THE INVARIANTS OF A GENUS ONE CURVE

TOM FISHER

Abstract. It was first pointed out by Weil [26] that we can use classical invariant theory to compute the Jacobian of a genus one curve. The invariants required for curves of degree $n = 2, 3, 4$ were already known to the nineteenth centuary invariant theorists. We have succeeded in extending these methods to curves of degree $n = 5$, where although the invariants are too large to write down as explicit polynomials, we have found a practical algorithm for evaluating them.

1. Introduction

We work throughout over a perfect field K with algebraic closure $\overline{K}$. In this introduction we further assume that char$\,(K) \neq 2, 3$. Let C be a smooth curve of genus one defined over K and let D be a K-rational divisor on C of degree n. If $n = 1$ then $C(K) \neq \emptyset$, and C is defined by a Weierstrass equation. If $n \geq 2$ then the complete linear system $|D|$ defines a morphism $C \to \mathbb{P}^{n-1}$. If $n \geq 3$ then this morphism is an embedding and we call the image a genus one normal curve of degree n. For $n \leq 5$ the pair (C, D) is described by data of the following form.

Definition 1.1. A genus one model of degree $n = 1, 2, 3, 4, 5$ is
(i) if $n = 1$ a Weierstrass equation
(ii) if $n = 2$ a binary quartic
(iii) if $n = 3$ a ternary cubic
(iv) if $n = 4$ a pair of quadrics in 4 variables
(v) if $n = 5$ a 5×5 alternating matrix of linear forms in 5 variables.

The equations defined by a genus one model of degree 5 are the 4×4 Pfaffians of the matrix. It is a classical fact that every genus one normal quintic is defined by equations of this form. An algorithm for computing these matrices is given in [12], based on the Buchsbaum-Eisenbud structure theorem [5], [6] for Gorenstein ideals of codimension 3.

We write X_n for the (affine) space of all genus one models of degree n and $K[X_n]$ for its co-ordinate ring. In §4 we specify a linear algebraic group G_n acting on X_n. In each case we find that the ring of invariants

Date: 9th October 2006.

$K[X_n]^{G_n}$ is a polynomial ring in two variables. (This could be deduced by a theorem of Kempf [18, Theorem 2.4] if char $(K) = 0$.) We label the generators c_4 and c_6. In the case $n = 1$ these are the usual polynomials defined in [24, Chapter III]. In the cases $n = 2, 3, 4, 5$ we find that c_4 and c_6 are homogeneous polynomials of degree $4n/(6 - n)$ and $6n/(6 - n)$. Moreover, as first pointed out by Weil [26] in the case $n = 2$, the invariants c_4 and c_6 give a formula for the Jacobian. The invariants for $n = 2, 3, 4$ have been known since the nineteenth century, and are surveyed in [1].

Our work has two main goals. The first is to describe the ring of invariants in a way that emphasises the similarities between the cases $n = 1, 2, 3, 4, 5$. The second is to give practical methods for evaluating the invariants. In both instances our main original contribution is in the case $n = 5$.

A relatively easy argument (reduction to the case $n = 1$) shows that if invariants c_4 and c_6 of the expected degrees exist then they generate the ring of invariants. In the cases $n = 2, 3$ the existence of these invariants is settled by writing them down as explicit polynomials. In the case $n = 4$ there is a classical trick for reducing to the case $n = 2$. But in the case $n = 5$ the invariants are too large to write down as explicit polynomials. This makes it difficult to show they exist.

One of the tools of classical invariant theory is the so-called symbolic notation, as described in [14]. This is an extremely compact notation for specifying invariants. For example in the case $n = 3$ the invariants may be written (see [22, §§220,221] or [25, §4.5])

$$\begin{aligned} c_4 &= 54 \times (abc)(bcd)(cda)(dab) \\ c_6 &= 972 \times (abc)(abd)(bce)(caf)(def)^2. \end{aligned}$$

By introducing non-commuting symbols it is possible to write down similar expressions in the case $n = 5$. But we have no way of showing these invariants are non-zero without expanding them as explicit polynomials. As remarked above, this is not feasible.

In principle we could use the representation theory of Lie algebras, specifically the Weyl character formula, to compute the dimension of the vector space of invariants of any given degree. For details in the case $n = 3$ we refer to [13, Exercise 13.20] or [25, §4.4]. Unfortunately, when we tried this approach in the case $n = 5$, we were again defeated by combinatorial explosion.

The plan of the paper is as follows. In §2 we explain the role played by the invariant differential in computing the Jacobian of a genus one curve. In §3 we revisit and motivate our definition of a genus one model.

Notice that we modify the definition in the case $n = 2$ to accommodate fields of characteristic 2.

In §4 we study the ring of invariants. We show that it is generated by invariants c_4 and c_6 of the expected degrees and that these invariants give a formula for the Jacobian. We also show (in all characteristics) that a genus one model defines a smooth curve of genus one if and only if its discriminant $\Delta = (c_4^3 - c_6^2)/1728$ is non-zero. The proofs rely on geometric results proved in §5 and formulae recorded in §6.

