Chapter 1

Curves of genus 2

1 **Canonical form.** We shall normally suppose that the characteristic¶ of the ground field is not 2 and consider curves $\mathcal{C}$ of genus 2 in the shape

$$\mathcal{C}: \quad Y^2 = F(X), \tag{1.1.1}$$

where

$$F(X) = f_0 + f_1 X + \ldots + f_6 X^6 \in k[X] \tag{1.1.2}$$

is of degree 6 and has no multiple factors. As we shall see in a moment, every curve of genus 2 defined over k is birationally equivalent over k to a curve of this type, which is unique up to a fractional linear transformation of X, and associated transformation of Y,

$$X \longmapsto (aX + b)/(cX + d), \quad Y \longmapsto eY/(cX + d)^3, \tag{1.1.3}$$

where

$$a, b, c, d \in k, \quad ad - bc \neq 0, \quad e \in k^*. \tag{1.1.4}$$

When k is algebraically closed, we can always use a transformation of this kind to ensure that F is of degree 5:† this is what is almost always done in the classical theory. From our point of view, this is very special. We shall assume, by using a transformation (3)‡ if necessary, that F is of precise

¶ A more systematic treatment would require consideration of finite fields of characteristic 2, since these arise e.g. by reduction mod 2 when $k = \mathbb{Q}$. We shall not need it. The modifications required for characteristic 2 are left as optional exercises for the reader.

† This is possible precisely when the sextic $F(X)$ has a root $\alpha \in k$. Then we can use the map $X \mapsto 1/(X-\alpha)$, $Y \mapsto Y/(X-\alpha)^3$ from $Y^2 = F(X)$ to a curve $Y^2 = (\text{quintic in } X)$. For example, $X \mapsto 1/(X-2)$, $Y \mapsto Y/(X-2)^3$ maps $Y^2 = X^6 - 64$ to $Y^2 = (2X+1)^6 - 64X^6 = (\text{quintic in } X)$ [The second equation is obtained by replacing X by $(2X+1)/X$, Y by Y/X^3 in the first equation, and then multiplying through by X^6].

‡ Displayed formulae are referred to by a number triple. For example, (2.3.4) is display 4 in Section 3 of Chapter 2. It is cited as (4) within Section 3 of Chapter 2, as (3.4) in the rest of Chapter 2, and as (2.3.4) outside Chapter 2.

degree 6.¶

If we attempt to obtain a complete curve from the affine curve (1) by replacing X, Y by $X/Z, Y/Z^3$, we get an unpleasant singularity at $Z = 0$. We will get round this in one of two ways. The first is *à la Weil* to use a transformation (3) to ensure that none of the points we are interested in is 'at infinity'. Alternatively, we can use the complete nonsingular model

$$\begin{aligned} Y^2 = f_0X_0^2 + f_1X_0X_1 + f_2X_1^2 + f_3X_1X_2 + f_4X_2^2 + f_5X_2X_3 + f_6X_3^2, \\ X_0X_2 - X_1^2 = 0, \\ X_0X_3 - X_1X_2 = 0, \\ X_1X_3 - X_2^2 = 0, \end{aligned} \tag{1.1.5}$$

in $\mathbb{P}^4$. Here the points of (1) correspond to those of (5) with $X_0 \neq 0$ by

$$X_j = X^j,\ Y = Y. \tag{1.1.6}$$

We denote the points on $\mathcal{C}$ by small Fraktur letters, e.g.

