3. *Via the ψ_{ij} of Lemma 2.2.*

One first derives the ψ_{ij} from the involution W^g (as outlined in Section 2). Then these clearly give all *even·even* terms of the ϕ_{ij}. It is now a matter of finding the missing *odd·odd* terms. By remark 3.3 (iv), the ϕ_{ii} along the leading diagonal have no *odd·odd* terms, and so are completely determined by the ψ_{ii}. Further, by Remark 3.3 (ii), the first 3 rows at $\mathbf{b} = \mathbf{a}$ lie in the ideal generated by the defining equations satisfied by $\mathbf{a}$. Since there are only 3 defining equations with purely *odd·odd* terms, we need only find a few integer coefficients to determine ϕ_{ij} completely. These remaining coefficients may be fixed by linear equations induced by a selection of specialised curves over $\mathbb{Z}$. Having found all ϕ_{ij} in the first 3 rows and the leading diagonal, the remaining: $\phi_{41}, \phi_{42}, \phi_{43}$ can be derived using Remark 3.3 (iv), by negating the *odd·odd* terms of $\phi_{14}, \phi_{24}, \phi_{34}$, respectively.

Conversely, the reader can easily perform the easier task of recovering the ψ_{ij} (which have not been listed separately) from the ϕ_{ij} of Appendix B. First, the *odd·odd* terms must be removed (by setting $a_1, a_2, a_6, a_7, a_8, a_9, b_1, b_2, b_6, b_7, b_9, b_9$ to 0). Then each even a_i should be replaced by $\rho_i(\mathbf{k})$ of Lemma 3.1, and similarly for each even b_i.

We conclude with a few corollaries of Theorem 3.2. Recall from Remark 3.3 (ii) that only the last row can be specialised to give the duplication law. If we set $\mathbf{b} = \mathbf{a}$ in this row to get: $\big(\phi_{41}(\mathbf{a}, \mathbf{a}), \phi_{42}(\mathbf{a}, \mathbf{a}), \phi_{43}(\mathbf{a}, \mathbf{a}), \phi_{44}(\mathbf{a}, \mathbf{a})\big)$, we obtain quadratic forms in $\mathbf{a}$ such that each monomial $a_i a_j$ has either both a_i, a_j even or both odd. If they are both odd, then $a_i a_j$ may be replaced by E_{ij} of (11). This gives quadratic forms in the even functions of $\mathbf{a}$ which may composed with the substitution $a_i = \rho_i(\mathbf{k})$ to give the duplication law in terms of homogeneous quartics on the Kummer surface. Alternatively, we can use the ψ_{ij} of Lemma 2.2 to get the same form of the duplication law as $\big(2\psi_{41}(\mathbf{k}, \mathbf{k}), 2\psi_{42}(\mathbf{k}, \mathbf{k}), 2\psi_{43}(\mathbf{k}, \mathbf{k}), \psi_{44}(\mathbf{k}, \mathbf{k})\big)$.

Corollary 3.8. *Let* $\mathbf{k} \in \mathcal{K}(\mathcal{C})$ *Then* $2\mathbf{k} = \big(\delta_1(\mathbf{k}), \delta_2(\mathbf{k}), \delta_3(\mathbf{k}), \delta_4(\mathbf{k})\big)$, *where each* $\delta_i(\mathbf{k})$, *given in Appendix C, is a quartic form in* $\mathbf{k}$. □

The initial parts give: $2\mathbf{k} \approx (4k_1k_4^3, 4k_2k_4^3, 4k_3k_4^3, k_4^4)$, which is strikingly similar in appearance to the duplication law on the X-coordinate of an elliptic curve ([14], p.59).

A second corollary follows from the fact that we can use ρ to give the even functions of $\mathbf{c}$, where $\mathbf{c} = \mathbf{a} + \mathbf{b}$, as quadratic forms in the ϕ_{ij}. That is, as biquadratic forms in $\mathbf{a}$, $\mathbf{b}$; this can be extended to the odd functions of $\mathbf{c}$ to give the entire group law on $J(\mathcal{C})$ as a biquadratic map.

Corollary 3.9. *Let* $\mathbf{a}, \mathbf{b}, \mathbf{c}, \bar{\mathbf{c}} \in J(\mathcal{C})$ *satisfy* $\mathbf{c} = \mathbf{a} + \mathbf{b}$, $\bar{\mathbf{c}} = \mathbf{a} - \mathbf{b}$. *Then there is a* 16×16 *matrix of biquadratic forms* $\big(\varsigma_{ij}(\mathbf{a}, \mathbf{b})\big)$ *over* $\mathbb{Z}[f_0, \ldots, f_6]$ *which is projectively equal to the matrix* $(\bar{c}_i c_j)$. *Any row gives the group law as a biquadratic map, with the row* $i = 0$, *namely* $\big(\varsigma_{0j}(\mathbf{a}, \mathbf{b})\big)$, *non-degenerate at duplication. The form* ς_{00} *has initial part* $a_0^2 b_0^2$.