In §7 we recall some classical methods for computing the invariants in the cases $n = 2, 3, 4$. These formulae have already been surveyed in [1], but are included here to demonstrate our preferred choice of scalings. In the case $n = 5$ we have found an algorithm for evaluating the invariants. Our algorithm, presented in §8, is inspired by the methods of nineteenth century invariant theory, in that we approach the invariants through the construction of certain covariants. The key step relies on a geometric "accident" satisfied by the secant variety of a genus one normal quintic. In §9 we compare our invariant-theoretic approach with some other methods for computing the Jacobian of a genus one curve.

Finally in §10 we include a brief note on the invariants in characteristics 2 and 3. We find in these cases that the invariants are insufficient to compute the Jacobian. Instead it should be possible to find a formula for the Jacobian that works in all characteristics by modifying the formulae in characteristic 0. This has been carried out by Artin, Rodriguez-Villegas and Tate [3] in the case $n = 3$.

The formulae and algorithms presented in §§7,8 have been contributed to MAGMA [19, Version 2.13] by the author.

2. Geometric Invariants

Let C be a smooth curve of genus one defined over K, and let ω be a non-zero regular 1-form on C, also defined over K. We say that ω is an invariant differential. Over $\overline{K}$, the pair (C, ω) may be put in the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with $\omega = dx/(2y + a_1x + a_3)$.

Definition 2.1. The geometric invariants of the pair (C, ω) are

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned}$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$.

It is clear from the formulae in [24, Chapter III] that c_4 and c_6 depend only on the pair (C, ω) and not on the choice of Weierstrass equation (1). We deduce by Galois theory that $c_4, c_6 \in K$.

Lemma 2.2. *If (C, ω) has geometric invariants c_4 and c_6, and $\lambda \in K^*$, then $(C, \lambda^{-1}\omega)$ has geometric invariants $\lambda^4 c_4$ and $\lambda^6 c_6$.*

Proof: This is again clear from [24, Chapter III]. □

We show in §5.4 that if a genus one model of degree n defines a smooth curve of genus one, then it also defines an invariant differential on the curve. This enables us to construct the invariants $c_4, c_6 \in K[X_n]^{G_n}$ as the geometric invariants of the generic genus one model of degree n. In particular we treat the cases $n = 2, 3, 4, 5$ in a uniform manner, and avoid the problem of combinatorial explosion in the case $n = 5$.

The geometric invariants give a formula for the Jacobian.

Proposition 2.3. *Assume* $\operatorname{char}(K) \neq 2, 3$. *If (C, ω) has geometric invariants c_4 and c_6 then C has Jacobian*

$$y^2 = x^3 - 27c_4x - 54c_6.$$

The proof relies on two easy lemmas.

Lemma 2.4. *Assume* $\operatorname{char}(K) \neq 2, 3$. *Let E be an elliptic curve defined over K with invariant differential ω. Let α be an automorphism of E. Then α is a translation map if and only if $\alpha^*\omega = \omega$.*

Proof: We write $\tau_P : E \to E$ for translation by $P \in E$. The map $P \mapsto \tau_P^*(\omega)/\omega$ is a morphism $E \to \mathbb{G}_m$. It must therefore be constant. Specialising to $P = 0$ we deduce that $\tau_P^*(\omega) = \omega$ for all $P \in E$. (An alternative proof is given by writing τ_P as the commutator of τ_Q and $[-1]$ where $2Q = P$.)

Conversely if α is not a translation then $\alpha - 1$ is not constant, and therefore surjective. So α has a fixed point. Conjugating by a translation, we may suppose that the fixed point is $0 \in E$. Since $\operatorname{char}(K) \neq 2, 3$ we can put E in shorter Weierstrass form $y^2 = x^3 + Ax + B$. Then the only automorphisms of $(E, 0)$ are of the form $(x, y) \mapsto (u^2x, u^3y)$. Since ω is a multiple of dx/y the result is now clear. □

Lemma 2.5. *Assume* $\operatorname{char}(K) \neq 2, 3$. *Let E be an elliptic curve and C a smooth curve of genus one, both defined over K. Let ω_E and ω_C be invariant differentials on E and C, also defined over K. If there is an isomorphism $\alpha : C \cong E$ defined over $\overline{K}$ with $\alpha^*\omega_E = \omega_C$ then E is the Jacobian of C.*

PROOF: Let $\xi_\sigma = \sigma(\alpha)\alpha^{-1}$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Since ω_E and ω_C are both K-rational we deduce that $\xi_\sigma^* \omega_E = \omega_E$. It follows by Lemma 2.4 that ξ_σ is a translation. So C is the twist of E by the class of $\{\xi_\sigma\}$ in $H^1(K,E)$. In particular C is a torsor under E, the action $\mu : E \times C \to C$ being given by

$$\mu(P,Q) = \alpha(P + \alpha^{-1}Q).$$

It follows that E is the Jacobian of C. □

PROOF OF PROPOSITION 2.3: We are given (C,ω) with geometric invariants c_4 and c_6. Let E be the elliptic curve over K with Weierstrass equation

$$y^2 = x^3 - 27c_4 x - 54c_6.$$

The pairs (C,ω) and $(E, 3dx/y)$ have the same geometric invariants, and are therefore isomorphic over $\overline{K}$. It follows by Lemma 2.5 that E is the Jacobian of C. □

Before we can use Proposition 2.3 to compute the Jacobian of a genus one curve, we first need to compute an invariant differential on the curve. It is easy to generalise the construction of §5.4 to genus one normal curves of arbitrary degree. An alternative is the following.

Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree n with hyperplane section H. We identify the Riemann-Roch space $\mathcal{L}(H)$ with the space of linear forms on $\mathbb{P}^{n-1}$. If we fix ω then there is a linear map

$$\wedge^2 \mathcal{L}(H) \to \mathcal{L}(2H)\,; \quad f \wedge g \mapsto \tfrac{fdg - gdf}{\omega}.$$

By Lemma 5.5 with $d = 2$ the natural map $S^2\mathcal{L}(H) \to \mathcal{L}(2H)$ is surjective. Thus there is an alternating matrix of quadrics $\Omega = (\Omega_{ij})$ with

$$\omega = \tfrac{x_j^2 d(x_i/x_j)}{\Omega_{ij}}$$

for all $i \neq j$. This matrix has the property that

$$\begin{pmatrix} \frac{\partial f}{\partial x_1} & \cdots & \frac{\partial f}{\partial x_n} \end{pmatrix} \Omega \equiv 0 \pmod{I(C)}$$

for all $f \in I(C)$. Starting from generators for $I(C)$ we can use this property to solve for Ω by linear algebra. Then Ω is the data we use to specify ω. Notice that the entries of Ω are determined only up to the addition of quadrics in $I(C)$.

In §9 we compare our invariant-theoretic approach with some other methods for computing the geometric invariants.

3. Genus one models

Let C be a smooth curve of genus one defined over K, and let D be a K-rational divisor on C of degree n. In each of the cases $n = 1, 2, 3, 4, 5$ we find equations for the pair (C, D), and use the form of these equations to motivate our definition of a genus one model.

3.1. **Genus one models of degree 1.** If $n = 1$ then we pick $x, y \in K(C)$ such that $\mathcal{L}(2D)$ and $\mathcal{L}(3D)$ have bases $1, x$ and $1, x, y$. The 7 elements $1, x, y, x^2, xy, x^3, y^2$ in the 6-dimensional space $\mathcal{L}(6D)$ satisfy a linear dependence relation. Moreover the coefficients of x^3 and y^2 are non-zero. Rescaling x and y if necessary we find that C has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

A genus one model of degree 1 is a tuple $\phi = (a_1, a_2, a_3, a_4, a_6)$. We write $C_\phi \subset \mathbb{P}^2$ for the curve with Weierstrass equation (2). Genus one models ϕ and ϕ' of degree 1 are equivalent if they are related by substitutions

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

and $\phi' = u^{-6}\phi$, with $u \neq 0$. We write $\mathcal{G}_1$ for the group of all such transformations $[u; r, s, t]$.

3.2. **Genus one models of degree 2.** If $n = 2$ then we pick $x, y \in K(C)$ such that $\mathcal{L}(D)$ and $\mathcal{L}(2D)$ have bases $1, x$ and $1, x, y, x^2$. The 9 elements $1, x, x^2, y, x^3, xy, x^4, x^2y, y^2$ in the 8-dimensional space $\mathcal{L}(4D)$ satisfy a linear dependence relation. Moreover the coefficient of y^2 is non-zero. We find that C has equation

$$y^2 + (\alpha_0x^2 + \alpha_1x + \alpha_2)y = ax^4 + bx^3 + cx^2 + dx + e.$$

A genus one model of degree 2 is a pair of homogeneous polynomials $\phi = (p(x, z), q(x, z))$ of degrees 2 and 4. We write $C_\phi \subset \mathbb{P}(1, 1, 2)$ for the curve defined by

$$y^2 + p(x, z)y = q(x, z).$$

Here the ambient space $\mathbb{P}(1, 1, 2)$ is a weighted project plane, with degrees $1, 1, 2$ assigned to the co-ordinates x, z, y. Genus one models ϕ and ϕ' of degree 2 are equivalent if they are related by substitutions

$$\begin{aligned} x &= B_{11}x' + B_{21}z' \\ z &= B_{12}x' + B_{22}z' \\ y &= \mu^{-1}y' + r_0x'^2 + r_1x'z' + r_2z'^2 \end{aligned}$$

and $\phi' = \mu^2\phi$, with $\mu \det B \neq 0$. We write $\mathcal{G}_2$ for the group of all such transformations $[\mu, r, B]$.

If $\operatorname{char}(K) \neq 2$ then by completing the square it suffices to consider models of the form $(0, q(x,z))$. These are the binary quartics of Definition 1.1.

If $n \geq 3$ then the complete linear system $|D|$ determines an embedding $C \to \mathbb{P}^{n-1}$. We identify C with its image, which is called a genus one normal curve of degree n. Some basic facts about these curves are recalled in §5.1.