$$\mathfrak{x} = (x, y). \tag{1.1.7}$$

The point

$$\bar{\mathfrak{x}} = (x, -y) \tag{1.1.8}$$

is the *conjugate* of $\mathfrak{x}$ (under the $\pm Y$ involution). A divisor of degree 2 of the type $\{\mathfrak{x}, \bar{\mathfrak{x}}\}$ is the intersection of $\mathcal{C}$ with $X = x$. Hence any two divisors of this type are linearly equivalent. We denote the corresponding element of Pic^2 by $\mathfrak{O}$: it is clearly the canonical class. By the Riemann-Roch Theorem, any other element $\mathfrak{A}$ of Pic^2 contains precisely one effective divisor. It is convenient, and with luck should cause no confusion, to identify $\mathfrak{A}$ with its unique effective divisor. Further, addition of $\mathfrak{O}$ in Pic identifies the jacobian $J(\mathcal{C}) = \mathrm{Pic}^0$ with Pic^2. Under this identification $0 \in J(\mathcal{C})$ goes to $\mathfrak{O}$ and the nonzero elements of $J(\mathcal{C})$ go to the effective $\mathfrak{A}$ of degree 2, $\mathfrak{A} \notin \mathfrak{O}$.

¶ If $F(X)$ is quintic it can be made sextic by using a map $X \mapsto 1/(X-\alpha)$, $Y \mapsto Y/(X-\alpha)^3$, but where now α is chosen to be any member of k which avoids the roots of $F(X)$. This is always possible when k has more than 5 elements. We shall exclude from consideration the few exceptional curves over $\mathbb{F}_3$ and $\mathbb{F}_5$ which cannot be put in the form $Y^2 =$ (sextic in X).

2 Group law. We can now describe the group law on $J(\mathcal{C})$, at least generically. Let $\mathfrak{A}$, $\mathfrak{B}$ be two effective divisors of degree 2 in general position defined over k. Then there is a unique $M(X) \in k[X]$ of degree 3 such that $Y = M(X)$ passes through the four points of $\mathfrak{A}$, $\mathfrak{B}$. The complete intersection of the cubic curve with $\mathcal{C}$ is given by

$$M(X)^2 = F(X), \quad Y = M(X). \tag{1.2.1}$$

Hence the residual intersection is an effective divisor $\mathfrak{C}$ of degree 2, also defined over k. The divisor of poles of the function $Y - M(X)$ is at infinity, and is in the divisor class $3\mathfrak{O} \in \mathrm{Pic}^6$. Identifying elements of Pic^0 with those of Pic^2, we have thus found a $\mathfrak{C}$ such that

$$\mathfrak{A} + \mathfrak{B} + \mathfrak{C} = \mathfrak{O}. \tag{1.2.2}$$

The divisor $\mathfrak{A} = \{\mathfrak{a}_1, \mathfrak{a}_2\}$ is rational (= defined over the ground field k) if either

(i) $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are both rational
or
(ii) they are defined over a quadratic extension of k and conjugate over k.¶

If $\mathfrak{A}$ and $\mathfrak{B}$ above are both rational, then so are $M(X)$ and $\mathfrak{C}$.

For $\mathfrak{A} = \{\mathfrak{a}_1, \mathfrak{a}_2\}$ we put $\bar{\mathfrak{A}} = \{\bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_2\}$. Clearly $\mathfrak{A} + \bar{\mathfrak{A}} = \mathfrak{O}$ in the sense of the group law, that is $\bar{\mathfrak{A}} = -\mathfrak{A}$. It follows that $\mathfrak{A}$ is of (precise) order 2 if $\mathfrak{A} \notin \mathfrak{O}$ and $\bar{\mathfrak{A}} = \mathfrak{A}$. Hence $\mathfrak{A} = \{(\theta_1, 0), (\theta_2, 0)\}$, where θ_1, θ_2 are distinct roots of $F(X)$. Thus over $\bar{k}$ there are $\binom{6}{2} = 15$ elements of Pic^0 of order 2, though, of course, they need not be defined over k.

We reserve the further investigation of the group law until later. For a worked example, see Chapter 8, Section 1. The rest of this chapter may be omitted at a first reading. Indeed, those wishing immediately to see the more computational side of things (such as computing the group law, the torsion group and rank of the Mordell-Weil group) can at this point proceed directly to Chapter 8, followed by Chapter 11. These are designed to be fairly self-contained, provided that a few results from earlier chapters are taken on faith.