Proof. We first note that, if $\bar{c}_i$, c_j are both even functions, we may use ρ_i, ρ_j of Lemma 3.1 to obtain: $(\bar{c}_i c_j) = \big(\rho_i(k_1(\bar{\mathbf{c}}), \ldots, k_4(\bar{\mathbf{c}}))\rho_j(k_1(\mathbf{c}), \ldots, k_4(\mathbf{c}))\big) = \big(Q_{ij}(\phi_{11}(\mathbf{a}, \mathbf{b}), \phi_{12}(\mathbf{a}, \mathbf{b}), \ldots, \phi_{44}(\mathbf{a}, \mathbf{b})\big)$, where Q_{ij} is a quadratic form in $\phi_{11}, \phi_{12}, \ldots, \phi_{44}$, and so is a biquadratic form in $\mathbf{a}, \mathbf{b}$, denoted $\varsigma_{ij}(\mathbf{a}, \mathbf{b})$. Each $\varsigma_{ij}(\mathbf{a}, \mathbf{b})$ is defined over $\mathbb{Z}[f_0, \ldots, f_6]$; this is immediate when $i, j \neq 4$, since then ρ_i, ρ_j are over $\mathbb{Z}[f_0, \ldots, f_6]$; when i or j (or both) $= 4$, then the denominator of 2 in ρ_4 is cancelled in $\big(Q_{ij}(\phi_{11}(\mathbf{a}, \mathbf{b}), \phi_{12}(\mathbf{a}, \mathbf{b}), \ldots, \phi_{44}(\mathbf{a}, \mathbf{b})\big)$. The initial part of $\varsigma_{ij}(\mathbf{a}, \mathbf{b})$ is therefore induced directly as Q_{ij} of the initial parts of the ϕ's. In particular, $\varsigma_{00}(\mathbf{a}, \mathbf{b}) = \rho_0(k_1(\bar{\mathbf{c}}), \ldots, k_4(\bar{\mathbf{c}}))\rho_0(k_1(\mathbf{c}), \ldots, k_4(\mathbf{c})) = k_4(\bar{\mathbf{c}})^2 k_4(\mathbf{c})^2 = (k_4(\bar{\mathbf{c}})k_4(\mathbf{c}))^2 = (\phi_{44})^2 \approx a_0^2 b_0^2$.

Finally, if either $\bar{c}_i$ or c_j (or both) is odd, then we use the quadratic forms of equation (11) to see that: $(\bar{c}_i c_j)^2 = E_{ii}(\mathcal{E}(\bar{\mathbf{c}}))E_{jj}(\mathcal{E}(\mathbf{c}))$, which, by the first part above, are quartic forms in $\mathbf{a}, \mathbf{b}$ over $\mathbb{Z}[f_0, \ldots, f_6]$. Thus, $(\bar{c}_i c_j)^2 \in \mathcal{L}\big(8(\Theta^+ + \Theta^-)\big) \otimes \mathcal{L}\big(8(\Theta^+ + \Theta^-)\big)$, and so the rational function $\bar{c}_i c_j \in \mathcal{L}\big(4(\Theta^+ + \Theta^-)\big) \otimes \mathcal{L}\big(4(\Theta^+ + \Theta^-)\big)$. Therefore, by Lemma 3.5, there must exist biquadratic forms $\varsigma_{ij}(\mathbf{a}, \mathbf{b})$ defined over $\mathbb{Q}(f_0, \ldots, f_6)$ such that $\varsigma_{ij}(\mathbf{a}, \mathbf{b}) = (\bar{c}_i c_j)$. Further, the localisation $(\varsigma_{ij}^\ell)^2 = \big(E_{ii}(\mathcal{E}(\bar{\mathbf{c}}))E_{jj}(\mathcal{E}(\mathbf{c}))\big)^\ell$, which by Lemma 3.7, is defined over $\mathbb{Z}[f_0, \ldots, f_6]$. Therefore, the same is true of ς_{ij}^ℓ, by the integral closure of the ring of power series in s_1, s_2, t_1, t_2 over $\mathbb{Z}[f_0, \ldots, f_6]$. It follows (by the reverse direction of Lemma 3.7) that $\varsigma_{ij}(\mathbf{a}, \mathbf{b})$ is also defined over $\mathbb{Z}[f_0, \ldots, f_6]$. □

The biquadratic forms are too large to be written out explicitly for a general curve $\mathcal{C}$ over $\mathbb{Z}[f_0,\ldots,f_6]$. However, for any specialisation over $\mathbb{Z}$, the above Lemmas provide a method for writing them out in full. That is, one first specialises the bilinear forms to $f_0,\ldots,f_6\in\mathbb{Z}$, and derives $\varsigma_{ij}(\mathbf{a},\mathbf{b})=\bar{c}_ic_j$ for $\bar{c}_i,c_j$ even (using ρ). Then, for either c_i or c_j odd (or both), one finds $\varsigma^\ell(\mathbf{a},\mathbf{b})$ up to terms $s_1^is_2^jt_1^mt_2^n$ of degree: $i+j\leqslant 12, m+n\leqslant 12$, and applies Lemma 3.6 to determine the coefficients of $\varsigma(\mathbf{a},\mathbf{b})$. In general, it seems better to work as much as possible with the Kummer surface; it is reassuring to know that the ς_{ij} exist, but the ϕ_{ij} should be sufficient for most computational purposes.