3.3. **Genus one models of degree 3.** If $n = 3$ then $C \subset \mathbb{P}^2$ is a plane cubic. A genus one model of degree 3 is a single homogeneous polynomial $\phi = (f(x_1, x_2, x_3))$ of degree 3. We write $C_\phi \subset \mathbb{P}^2$ for the variety defined by $f = 0$. Genus one models ϕ and ϕ' of degree 3 are equivalent if they are related by substitutions $\phi' = \mu\phi$ and $x_j = \sum_{i=1}^3 B_{ij} x'_i$ with $\mu \det B \neq 0$. We write $\mathcal{G}_3 = \mathbb{G}_m \times \mathrm{GL}_3$ for the group of all such transformations.

3.4. **Genus one models of degree 4.** If $n = 4$ then $C \subset \mathbb{P}^3$ is the complete intersection of two quadrics. A genus one model of degree 4 is a pair of homogeneous polynomials

$$\phi = \begin{pmatrix} q_1(x_1, x_2, x_3, x_4) \\ q_2(x_1, x_2, x_3, x_4) \end{pmatrix}$$

of degree 2. We write $C_\phi \subset \mathbb{P}^3$ for the variety defined by $q_1 = q_2 = 0$. Genus one models ϕ and ϕ' of degree 4 are equivalent if they are related by substitutions $\phi' = A\phi$ and $x_j = \sum_{i=1}^4 B_{ij} x'_i$ with $\det A \det B \neq 0$. We write $\mathcal{G}_4 = \mathrm{GL}_2 \times \mathrm{GL}_4$ for the group of all such transformations.

3.5. **Genus one models of degree 5.** If $n = 5$ then $C \subset \mathbb{P}^4$ is defined by the 4×4 Pfaffians of a 5×5 alternating matrix of linear forms. (See for example [12] and the references cited there.) A genus one model of degree 5 is a 5×5 alternating matrix of linear forms in 5 variables. We write $C_\phi \subset \mathbb{P}^4$ for the variety defined by its 4×4 Pfaffians. Genus one models ϕ and ϕ' of degree 5 are equivalent if they are related by substitutions $\phi' = A\phi A^T$ and $x_j = \sum_{i=1}^4 B_{ij} x'_i$ with $\det A \det B \neq 0$. We write $\mathcal{G}_5 = \mathrm{GL}_5 \times \mathrm{GL}_5$ for the group of all such transformations.

4. The ring of invariants

Let X_n be the space of genus one models of degree n. For $n = 1, 2, 3, 4, 5$ this is an affine space of dimension $N = 5, 8, 10, 20, 50$. The co-ordinate ring $K[X_n]$ is a polynomial ring in N variables. For $n =$

$3, 4, 5$ we give this ring its usual grading by degree. In the cases $n = 1, 2$ the rings are

$$\begin{array}{rcl} K[X_1] & = & K[a_1, a_2, a_3, a_4, a_6] \\ K[X_2] & = & K[\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e]. \end{array}$$

We assign degrees $\deg(a_i) = i$, $\deg(\alpha_i) = 1$, $\deg(a) = \ldots = \deg(e) = 2$. In §3 we defined a linear algebraic group $\mathcal{G}_n$ acting on X_n. We now write G_n for the commutator subgroup, *i.e.*

$$\begin{array}{rcl} G_1 & = & \{[1; r, s, t] \in \mathcal{G}_1\} \\ G_2 & = & \{[1, r, B] \in \mathcal{G}_2 : B \in \mathrm{SL}_2\} \\ G_3 & = & \mathrm{SL}_3 \\ G_4 & = & \mathrm{SL}_2 \times \mathrm{SL}_4 \\ G_5 & = & \mathrm{SL}_5 \times \mathrm{SL}_5. \end{array}$$

Definition 4.1. The ring of invariants is

$$K[X_n]^{G_n} = \{F \in K[X_n] : F \circ g = F \text{ for all } g \in G_n(\overline{K})\}.$$

The definition is extended to an integral domain R by putting

$$R[X_n]^{G_n} = R[X_n] \cap K[X_n]^{G_n}.$$

where K is the field of fractions of R.

We define a rational character $\det : \mathcal{G}_n \to \mathbb{G}_m$

$$\begin{array}{lrcl} n = 1 & [u; r, s, t] & \mapsto & u^{-1} \\ n = 2 & [\mu, r, B] & \mapsto & \mu \det B \\ n = 3 & [\mu, B] & \mapsto & \mu \det B \\ n = 4 & [A, B] & \mapsto & \det A \det B \\ n = 5 & [A, B] & \mapsto & (\det A)^2 \det B. \end{array}$$

Definition 4.2. The vector space of invariants of weight k is

$$K[X_n]^{G_n}_k = \{F \in K[X_n] : F \circ g = (\det g)^k F \text{ for all } g \in \mathcal{G}_n(\overline{K})\}.$$

Lemma 4.3. *Every homogeneous invariant of degree d is an invariant of weight k where*

$$d = \begin{cases} k & \textit{if } n = 1, 2, 3 \\ 2k & \textit{if } n = 4 \\ 5k & \textit{if } n = 5. \end{cases}$$

In particular the ring of invariants is graded by weight, i.e.