¶ There are two notions of 'conjugate' in this book: 'conjugate over k' [e.g. $(\sqrt{2}, 1+\sqrt{2})$ and $(-\sqrt{2}, 1-\sqrt{2})$ are conjugate over $\mathbb{Q}$] and 'conjugate under the $\pm Y$ involution' [e.g. $(\sqrt{2}, 1+\sqrt{2})$ and $(\sqrt{2}, -1-\sqrt{2})$]. The word 'conjugate' may be used on its own when it is clear from the context which usage applies. When $\mathfrak{x} = (x, y)$ is defined over some $k(\sqrt{d})$ we may sometimes wish to refer to both types of conjugate of $\mathfrak{x}$; we distinguish them by using $\bar{\mathfrak{x}}$ for $(x, -y)$ and $\mathfrak{x}'$ for the conjugate of $\mathfrak{x}$ over k.

3 The form is canonical. We can now confirm that every curve $\mathcal{D}$ of genus 2 defined over a perfect field k of characteristic not 2 is birationally equivalent over k to a curve (1.1).

By Riemann-Roch the differentials of the first kind¶ on $\mathcal{D}$ are a $\bar{k}$-vector space of dimension 2. By the Appendix of 'Background and Notation' there is a differential of the first kind defined over k. Its divisor of zeros $\mathfrak{H}$ is an effective divisor defined over k in the canonical class.

By Riemann-Roch again, the space of functions f with $[f] \succ -\mathfrak{H}$ has dimension 2. As before, it contains a nonconstant function X defined over k. The divisor of poles of X is $\mathfrak{H}$. By† Riemann-Roch yet again, there is a function Y defined over k which has $3\mathfrak{H}$ as divisor of poles and which is linearly independent of $1, X, X^2, X^3$. Finally,

$$\{1, X, X^2, X^3, X^4, X^5, X^6, Y, YX, YX^2, YX^3, Y^2\} \tag{1.3.1}$$

have at worst $6\mathfrak{H}$ as divisor of poles, so are linearly dependent. After a transformation $Y \mapsto Y +$ cubic in X, this gives (1.1). The same argument shows that the transformations (1.3) are the only birational transformations which take $\mathcal{C}$ into another curve of the same form.

More generally, a hyperelliptic curve of *even* genus $g > 0$ is birationally equivalent over the ground field to a curve $Y^2 = F(X)$ with F of degree $2g + 2$; see Chevalley (1951), p. 77 [the paragraph before the enunciation of Theorem 10, but ignore from 'it can be proved' onward] or Mestre (1991b), p. 322.

4 Plane quartics. A further example of a curve of genus 2 is the plane quartic $\mathcal{D}$ with a single double point, say

$$G(U, V) = 0, \tag{1.4.1}$$

where $G \in k[U, V]$ is of degree 4. We shall assume that the ground field k is perfect and of characteristic not 2. The double point is defined over k by Galois theory, and so can be taken to be the origin. Then

$$G(U, V) = G_2(U, V) + G_3(U, V) + G_4(U, V), \tag{1.4.2}$$

¶ A differential is of the first kind if it has no poles.

† Alternatively, by a general theorem, the degree of the function field $k(\mathcal{D})$ over $k(X)$ is the degree of the divisor of poles of X, namely 2: and the rest is easy.

where G_j is homogeneous of degree j. On putting $V = UX$ in (2) and completing the square, (1) takes the form $\mathcal{C}: Y^2 = F(X)$ with

$$\begin{aligned} Y &= 2G_4(1,X)U + G_3(1,X), \\ F(X) &= G_3(1,X)^2 - 4G_2(1,X)G_4(1,X). \end{aligned} \tag{1.4.3}$$

This gives a birational correspondence between $\mathcal{C}$ and $\mathcal{D}$, the double point corresponding to the divisor

$$G_2(1,X) = 0, \quad Y = G_3(1,X) \tag{1.4.4}$$

on $\mathcal{C}$.