In retrospect, there is a slight improvement on the embedding in Definition 1.1 which would have simplified a portion of the above discussion. Namely, one could replace a_4 with $2a_4+f_1a_{15}+f_3a_{13}+f_5a_{10}=(x_1+x_2)a_5$, and replace a_{12} with $a_{12}+2a_{13}=(x_1+x_2)^2$. This would remove the denominator of 2 from ρ_4 of Lemma 3.1, and indeed would transform every ρ_i and θ_j^i (the maps between $\mathcal{E}(\mathcal{C})$ and $\mathcal{K}(\mathcal{C})$) into a monomial. A change of basis along these lines would certainly be a prerequisite for a development in characteristic 2 (as well as alterations to $a_0,\ldots,a_{15}$ induced by including Y, XY and X^2Y terms in the original curve $\mathcal{C}$). There is also a case to be made for replacing a_{12} with $a_{12}-2a_{13}=(x_1-x_2)^2$ so that the local power series expansions in equation (4) would all have independent polynomials of lowest degree. However, it was felt that remaining consistent with the notation of [8] was more important than such minor technical simplifications.

A fringe benefit of the bilinear forms of Theorem 3.2 is an improved proof of Theorem 1.5, that the formal group law, induced by the choice of local parameters s_1,s_2, is defined over $\mathbb{Z}[f_0,\ldots,f_6]$.

Corollary 3.10. *Let ς_{ij} be as in Corollary 3.9. The local power series expansion of ς_{00} has initial term* 1*, and so is invertible. Therefore, the formal group given by $\varsigma_{01}/\varsigma_{00}$, $\varsigma_{02}/\varsigma_{00}$ is defined over $\mathbb{Z}[f_0,\ldots,f_6]$ and converges for all $\mathbf{a},\mathbf{b}\in\mathcal{N}$.*

Proof. The form ς_{00} has initial term $a_0^2b_0^2$, and so ς_{00}^ℓ has initial term 1. That is, $\varsigma^\ell(s_1,s_2,t_1,t_2)=1+$ terms of degree $\geqslant 1$ in s_1,s_2,t_1,t_2, and so is an invertible power series. Therefore, $\varsigma_{01}/\varsigma_{00}$, $\varsigma_{02}/\varsigma_{00}$ are defined over $\mathbb{Z}[f_0,\ldots,f_6]$, and converge in $\mathcal{N}\times\mathcal{N}$. □

This improves on the proof in [8] in that it does not require the use of the theory of Lie Groups to guarantee the existence of the formal group over the field of fractions.

There are promising signs that the Jacobians of curves of genus 2 will become rapidly more amenable to arithmetic investigation over the next few years. A temporary problem is that, at present, computational work is only accessible to a small group working in the area. We suggest that it is well worth the trouble to place the general forms of equations in the public domain, even if these are of rather unwieldy size. Presentations along these lines have already been made in [10] (the general form of the homogeneous spaces for a complete 2-descent) and [8],[9] (formal groups). Such presentations have the advantage (over loose descriptions of algorithms) that a wider group of users who wish to experiment with specific curves need merely specialise the given equations to the chosen values of $f_0, \ldots, f_6$, and need not necessarily become acquainted with the mechanics of their derivation. We have made the expressions derived in Secions 2 and 3 available by anonymous ftp, as described in the appendices below.

Appendix A. Addition by a Point of Order 2 on the Kummer Surface

All of the following files are available at: www.maths.ox.ac.uk/~flynn/genus2 and the file README will be regularly updated and contains a listing and brief description of all the files in www.maths.ox.ac.uk/~flynn/genus2 which might be of use to the reader.

The file www.maths.ox.ac.uk/~flynn/genus2/kummer/defeqns contains the following equations in Appendix A. It will not be altered in name or content; any enhanced version will be added to the directory as a new file.