$$K[X_n]^{G_n} = \oplus_{k \geq 0} K[X_n]^{G_n}_k.$$

Proof: We treat the cases $n = 4, 5$. Since the only rational characters of $\mathcal{G}_n$ are of the form $[A, B] \mapsto (\det A)^p (\det B)^q$ we have

$$F \circ [A, B] = (\det A)^p (\det B)^q F$$

for some integers p, q. Considering $[A, B]$ in the centre of $\mathcal{G}_n$ we deduce

$$n = 4 \quad \left\{ \begin{array}{rcl} d & = & 2p \\ 2d & = & 4q \end{array} \right.$$
$$n = 5 \quad \left\{ \begin{array}{rcl} 2d & = & 5p \\ d & = & 5q \end{array} \right.$$

We are done by the definition of $\det : \mathcal{G}_n \to \mathbb{G}_m$. The cases $n = 1, 2, 3$ are similar. □

We are ready to state our main theorem.

Theorem 4.4. *There are invariants $c_4, c_6, \Delta \in K[X_n]^{G_n}$ of weights* 4, 6 *and* 12, *related by $c_4^3 - c_6^2 = 1728\Delta$, such that*
(i) If $\operatorname{char}(K) \neq 2, 3$ *then $K[X_n]^{G_n} = K[c_4, c_6]$.*
(ii) The variety C_ϕ defined by $\phi \in X_n$ is a smooth curve of genus one if and only if $\Delta(\phi) \neq 0$.
(iii) If $\operatorname{char}(K) \neq 2, 3$ *and $\phi \in X_n$ with $\Delta(\phi) \neq 0$ then C_ϕ has Jacobian*

$$y^2 = x^3 - 27c_4(\phi)x - 54c_6(\phi).$$

The proof depends on the following geometric statements.

Proposition 4.5. *Assume $K = \overline{K}$. Let X_n^{sing} be the set of all models $\phi \in X_n$ which do not define a smooth curve of genus one. Then X_n^{sing} is an irreducible Zariski closed subset of X_n. In particular the generic genus one model of degree n defines a smooth curve of genus one.*

Proof: The cases $n = 1, 2, 3$ are well known. A proof for $n = 3, 4, 5$ is given in §5.3. □

Let $\mathbb{P}(X_n)$ be the projective space determined by X_n. (This is a weighted projective space in the cases $n = 1, 2$.) We recall that elements of X_n are equivalent if they lie in the same $\mathcal{G}_n$-orbit.

Proposition 4.6. *Assume $K = \overline{K}$. Let $\phi, \phi' \in X_n$ with C_ϕ and $C_{\phi'}$ either smooth curves of genus one or rational curves with a single node. Then C_ϕ and $C_{\phi'}$ are isomorphic as curves if and only if ϕ and ϕ' are equivalent. Moreover the stabiliser of ϕ for the action of G_n on $\mathbb{P}(X_n)$ is finite.*

Proof: The cases $n = 1, 2$ are straightforward. A proof for $n = 3, 4, 5$ is given in §5.2. □

We identify $K[X_n]^{G_n}$ as a subring of $K[X_1]^{G_1}$. To do this we start with an elliptic curve E in Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The complete linear system $|n.0|$ determines a morphism $E \to \mathbb{P}^{n-1}$. The image is described by a genus one model of degree n. In §6 we specify such a model and hence define a morphism $\pi_n : X_1 \to X_n$. The models $\pi_n(\phi)$ for $\phi \in X_1$ are called Weierstrass models. Collectively they form the Weierstrass family.

Proposition 4.7. *There are morphisms $\pi_n : X_1 \to X_n$ and $\gamma_n : \mathcal{G}_1 \to \mathcal{G}_n$ with the following properties.*
(i) If $\phi' = \pi_n(\phi)$ then C_ϕ and $C_{\phi'}$ are isomorphic as curves.
(ii) γ_n is a group homomorphism.
(iii) $(\gamma_n g)(\pi_n \phi) = \pi_n(g\phi)$ for all $g \in \mathcal{G}_1$ and $\phi \in X_1$.
(iv) $\det(\gamma_n g) = \det(g)$ for all $g \in \mathcal{G}_1$.

Proof: The proposition is checked by direct computation using the formulae in §6. □

The map $\pi_n : X_1 \to X_n$ induces a homomorphism of polynomial rings $\pi_n^* : K[X_n] \to K[X_1]\,;\, F \mapsto F \circ \pi_n$. By Proposition 4.7 it restricts to a homomorphism of graded rings

$$\pi_n^* : K[X_n]^{G_n} \to K[X_1]^{G_1}$$

where the grading is by weight.