Conversely, an effective divisor $\mathfrak{A} \notin \mathfrak{O}$ of degree 2 on $\mathcal{C}$ is given by

$$H(X) = 0, \quad Y = M(X) \tag{1.4.5}$$

for some $H, M \in k[X]$ of degree 2 and $\leqslant 3$ respectively. Then $F(X) - M(X)^2$ is divisible by $H(X)$ and it is easy to reverse the process and to recover $\mathcal{D}$. Further, a homogeneous linear transformation of the coefficients U, V for $\mathcal{D}$ corresponds to a transformation (1.3) in the equation for $\mathcal{C}$.

Chapter 2

Construction of the jacobian

0 Introduction. In this chapter we construct the jacobian of a general curve of genus 2. A discussion of the group law is left until later. We do, however, discuss briefly the local behaviour.

1 Construction of a basis. The jacobian $J(\mathcal{C})$ is an algebraic variety whose points correspond to the elements of Pic^0. Classically it was obtained over $\mathbb{C}$ using complex-function theory, but we require an algebraic construction valid over any ground field. In the preceding chapter we identified Pic^0 with Pic^2. We thus have to take the symmetric product $\mathcal{C}^{(2)}$ of two copies of $\mathcal{C}$ and 'blow down'¶ the divisor $\mathfrak{O}$ on it consisting of the points $\{\mathfrak{x}, \bar{\mathfrak{x}}\}$.

Not every curve on a surface can be blown down: a theorem of Castelnuevo characterizes those which can. We do not need to check that his conditions are satisfied, since wiser people have already shown that the jacobian exists, at least over $\mathbb{C}$. To perform the blowing down we mimic one of the proofs of Castelnuevo's Theorem. Let

$$\mathfrak{X} = \{\mathfrak{x}, \mathfrak{u}\}, \tag{2.1.1}$$

where

$$\mathfrak{x} = (x, y), \ \mathfrak{u} = (u, v) \tag{2.1.2}$$

is a pair of generic points on $\mathcal{C}$. Then the divisor $\mathfrak{O}$ on $\mathcal{C}^{(2)}$ is given by $u = x, \ v = -y$. It turns out to be a good idea to consider functions of $\mathfrak{X}$ symmetric in $\mathfrak{x}$, $\mathfrak{u}$ which may have a pole of any order on $\mathfrak{O}$ and are large at worst like x^2u^2 at infinity, but have no other poles. Such functions are a linear space L (say) over k. The symmetric functions of x, u of order at most 2 are included, but there are others. The function

$$\alpha_0 = \frac{y - v}{x - u} \tag{2.1.3}$$

¶ For a brief discussion of blowing up and down and of Castelnuevo's Theorem see Appendix I to this chapter.

is symmetric and small enough at infinity. At the finite poles we must have $u = x$, so $v = \pm y$. But α_0 is clearly finite on the 'diagonal' $\mathfrak{u} = \mathfrak{x}$, so its only finite pole is $\mathfrak{O}$. Hence $\alpha_0 \in L$. The square ${\alpha_0}^2$ is too large at infinity, but by subtracting an appropriate polynomial in x, u, we obtain the element

$$\begin{aligned} \beta_0 &= \frac{F_0(x,u) - 2yv}{(x-u)^2}, \\ F_0 &= 2f_0 + f_1(x+u) + 2f_2xu + f_3xu(x+u) \\ &\quad + 2f_4x^2u^2 + f_5x^2u^2(x+u) + 2f_6x^3u^3 \end{aligned} \tag{2.1.4}$$

of L with a pole of order 2 along $\mathfrak{O}$.