Let $\mathcal{C}$ be as in equation (1), and let $\mathbf{k} = (k_1, k_2, k_3, k_4) \in \mathcal{K}(\mathcal{C})$. Then $\mathbf{k}$ satisfies the quartic:

$$R(k_1, k_2, k_3)k_4^2 + S(k_1, k_2, k_3)k_4 + T(k_1, k_2, k_3)$$

where R, S, T are given by:

$$\begin{aligned}
R(k_1, k_2, k_3) = {} & k_2^2 - 4k_1k_3 \\
S(k_1, k_2, k_3) = {} & -2(2k_1^3f_0 + k_1^2k_2f_1 + 2k_1^2k_3f_2 + k_1k_2k_3f_3 + 2k_1k_3^2f_4 + k_2k_3^2f_5 + 2k_3^3f_6) \\
T(k_1, k_2, k_3) = {} & -4k_1^4f_0f_2 + k_1^4f_1^2 - 4k_1^3k_2f_0f_3 - 2k_1^3k_3f_1f_3 - 4k_1^2k_2^2f_0f_4 + 4k_1^2k_2k_3f_0f_5 - 4k_1^2k_2k_3f_1f_4 - \\
& 4k_1^2k_3^2f_0f_6 + 2k_1^2k_3^2f_1f_5 - 4k_1^2k_3^2f_2f_4 + k_1^2k_3^2f_3^2 - 4k_1k_2^3f_0f_5 + 8k_1k_2^2k_3f_0f_6 - 4k_1k_2^2k_3f_1f_5 + \\
& 4k_1k_2k_3^2f_1f_6 - 4k_1k_2k_3^2f_2f_5 - 2k_1k_3^3f_3f_5 - 4k_2^4f_0f_6 - 4k_2^3k_3f_1f_6 - 4k_2^2k_3^2f_2f_6 - 4k_2k_3^3f_3f_6 - \\
& 4k_3^4f_4f_6 + k_3^4f_5^2
\end{aligned}$$

Let us temporarily assume that our curve has the form $\mathcal{C}^g$ of equation (8). Then the following is the matrix W^g (Lemma 2.1) which gives the addition of a rational point, $\mathbf{b}^g$, of order 2.

$$
\begin{aligned}
W^g_{11} &= -g_2^2h_0 + g_0g_2h_2 + g_0^2h_4\\
W^g_{12} &= -g_1g_2h_0 + g_0g_2h_1\\
W^g_{13} &= -g_1^2h_0 + 2g_0g_2h_0 + g_0g_1h_1\\
W^g_{14} &= g_0\\
W^g_{21} &= g_2^2h_1 - g_1g_2h_2 - g_0g_2h_3\\
W^g_{22} &= g_2^2h_0 - g_0g_2h_2 + g_0^2h_4\\
W^g_{23} &= -g_0g_2h_1 - g_0g_1h_2 + g_0^2h_3\\
W^g_{24} &= -g_1\\
W^g_{31} &= g_1g_2h_3 - g_1^2h_4 + 2g_0g_2h_4\\
W^g_{32} &= g_0g_2h_3 - g_0g_1h_4\\
W^g_{33} &= g_2^2h_0 + g_0g_2h_2 - g_0^2h_4\\
W^g_{34} &= g_2\\
W^g_{41} &= -g_0g_2^2h_1h_3 - g_0g_1g_2h_2h_3 + g_0g_1g_2h_1h_4 + g_0g_1^2h_2h_4 + g_0^2g_2h_3^2 - 4g_0^2g_2h_2h_4 - g_0^2g_1h_3h_4\\
W^g_{42} &= g_1^2g_2h_0h_3 - g_1^3h_0h_4 - 2g_0g_2^2h_0h_3 - g_0g_1g_2h_1h_3 + 4g_0g_1g_2h_0h_4 + g_0g_1^2h_1h_4 - 2g_0^2g_2h_1h_4\\
W^g_{43} &= -g_1g_2^2h_0h_1 + g_1^2g_2h_0h_2 + g_0g_2^2h_1^2 - 4g_0g_2^2h_0h_2 - g_0g_1g_2h_1h_2 + g_0g_1g_2h_0h_3 - g_0^2g_2h_1h_3\\
W^g_{44} &= -g_2^2h_0 - g_0g_2h_2 - g_0^2h_4
\end{aligned}
$$

Appendix B. Bilinear Forms on the Jacobian

The file www.maths.ox.ac.uk/~flynn/genus2/jac/bilforms contains the bilinear forms $\phi_{ij}(\mathbf{a},\mathbf{b})$ described in Theorem 3.2, satisfying $\big(\phi_{ij}(\mathbf{a},\mathbf{b})\big) = \big(k_i(\mathbf{a}-\mathbf{b})k_j(\mathbf{a}+\mathbf{b})\big)$. The terms of each form are arranged in paragraphs; the initial part (free of $f_0,\ldots,f_6$) is given first, and subsequent paragraphs are in order of increasing degree in $f_0,\ldots,f_6$.