Lemma 4.8. *The map $\pi_n^* : K[X_n]^{G_n} \to K[X_1]^{G_1}$ is an injective homomorphism of graded rings.*

Proof: We must show that π_n^* is injective. For this we are free to assume that K is algebraically closed. If $F \in K[X_n]^{G_n}$ is a homogeneous invariant vanishing on the Weierstrass family then by Propositions 4.6 and 4.7 it also vanishes at every $\phi \in X_n$ for which C_ϕ is a smooth curve of genus one. Proposition 4.5 tells us that the latter are Zariski dense in X_n. It follows that F is identically zero and hence π_n^* is injective. □

Computing the ring $K[X_1]^{G_1}$ is entirely routine. We recall that

$$K[X_1] = K[a_1, a_2, a_3, a_4, a_6].$$

Following Tate's formulaire [24, Chapter III] we put

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned} \tag{3}$$

and

$$\begin{array}{rcl} c_4 & = & b_2^2 - 24b_4 \\ c_6 & = & -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta & = & -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{array} \tag{4}$$

It is well known that $c_4, c_6, \Delta \in \mathbb{Z}[X_1]^{G_1}$ and $c_4^3 - c_6^2 = 1728\Delta$.

Lemma 4.9. *If* $\mathrm{char}\,(K) \neq 2, 3$ *then* $K[X_1]^{G_1} = K[c_4, c_6]$.

PROOF: This is Theorem 4.4(i) in the case $n = 1$. It is an immediate consequence of the standard procedure for putting a Weierstrass equation in the shorter form $y^2 = x^3 + Ax + B$. The required isomorphism is ι^* where

$$\iota : \mathbb{A}^2 \to X_1 \,; \quad (c_4, c_6) \mapsto (0, 0, 0, -c_4/48, -c_6/864).$$

□

We have reduced the proof of Theorem 4.4(i) to showing that π_n^* is surjective. Equivalently, we must show that $K[X_n]^{G_n}$ contains invariants of weights 4 and 6. One method would be to split into the cases $n = 2, 3, 4, 5$ and use the explicit constructions presented in §§7,8. This makes the theorem appear an accident, especially in the case $n = 5$. Instead we give a construction based on Proposition 4.6.

Lemma 4.10. *Assume* $K = \overline{K}$. *Let* $\phi, \phi' \in X_n$ *with* C_ϕ *and* $C_{\phi'}$ *either smooth curves of genus one or rational curves with a single node. Then the Zariski closure of the* $\mathcal{G}_n$*-orbit of* ϕ *is the zero locus of an irreducible homogeneous invariant* $F \in K[X_n]^{\mathcal{G}_n}$. *Moreover* $F(\phi') = 0$ *if and only if* ϕ *and* ϕ' *are equivalent.*

PROOF: By Proposition 4.6 the morphism $G_n \to \mathbb{P}(X_n)$; $g \mapsto g(\phi)$ has zero-dimensional fibres. But for each n we find

$$\dim(G_n) = \dim(X_n) - 2.$$

So the G_n-orbit of ϕ in $\mathbb{P}(X_n)$ has codimension 1. Moreover since G_n is irreducible, every G_n-orbit is irreducible. Therefore the Zariski closure of the orbit of ϕ is the zero locus of an irreducible homogeneous polynomial $F \in K[X_n]$. Since the equivalence class of ϕ determines F uniquely up to scalars, and G_n is the commutator subgroup of $\mathcal{G}_n$, it follows that F is an invariant.

If ϕ and ϕ' are equivalent then clearly $F(\phi') = 0$. For the converse we suppose $F(\phi') = 0$. Then the G_n-orbits of ϕ and ϕ' in $\mathbb{P}(X_n)$ have the same Zariski closure, Z say. A standard argument (see e.g. [23, Chapter I, §5.3, Theorem 6]) shows that each of these orbits contains a non-empty open subset of Z. Since Z is irreducible these open sets must intersect. It follows that ϕ and ϕ' are equivalent. □

We restrict these invariants to the Weierstrass family.

Lemma 4.11. *Assume* $K = \overline{K}$ *and* char $(K) \neq 2, 3$. *Then there are irreducible invariants* $F_4, F_6 \in K[X_n]^{G_n}$ *and integers* $p, q \geq 1$ *such that* $F_4 \circ \pi_n = c_4^p$ *and* $F_6 \circ \pi_n = c_6^q$.

Proof: By Proposition 4.7 we can pick $\phi \in X_n$ with C_ϕ a smooth curve of genus one with j-invariant 0. Let $F_4 \in K[X_n]^{G_n}$ be the invariant constructed from ϕ in Lemma 4.10. Then $F_4 \circ \pi_n$ is a homogeneous element of $K[X_1]^{G_1} = K[c_4, c_6]$. Rescaling F_4 we can write

$$F_4 \circ \pi_n = c_4^p \; c_6^q \; \Delta^r \prod_{\nu=1}^{s} (c_4^3 - j_\nu \Delta)$$

for some integers $p, q, r, s \geq 0$ and constants $j_1, \ldots j_s \neq 0, 1728$.

Now let $\phi' = \pi_n(\phi_1)$ be a Weierstrass model with $C_{\phi'}$ a smooth curve of genus one. If this curve has j-invariant not equal to 0 then by Lemma 4.10 we have $F_4(\phi') \neq 0$. By varying the choice of ϕ_1 we deduce that $q = s = 0$. We then repeat the argument for $C_{\phi'}$ a Weierstrass model with a node. This shows that $r = 0$. The statement for c_6 is proved similarly, starting with j-invariant 1728. □

The proof of Theorem 4.4(i) now reduces to showing that $p = q = 1$ in Lemma 4.11. For this we quote a geometric result whose proof uses properties of the invariant differential.