Arguing along these lines we get the following 16 elements of L:

Double zero at $\mathfrak{O}$:

$$\rho = (x-u)^2. \tag{2.1.5}$$

Regular nonzero at $\mathfrak{O}$:

$$\sigma_0 = 1, \quad \sigma_1 = x+u, \quad \sigma_2 = xu, \quad \sigma_3 = xu(x+u), \quad \sigma_4 = (xu)^2. \tag{2.1.6}$$

Simple pole at $\mathfrak{O}$:

$$\alpha_j = \frac{u^j y - x^j v}{x-u} \quad (j = 0,1,2,3). \tag{2.1.7}$$

Double pole at $\mathfrak{O}$:

$$\beta_0 = \frac{F_0(x,u) - 2yv}{(x-u)^2}, \quad \beta_1 = \frac{F_1(x,u) - (x+u)yv}{(x-u)^2}, \quad \beta_2 = xu\beta_0, \tag{2.1.8}$$

where

$$\begin{aligned} F_0(x,u) &= 2f_0 + f_1(x+u) + 2f_2xu + f_3xu(x+u) \\ &\quad + 2f_4(xu)^2 + f_5(xu)^2(x+u) + 2f_6(xu)^3, \\ F_1(x,u) &= f_0(x+u) + 2f_1xu + f_2xu(x+u) + 2f_3(xu)^2 \\ &\quad + f_4(xu)^2(x+u) + 2f_5(xu)^3 + f_6(xu)^3(x+u). \end{aligned} \tag{2.1.9}$$

Triple pole at $\mathfrak{O}$:

$$\gamma_0 = \frac{G(x,u)y - G(u,x)v}{(x-u)^3}, \quad \gamma_1 = \frac{H(x,u)y - H(u,x)v}{(x-u)^3}, \tag{2.1.10}$$

where

$$\begin{aligned} G(x,u) &= 4f_0 + f_1(x+3u) + f_2(2xu+2u^2) + f_3(3xu^2+u^3) + 4f_4xu^3 \\ &\quad + f_5(x^2u^3 + 3xu^4) + f_6(2x^2u^4 + 2xu^5), \\ H(x,u) &= f_0(2x+2u) + f_1(3xu+u^2) + 4f_2xu^2 + f_3(x^2u^2 + 3xu^3) \\ &\quad + f_4(2x^2u^3 + 2xu^4) + f_5(3x^2u^4 + xu^5) + 4f_6x^2u^5. \end{aligned} \tag{2.1.11}$$

And, finally,
Quadruple pole at $\mathfrak{O}$:

$$\delta = {\beta_0}^2. \tag{2.1.12}$$

It is readily verified that the given functions have poles of the specified orders at $\mathfrak{O}$. It is enough to show that they are well defined at points of the diagonal $\mathfrak{X} = \{\mathfrak{x}, \mathfrak{x}\}$ not on $\mathfrak{O}$. For γ_0, for example, one checks that $G(x,u)^2F(x) - G(u,x)^2F(u)$ is divisible by $(x-u)^3$.

2 We have not proved that these 16 functions are a basis for L over k, but that will soon be apparent. We denote them in inverse order as $\{z_0, ..., z_{15}\}$ (so $z_0 = \delta$, $z_1 = \gamma_1$, $z_2 = \gamma_0$, ..., $z_{15} = \rho$). Anticipating its identification with the jacobian, we denote by $J(\mathcal{C})$ the projective locus¶ of $\mathbf{z} = (z_0, \ldots, z_{15})$ in $\mathbb{P}^{15}$. We show that the map from $\mathcal{C}^{(2)}$ to $J(\mathcal{C})$ is just the required blowdown: more precisely, that it is biregular outside $\mathfrak{O}$ but maps $\mathfrak{O}$ onto the single point $(1, 0, \ldots, 0)$. A divisor of the shape (1.1), (1.2) with $u \neq x$ is given by

$$\sigma_0 X^2 - \sigma_1 X + \sigma_2 = 0, \quad \sigma_0 Y = \alpha_0 X - \alpha_1; \tag{2.2.1}$$

which shows biregularity there. This extends to $u = x$, $v = y \neq 0$, on noting that there α_0, α_1 specialize to $F'(x)/2y$, $y + xF'(x)/2y$ respectively.