Appendix C. The Duplication Law

Let $\mathbf{k} \in \mathcal{K}(\mathcal{C})$. Then the following are the quartic forms $\delta_i(\mathbf{k})$ described in Corollary 3.8, which satisfy $2\mathbf{k} = \big(\delta_1(\mathbf{k}),\delta_2(\mathbf{k}),\delta_3(\mathbf{k}),\delta_4(\mathbf{k})\big)$. These are in the file www.maths.ox.ac.uk/~flynn/genus2/kummer/dupl

$$
\begin{aligned}
\delta_1(\mathbf{k}) = {} & 4k_1k_4^3+\\
& 4k_4^2(k_1^2f_2 - k_2k_3f_5 - 3k_3^2f_6)+\\
& 4k_4(-4k_1^3f_0f_4 + k_1^3f_1f_3 - 8k_1^2k_2f_0f_5 - 2k_1^2k_3f_1f_5 - 12k_1k_2^2f_0f_6 - k_1k_2^2f_1f_5 - 6k_1k_2k_3f_1f_6 -\\
& 2k_1k_2k_3f_2f_5 - 4k_1k_3^2f_2f_6 - k_1k_3^2f_3f_5 - 2k_2^3f_1f_6 - 4k_2^2k_3f_2f_6 - 6k_2k_3^2f_3f_6 - 8k_3^3f_4f_6 + 2k_3^3f_5^2)+\\
& 4(-4k_1^4f_0^2f_6 - 4k_1^4f_0f_2f_4 + k_1^4f_0f_3^2 + k_1^4f_1^2f_4 - 4k_1^3k_2f_0f_1f_6 - 8k_1^3k_2f_0f_2f_5 + 2k_1^3k_2f_1^2f_5 +\\
& 8k_1^3k_3f_0f_2f_6 - 4k_1^3k_3f_0f_3f_5 - 4k_1^3k_3f_1^2f_6 - 16k_1^2k_2^2f_0f_2f_6 - 2k_1^2k_2^2f_0f_3f_5 + 3k_1^2k_2^2f_1^2f_6 -\\
& 4k_1^2k_2k_3f_0f_4f_5 - 4k_1^2k_2k_3f_1f_2f_6 - k_1^2k_2k_3f_1f_3f_5 - 12k_1^2k_3^2f_0f_4f_6 + 4k_1^2k_3^2f_0f_5^2 + 6k_1^2k_3^2f_1f_3f_6 -\\
& 2k_1^2k_3^2f_1f_4f_5 - 4k_1^2k_3^2f_2^2f_6 - 8k_1k_2^3f_0f_3f_6 - 4k_1k_2^2k_3f_0f_5^2 - 6k_1k_2^2k_3f_1f_3f_6 - 4k_1k_2k_3^2f_0f_5f_6 -
\end{aligned}
$$

$$2k_1k_2k_3^2f_1f_5^2 - 4k_1k_2k_3^2f_2f_3f_6 + 8k_1k_3^3f_0f_6^2 - 4k_1k_3^3f_1f_5f_6 - 2k_1k_3^3f_3^2f_6 - 4k_2^4f_0f_4f_6 + k_2^4f_0f_5^2 - 4k_2^3k_3f_0f_5f_6 - 4k_2^3k_3f_1f_4f_6 + k_2^3k_3f_1f_5^2 - 12k_2^2k_3^2f_0f_6^2 - 2k_2^2k_3^2f_1f_5f_6 - 4k_2^2k_3^2f_2f_4f_6 + k_2^2k_3^2f_2f_5^2 - 8k_2k_3^3f_1f_6^2 - 4k_2k_3^3f_3f_4f_6 + k_2k_3^3f_3f_5^2 - 4k_3^4f_2f_6^2 + 2k_3^4f_3f_5f_6 - 4k_3^4f_4^2f_6 + k_3^4f_4f_5^2)$$

$$\delta_2(\mathbf{k}) = 4k_2k_4^3 +$$

$$k_4^2(4k_1^2f_1 + 8k_1k_2f_2 - 8k_1k_3f_3 + 5k_2^2f_3 + 8k_2k_3f_4 + 4k_3^2f_5) +$$

$$2k_4(2k_1^3f_0f_3 + 8k_1^2k_2f_0f_4 + k_1^2k_2f_1f_3 - 8k_1^2k_3f_0f_5 + 8k_1^2k_3f_1f_4 - 6k_1^2k_3f_2f_3 + 4k_1k_2^2f_0f_5 + 4k_1k_2^2f_1f_4 - 24k_1k_2k_3f_0f_6 + 8k_1k_2k_3f_1f_5 + 8k_1k_2k_3f_2f_4 - 5k_1k_2k_3f_3^2 - 8k_1k_3^2f_1f_6 + 8k_1k_3^2f_2f_5 - 6k_1k_3^2f_3f_4 + 2k_2^3f_1f_5 + 4k_2^2k_3f_1f_6 + 4k_2^2k_3f_2f_5 + 8k_2k_3^2f_2f_6 + k_2k_3^2f_3f_5 + 2k_3^3f_3f_6) +$$