Definition 4.12. Genus one models $\phi, \phi' \in X_n$ are properly equivalent if there exists $g \in \mathcal{G}_n$ with $g\phi = \phi'$ and $\det(g) = 1$.

Proposition 4.13. *Assume* $K = \overline{K}$ *and* char $(K) \neq 2, 3$. *Let* $\phi \in X_n$ *with* C_ϕ *a smooth curve of genus one. Then* ϕ *is properly equivalent to* $\pi_n(0, 0, 0, A, B)$ *for some unique* $A, B \in K$.

Proof: The existence is already clear from Propositions 4.6 and 4.7. We prove uniqueness in §5.4. □

Lemma 4.14. *Assume* $K = \overline{K}$ *and* char $(K) = 0$. *Then the map* $\pi_n^* : K[X_n]^{G_n} \to K[X_1]^{G_1}$ *is surjective.*

Proof: Let $\phi \in X_n(\mathbb{K})$ be the generic model defined over the function field $\mathbb{K} = K(X_n)$. We have assumed char $(K) = 0$ so that $\mathbb{K}$ is perfect. Proposition 4.5 tells us that C_ϕ is a smooth curve of genus one. So by Proposition 4.13, ϕ is properly equivalent to $\pi_n(0, 0, 0, A, B)$ for some unique $A, B \in \overline{\mathbb{K}}$. The uniquess statement shows that A and B are fixed by Gal$(\overline{\mathbb{K}}/\mathbb{K})$ and hence $A, B \in \mathbb{K}$.

Let $F_4, F_6 \in K[X_n]^{G_n}$ be the irreducible invariants constructed in Lemma 4.11. Then $F_4 = f_4^p$ and $F_6 = f_6^q$ where

$$\begin{array}{rclcl} f_4 & = & c_4(0,0,0,A,B) & = & -48A \\ f_6 & = & c_6(0,0,0,A,B) & = & -864B. \end{array}$$

Since $K[X_n]$ is integrally closed (in its field of fractions $\mathbb{K}$) and F_4, $F_6 \in K[X_n]$ are irreducible it follows that $p = q = 1$. □

Applying Lemma 4.14 with $K = \overline{\mathbb{Q}}$ we learn that the invariants $c_4, c_6, \Delta \in \mathbb{Z}[X_1]^{G_1}$ extend to invariants in $\overline{\mathbb{Q}}[X_n]^{G_n}$. These invariants are again denoted c_4, c_6, Δ. Since π_n^* is injective it follows by Galois theory that $c_4, c_6, \Delta \in \mathbb{Q}[X_n]$. In fact the coefficients are integers.

Lemma 4.15. *$c_4, c_6, \Delta \in \mathbb{Z}[X_n]$.*

Proof: Let $F = c_4, c_6$ or Δ. Let p be a prime and $r \geq 0$ an integer. We suppose for a contradiction that $p^{r+1}F \in \mathbb{Z}_p[X_n]$ yet $p^rF \notin \mathbb{Z}_p[X_n]$. Then each coefficient of $\pi_n^*(p^{r+1}F) \in \mathbb{Z}[X_1]$ is divisible by p. So if $G \in \mathbb{F}_p[X_n]$ is the reduction of $p^{r+1}F$ mod p then $\pi_n^*G = 0$. The injectivity established in Lemma 4.8 shows that $G = 0$. Therefore $p^rF \in \mathbb{Z}_p[X_n]$. This is the required contradiction. □

Remark 4.16. Since the original $c_4, c_6, \Delta \in \mathbb{Z}[X_1]$ are primitive it is clear that the new $c_4, c_6, \Delta \in \mathbb{Z}[X_n]$ are also primitive. This means it is possible to specify our scalings of c_4, c_6, Δ, at least up to sign, without the need to compute their restrictions to the Weierstrass family.

We revert to working over an arbitrary perfect field K.

Proof of Theorem 4.4: Let $c_4, c_6, \Delta \in K[X_n]$ be the images of $c_4, c_6, \Delta \in \mathbb{Z}[X_n]$. These polynomials are invariants of weights 4, 6 and 12, satisfying $c_4^3 - c_6^2 = 1728\Delta$. They are non-zero by Remark 4.16.
(i) If char $(K) \neq 2, 3$ then by Lemmas 4.8 and 4.9 the map

$$\pi_n^* : K[X_n]^{G_n} \to K[X_1]^{G_1} = K[c_4, c_6]$$

is an isomorphism of graded rings.
(ii) We may assume that K is algebraically closed. If $\phi \in X_n$ with C_ϕ a smooth curve of genus one then by Propositions 4.6 and 4.7 it is equivalent to a Weierstrass model. We deduce $\Delta(\phi) \neq 0$. So there is an inclusion

$$\{\Delta = 0\} \subset X_n^{\text{sing}}.$$

But Proposition 4.5 asserts that X_n^{sing} is closed and irreducible. So the inclusion is in fact an equality.
(iii) Let $\phi \in X_n$ with C_ϕ a smooth curve of genus one. In §5.4 we use $\phi \in X_n$ to define an invariant differential ω_ϕ on C_ϕ. In the case $n = 5$

we must assume $\operatorname{char}(K) \neq 2$. We then show that $c_4(\phi)$ and $c_6(\phi)$ are the geometric invariants of the pair (C_ϕ, ω_ϕ). The formula for the Jacobian follows by Proposition 2.3. □

Theorem 4.4(iii) is proved in [1] for $n = 2, 3, 4$ by giving formulae for the covering map (of degree n^2) from a genus one curve to its Jacobian. We have extended to the case $n = 5$ by taking a different approach, based on properties of the invariant differential.