Finally, on dividing the projective coordinates by δ, it is easily seen that the $\mathfrak{X}$ with $u = x$, $v = -y$ (including $v = y = 0$) all go to

$$\mathbf{o} \text{ (say)} \quad = (1, 0, \ldots, 0). \tag{2.2.2}$$

Since the constructed basis behaves beautifully under the transformations induced by $X \mapsto X + \text{constant}$ and $X \mapsto X^{-1}$ (see Appendix II to this chapter), this completes the proof that $J(\mathcal{C})$ is indeed the jacobian of $\mathcal{C}$. Note that the diagonal gives an embedding of $\mathcal{C}$ in $J(\mathcal{C})$.

¶ By this is meant the projective variety defined as follows. Let $P(\mathbf{Z})$ run through the homogeneous polynomials, defined over k, in $\mathbf{Z} = (Z_0, \ldots, Z_{15})$ such that $P(\mathbf{z}) = 0$ when (x, y) and (u, v) are independent generic points of $\mathcal{C}$. The set $\mathcal{P}$ of such P is a graded ideal over $k[\mathbf{Z}]$. By Hilbert's Basissatz it has a finite basis over $k[\mathbf{Z}]$. The projective locus is the projective variety defined by the vanishing of the basis (and so of $\mathcal{P}$). In the case under discussion, a basis is given by the 72 quadratic polynomials introduced below.

We illustrate the definitions by the example

$$\mathcal{C}: \quad Y^2 = (X^2+1)(X^2+2)(X^2+X+1) \tag{2.2.3}$$

with $k = \mathbb{Q}$. As described in Chapter 1, the element $\mathfrak{A} = \{(i,0),(-i,0)\}$ of Pic^2 specifies an element of the jacobian: it is defined over $\mathbb{Q}$ [cf. discussion following (1.2.2)]. Substituting $x = i, y = 0, u = -i, v = 0$ into $(1.5),\dots,(1.12)$ gives

$$\mathbf{z}(\mathfrak{A}) = \big(z_i(\mathfrak{A})\big) = (36,0,0,-6,-3,-6,0,0,0,0,1,0,1,0,1,-4) \tag{2.2.4}$$

where $z_0,\dots z_{15}$ are as defined at the beginning of this section. Thus, $\{(i,0),(-i,0)\}$ and the right hand side of (4) represent the same member of J. Similarly $\{\infty^+,\infty^+\}$ corresponds to

$$(225,-18,-60,-60,-8,0,-8,16,0,0,16,0,0,0,0,0), \tag{2.2.5}$$

where ∞^+ is the point at infinity for which $Y/X^3 = 1$.

3 Local behaviour. We now consider more closely the behaviour of the basis elements in the neighbourhood of $\mathfrak{O}$, say at

$$u = x + h, \quad v \approx -y, \tag{2.3.1}$$

where h is small and $y \neq 0$. It is easy to deduce from the formulae for the base elements that

$$\begin{array}{ccccccccc}
 & & & & \rho \approx h^2 & & & & \\
\sigma_0 \approx 1 & & \sigma_1 \approx 2x & & \sigma_2 \approx x^2 & & \sigma_3 \approx 2x^3 & & \sigma_4 \approx x^4 \\
 & \alpha_0 \approx \frac{2y}{h} & & \alpha_1 \approx \frac{2xy}{h} & & \alpha_2 \approx \frac{2x^2y}{h} & & \alpha_3 \approx \frac{2x^3y}{h} & \\
 & & \beta_0 \approx \frac{4y^2}{h^2} & & \beta_1 \approx \frac{4xy^2}{h^2} & & \beta_2 \approx \frac{4x^2y^2}{h^2} & & \\
 & & & \gamma_0 \approx \frac{8y^3}{h^3} & & \gamma_1 \approx \frac{8xy^3}{h^3} & & & \\
 & & & & \delta \approx \frac{16y^4}{h^4} & & & &
\end{array} \tag{2.3.2}$$