$$16k_1^4f_0^2f_5 - 4k_1^4f_0f_2f_3 + k_1^4f_1^2f_3 + 32k_1^3k_2f_0^2f_6 + 16k_1^3k_2f_0f_1f_5 - 4k_1^3k_2f_0f_3^2 - 32k_1^3k_3f_0f_2f_5 + 16k_1^3k_3f_0f_3f_4 + 16k_1^3k_3f_1^2f_5 - 6k_1^3k_3f_1f_3^2 + 32k_1^2k_2^2f_0f_1f_6 - 4k_1^2k_2^2f_0f_3f_4 + 4k_1^2k_2^2f_1^2f_5 - 64k_1^2k_2k_3f_0f_2f_6 - 20k_1^2k_2k_3f_0f_3f_5 + 32k_1^2k_2k_3f_0f_4^2 + 32k_1^2k_2k_3f_1^2f_6 + 16k_1^2k_2k_3f_1f_2f_5 - 12k_1^2k_2k_3f_1f_3f_4 - 20k_1^2k_3^2f_0f_3f_6 - 14k_1^2k_3^2f_1f_3f_5 + 16k_1^2k_3^2f_1f_4^2 + 16k_1^2k_3^2f_2^2f_5 - 20k_1^2k_3^2f_2f_3f_4 + 5k_1^2k_3^2f_3^3 - 4k_1k_2^3f_0f_3f_5 + 8k_1k_2^3f_1^2f_6 - 56k_1k_2^2k_3f_0f_3f_6 + 32k_1k_2^2k_3f_0f_4f_5 + 32k_1k_2^2k_3f_1f_2f_6 - 8k_1k_2^2k_3f_1f_3f_5 - 64k_1k_2k_3^2f_0f_4f_6 + 32k_1k_2k_3^2f_0f_5^2 - 20k_1k_2k_3^2f_1f_3f_6 + 16k_1k_2k_3^2f_1f_4f_5 + 32k_1k_2k_3^2f_2^2f_6 - 12k_1k_2k_3^2f_2f_3f_5 - 32k_1k_3^3f_1f_4f_6 + 16k_1k_3^3f_1f_5^2 + 16k_1k_3^3f_2f_3f_6 - 6k_1k_3^3f_3^2f_5 - 4k_2^4f_0f_3f_6 + 8k_2^3k_3f_0f_5^2 - 4k_2^3k_3f_1f_3f_6 + 32k_2^2k_3^2f_0f_5f_6 + 4k_2^2k_3^2f_1f_5^2 - 4k_2^2k_3^2f_2f_3f_6 + 32k_2k_3^3f_0f_6^2 + 16k_2k_3^3f_1f_5f_6 - 4k_2k_3^3f_3^2f_6 + 16k_3^4f_1f_6^2 - 4k_3^4f_3f_4f_6 + k_3^4f_3f_5^2$$

$$\delta_3(\mathbf{k}) = 4k_3k_4^3 +$$

$$4k_4^2(-3k_1^2f_0 - k_1k_2f_1 + k_3^2f_4) +$$

$$4k_4(-8k_1^3f_0f_2 + 2k_1^3f_1^2 - 6k_1^2k_2f_0f_3 - 4k_1^2k_3f_0f_4 - k_1^2k_3f_1f_3 - 4k_1k_2^2f_0f_4 - 6k_1k_2k_3f_0f_5 - 2k_1k_2k_3f_1f_4 - 2k_1k_3^2f_1f_5 - 2k_2^3f_0f_5 - 12k_2^2k_3f_0f_6 - k_2^2k_3f_1f_5 - 8k_2k_3^2f_1f_6 - 4k_3^3f_2f_6 + k_3^3f_3f_5) +$$

$$4(-4k_1^4f_0^2f_4 + 2k_1^4f_0f_1f_3 - 4k_1^4f_0f_2^2 + k_1^4f_1^2f_2 - 8k_1^3k_2f_0^2f_5 - 4k_1^3k_2f_0f_2f_3 + k_1^3k_2f_1^2f_3 + 8k_1^3k_3f_0^2f_6 - 4k_1^3k_3f_0f_1f_5 - 2k_1^3k_3f_0f_3^2 - 12k_1^2k_2^2f_0^2f_6 - 2k_1^2k_2^2f_0f_1f_5 - 4k_1^2k_2^2f_0f_2f_4 + k_1^2k_2^2f_1^2f_4 - 4k_1^2k_2k_3f_0f_1f_6 - 4k_1^2k_2k_3f_0f_3f_4 - 2k_1^2k_2k_3f_1^2f_5 - 12k_1^2k_3^2f_0f_2f_6 + 6k_1^2k_3^2f_0f_3f_5 - 4k_1^2k_3^2f_0f_4^2 + 4k_1^2k_3^2f_1^2f_6 - 2k_1^2k_3^2f_1f_2f_5 - 4k_1k_2^3f_0f_1f_6 - 4k_1k_2^3f_0f_2f_5 + k_1k_2^3f_1^2f_5 - 6k_1k_2^2k_3f_0f_3f_5 - 4k_1k_2^2k_3f_1^2f_6 - 4k_1k_2k_3^2f_0f_4f_5 - 4k_1k_2k_3^2f_1f_2f_6 - k_1k_2k_3^2f_1f_3f_5 + 8k_1k_3^3f_0f_4f_6 - 4k_1k_3^3f_0f_5^2 - 4k_1k_3^3f_1f_3f_6 - 4k_2^4f_0f_2f_6 + k_2^4f_1^2f_6 - 8k_2^3k_3f_0f_3f_6 - 16k_2^2k_3^2f_0f_4f_6 + 3k_2^2k_3^2f_0f_5^2 - 2k_2^2k_3^2f_1f_3f_6 - 4k_2k_3^3f_0f_5f_6 - 8k_2k_3^3f_1f_4f_6 + 2k_2k_3^3f_1f_5^2 - 4k_3^4f_0f_6^2 - 4k_3^4f_2f_4f_6 + k_3^4f_2f_5^2 + k_3^4f_3^2f_6)$$

$$\delta_4(\mathbf{k}) = k_4^4 +$$

$$0 +$$

$$2k_4^2(4k_1^2f_0f_4 - k_1^2f_1f_3 + 4k_1k_2f_0f_5 + 8k_1k_3f_0f_6 + 4k_2^2f_0f_6 + 4k_2k_3f_1f_6 + 4k_3^2f_2f_6 - k_3^2f_3f_5) +$$

$$4k_4(8k_1^3f_0f_2f_4 - 2k_1^3f_0f_3^2 - 2k_1^3f_1^2f_4 + 12k_1^2k_2f_0f_2f_5 - 3k_1^2k_2f_1^2f_5 + 8k_1^2k_3f_0f_2f_6 + 4k_1^2k_3f_0f_3f_5 - 2k_1^2k_3f_1^2f_6 + 16k_1k_2^2f_0f_2f_6 + 2k_1k_2^2f_0f_3f_5 - 4k_1k_2^2f_1^2f_6 + 20k_1k_2k_3f_0f_3f_6 + k_1k_2k_3f_1f_3f_5 + 8k_1k_3^2f_0f_4f_6 - 2k_1k_3^2f_0f_5^2 + 4k_1k_3^2f_1f_3f_6 + 4k_2^3f_0f_3f_6 + 16k_2^2k_3f_0f_4f_6 - 4k_2^2k_3f_0f_5^2 + 2k_2^2k_3f_1f_3f_6 + 12k_2k_3^2f_1f_4f_6 - 3k_2k_3^2f_1f_5^2 + 8k_3^3f_2f_4f_6 - 2k_3^3f_2f_5^2 - 2k_3^3f_3^2f_6) +$$

$$16k_1^4f_0^2f_2f_6 - 16k_1^4f_0^2f_3f_5 + 16k_1^4f_0^2f_4^2 - 4k_1^4f_0f_1^2f_6 + 8k_1^4f_0f_1f_2f_5 - 8k_1^4f_0f_1f_3f_4 + 16k_1^4f_0f_2^2f_4 - 4k_1^4f_0f_2f_3^2 - 2k_1^4f_1^3f_5 - 4k_1^4f_1^2f_2f_4 + k_1^4f_1^2f_3^2 - 32k_1^3k_2f_0^2f_3f_6 + 32k_1^3k_2f_0^2f_4f_5 + 32k_1^3k_2f_0f_1f_2f_6 - 16k_1^3k_2f_0f_1f_3f_5 + 32k_1^3k_2f_0f_2^2f_5 - 8k_1^3k_2f_1^3f_6 -$$