Locally, one normalizes to $\delta = 1$. Put

$$\lambda = \frac{\gamma_0}{\delta} \approx \frac{h}{2y}, \quad \mu = \frac{\gamma_1}{\delta} \approx \frac{xh}{2y}. \tag{2.3.3}$$

Then

$$\begin{gathered}\frac{\beta_0}{\delta} \approx \lambda^2 \qquad \frac{\beta_1}{\delta} \approx \lambda\mu \qquad \frac{\beta_2}{\delta} \approx \mu^2 \\ \frac{\alpha_0}{\delta} \approx \lambda^3 \qquad \frac{\alpha_1}{\delta} \approx \lambda^2\mu \qquad \frac{\alpha_2}{\delta} \approx \lambda\mu^2 \qquad \frac{\alpha_3}{\delta} \approx \mu^3 \\ \frac{\sigma_0}{\delta} \approx \lambda^4 \qquad \frac{\sigma_1}{\delta} \approx 2\lambda^3\mu \qquad \frac{\sigma_2}{\delta} \approx \lambda^2\mu^2 \qquad \frac{\sigma_3}{\delta} \approx 2\lambda\mu^3 \qquad \frac{\sigma_4}{\delta} \approx \mu^4 \end{gathered} \tag{2.3.4}$$

and

$$\frac{\rho}{\delta} \approx \frac{h^6}{16y^4} = \frac{h^6F(x)}{16y^6} \approx 4\sum_{j=0}^{6} f_j\lambda^{6-j}\mu^j \tag{2.3.5}$$

Using the local behaviour, one can determine a basis for the quadratic relations between the base elements: for example ${\alpha_0}^2$ and $\beta_0\sigma_0$ have the same dominant term λ^6, so their difference must be expressible in terms of 'smaller' products. The reader can verify that in fact

$$\begin{aligned} &z_9^2 - z_5z_{14} - f_2z_{14}^2 - f_3z_{14}z_{13} - f_4z_{13}^2 - 3f_5z_{13}z_{12} \\ &- f_5z_{13}z_{15} - f_6z_{14}z_{10} - 6f_6z_{12}z_{15} - 8f_6z_{12}^2 - f_6z_{15}^2 = 0, \end{aligned} \tag{2.3.6}$$

where $z_0, \ldots, z_{15}$ are as defined at the beginning of Section 2.

It turns out that the set of quadratic relations has dimension 72 over k. Hence $L^{\otimes 2}$ has dimension $\binom{16+1}{2} - 72 = 64$ in accordance with the classical theory. The jacobian is given by the quadratic relations, in conformity with a theorem of Mumford (1966, I) about the defining equations of abelian varieties. We have made a basis for the quadratic relations (and so a set of defining equations for the jacobian) available by anonymous ftp, as explained in Appendix II at the end of the book. Those familiar with the classical theory will also note the similarity between the form of the *local parameters* λ, μ, and the fact that $\mathrm{d}X/Y$ and $X\mathrm{d}X/Y$ are a basis of the differentials of the first kind on $\mathcal{C}$. For details see Flynn (1990a).¶

4 Formal group law. We leave the derivation of the group law on the jacobian until the end of Chapter 3. The corresponding formal group is discussed fully in Chapter 7, but we introduce it briefly here. This section may be omitted in a first reading.

¶ The notation in Flynn's earlier papers differs from that of these prolegomena. Apart from the use of different symbols, the main difference is that they have $x^2 + u^2$ as a basis element instead of $\rho = (x - u)^2$. The files available by ftp use the notation introduced here.