$8k_1^3k_2f_1^2f_2f_5 - 64k_1^3k_3f_0^2f_4f_6 + 32k_1^3k_3f_0^2f_5^2 + 16k_1^3k_3f_0f_1f_3f_6 + 16k_1^3k_3f_0f_2f_3f_5 - 4k_1^3k_3f_1^2f_3f_5 + 32k_1^2k_2^2f_0^2f_4f_6 + 16k_1^2k_2^2f_0^2f_5^2 - 24k_1^2k_2^2f_0f_1f_3f_6 + 64k_1^2k_2^2f_0f_2^2f_6 + 8k_1^2k_2^2f_0f_2f_3f_5 - 16k_1^2k_2^2f_1^2f_2f_6 - 2k_1^2k_2^2f_1^2f_3f_5 + 64k_1^2k_2k_3f_0^2f_5f_6 - 32k_1^2k_2k_3f_0f_1f_4f_6 + 16k_1^2k_2k_3f_0f_1f_5^2 + 64k_1^2k_2k_3f_0f_2f_3f_6 + 8k_1^2k_2k_3f_0f_3^2f_5 - 8k_1^2k_2k_3f_1^2f_3f_6 + 64k_1^2k_3^2f_0^2f_6^2 + 96k_1^2k_3^2f_0f_2f_4f_6 - 32k_1^2k_3^2f_0f_2f_5^2 - 16k_1^2k_3^2f_0f_3^2f_6 + 8k_1^2k_3^2f_0f_3f_4f_5 - 32k_1^2k_3^2f_1^2f_4f_6 + 12k_1^2k_3^2f_1^2f_5^2 + 8k_1^2k_3^2f_1f_2f_3f_6 + 32k_1k_2^3f_0^2f_5f_6 + 32k_1k_2^3f_0f_2f_3f_6 - 8k_1k_2^3f_1^2f_3f_6 + 64k_1k_2^2k_3f_0^2f_6^2 + 32k_1k_2^2k_3f_0f_1f_5f_6 + 48k_1k_2^2k_3f_0f_3^2f_6 + 64k_1k_2k_3^2f_0f_1f_6^2 - 32k_1k_2k_3^2f_0f_2f_5f_6 + 64k_1k_2k_3^2f_0f_3f_4f_6 - 8k_1k_2k_3^2f_0f_3f_5^2 + 16k_1k_2k_3^2f_1^2f_5f_6 + 8k_1k_2k_3^2f_1f_3^2f_6 - 64k_1k_3^3f_0f_2f_6^2 + 16k_1k_3^3f_0f_3f_5f_6 + 32k_1k_3^3f_1^2f_6^2 + 16k_1k_3^3f_1f_3f_4f_6 - 4k_1k_3^3f_1f_3f_5^2 + 16k_2^4f_0^2f_6^2 + 16k_2^4f_0f_2f_4f_6 - 4k_2^4f_0f_2f_5^2 - 4k_2^4f_1^2f_4f_6 + k_2^4f_1^2f_5^2 + 32k_2^3k_3f_0f_1f_6^2 + 32k_2^3k_3f_0f_3f_4f_6 - 8k_2^3k_3f_0f_3f_5^2 + 32k_2^2k_3^2f_0f_2f_6^2 - 24k_2^2k_3^2f_0f_3f_5f_6 + 64k_2^2k_3^2f_0f_4^2f_6 - 16k_2^2k_3^2f_0f_4f_5^2 + 16k_2^2k_3^2f_1^2f_6^2 + 8k_2^2k_3^2f_1f_3f_4f_6 - 2k_2^2k_3^2f_1f_3f_5^2 - 32k_2k_3^3f_0f_3f_6^2 + 32k_2k_3^3f_0f_4f_5f_6 - 8k_2k_3^3f_0f_5^3 + 32k_2k_3^3f_1f_2f_6^2 - 16k_2k_3^3f_1f_3f_5f_6 + 32k_2k_3^3f_1f_4^2f_6 - 8k_2k_3^3f_1f_4f_5^2 + 16k_3^4f_0f_4f_6^2 - 4k_3^4f_0f_5^2f_6 - 16k_3^4f_1f_3f_6^2 + 8k_3^4f_1f_4f_5f_6 - 2k_3^4f_1f_5^3 + 16k_3^4f_2^2f_6^2 - 8k_3^4f_2f_3f_5f_6 + 16k_3^4f_2f_4^2f_6 - 4k_3^4f_2f_4f_5^2 - 4k_3^4f_3^2f_4f_6 + k_3^4f_3^2f_5^2$

REFERENCES

[1] Adleman, L. M. and Huang, M. A. *Recognising Primes in Random Polynomial Time.* Proceedings of the Nineteenth Annual Symposium on Theory of Computing (1987), Association for Computing Machinery, 462-469.

[2] Bost, J. B. and Mestre, J.-F. *Moyenne arithmético-géometrique et périodes des courbes de genre 1 et 2.* Gaz. Math. Soc. France, **38** (1988), 36-64.

[3] Cantor, D. G. *Computing in the Jacobian of a Hyperelliptic Curve.* Mathematics of Computation, **48** (1987), 95-101.

[4] Cantor, D. G. *On the Analogue of the Division Polynomials for Hyperelliptic Curves I.* (preprint, U.C.L.A., 1991).

[5] Cassels, J. W. S. *Diophantine Equations with Special Reference to Elliptic Curves.* J. London Math. Soc. **41** (1966), 193-291.

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

[7] Davenport, J. H. *On the Integration of Algebraic Functions*, Springer Lecture Notes in Computer Science, 102, Springer-Verlag (1981).

[8] Flynn, E. V. *The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field.* Math. Proc. Camb. Phil. Soc. **107** (1990), 425-441.

[9] Grant, D. *Formal Groups in Genus 2.* J. Reine Angew. Math. **411** (1990), 96-121.

[10] Gordon, D.M. and Grant, D. *Computing the Mordell-Weil rank of Jacobians of curves of genus 2.* Transactions of the American Mathematical Association (to appear).

[11] Hudson, R. W. H. T., *Kummer's Quartic Surface*, University Press, Cambridge (1905). Reprint, 1990.

[12] Lang, S. *Introduction to Algebraic and Abelian Functions*, 2nd edition, Graduate Texts in Mathematics **89**, Springer-Verlag, New York (1982).

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

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

Prof. E.V. Flynn

Mathematical Institute

University of Oxford

Oxford OX1 3LB

United Kingdom

flynn@maths.ox.ac.uk