It turns out that the map $\pi_n^* : K[X_n]^{G_n} \to K[X_1]^{G_1}$ is an isomorphism in all characteristics. The proof in characteristics 2 and 3 is given in §10.

The remaining sections of the paper may be read in any order.

5. Geometry

The aim of this section is to prove the geometric results cited in §4. We work over an algebraically closed field K. The homogeneous ideal of a projective variety X is denoted $I(X)$.

5.1. **Genus one normal curves.**

We recall some basic facts about genus one normal curves and rational nodal curves.

Definition 5.1. Let $n \geq 3$ be an integer.
(i) A genus one normal curve $C \subset \mathbb{P}^{n-1}$ is a smooth curve of genus one and degree n that spans $\mathbb{P}^{n-1}$.
(ii) A rational nodal curve $C \subset \mathbb{P}^{n-1}$ is a rational curve of degree n that spans $\mathbb{P}^{n-1}$ and has a single node.

Remark 5.2. Equivalently, a genus one normal curve is a smooth curve of genus one embedded by a complete linear system of degree n. A rational nodal curve is the image of a morphism $\mathbb{P}^1 \to \mathbb{P}^{n-1}$ determined by a linear system of the form

$$\{f \in \mathcal{L}(D) | f(P_1) = f(P_2)\}$$

for D a divisor on $\mathbb{P}^1$ of degree n, and P_1, $P_2 \in \mathbb{P}^1$ distinct.

Proposition 5.3. *Let $C \subset \mathbb{P}^{n-1}$ be either a genus one normal curve or a rational nodal curve. If $n \geq 4$ then the ideal $I(C)$ is generated by a vector space of quadrics of dimension $n(n-3)/2$.*

This proposition is well known, at least for genus one normal curves. Our proof, based on an argument in [17], has the advantage of working for rational nodal curves at the same time. We write $R = K[x_1, \ldots, x_n]$ and $R' = K[x_1, \ldots, x_{n-1}]$ for the homogeneous co-ordinate rings of $\mathbb{P}^{n-1}$ and $\mathbb{P}^{n-2}$. We give each ring its usual grading by degree, say $R = \oplus_{d \geq 0} R_d$ and $R' = \oplus_{d \geq 0} R'_d$.

Lemma 5.4. *Let $X \subset \mathbb{P}^{n-2}$ be a set of n points in general position.*
(i) The evaluation map $\pi_X : R'_d \to K^n$ is surjective for all $d \geq 2$.
(ii) If $n \geq 4$ then the ideal $I(X) \subset R'$ is generated by quadrics.

Proof: We change co-ordinates so that X is the set of points $(1 : 0 : \ldots : 0)$, $(0 : 1 : \ldots : 0)$, $\ldots$, $(0 : 0 : \ldots : 1)$ and $(1 : 1 : \ldots : 1)$. The proof is now straightforward. □

We show that the curves defined in Definition 5.1 are projectively normal.

Lemma 5.5. *Let $C \subset \mathbb{P}^{n-1}$ be either a genus one normal curve or a rational nodal curve. Let H be the divisor of a hyperplane section, say cut out by a linear form $h \in R_1$. Then the map*

$$\pi_C : R_d \to \mathcal{L}(dH)\,; \;\; f \mapsto f/h^d$$

is surjective for all $d \geq 1$.

Proof: The proof is by induction on d, the case $d = 1$ being clear from Riemann-Roch. For the induction step we choose a hyperplane $\{\xi = 0\}$ meeting C in n distinct points disjoint from H. Again by Riemann-Roch any $n - 1$ distinct points on C span a hyperplane. So $X = C \cap \{\xi = 0\}$ satisfies the hypothesis of Lemma 5.4.

Let $d \geq 2$. We are given $f \in \mathcal{L}(dH)$ and wish to show that it belongs to the image of π_C. By Lemma 5.4(i) it suffices to treat the case where f vanishes on X. But then $f = (\xi/h)f'$ for some $f' \in \mathcal{L}((d-1)H)$. Applying the induction hypothesis to f', we deduce that f is in the image of π_C as required. □

Proof of Proposition 5.3: We continue with the notation of the last proof. Since C is contained in no hyperplane, the natural map

$$I(C) \cap R_2 \to I(X) \cap R'_2 \tag{5}$$

is injective. By Lemmas 5.4 and 5.5 these spaces each have dimension $n(n-3)/2$. So (5) is an isomorphism. Now let $f \in I(C) \cap R_d$. We must show that f is in the ideal generated by $I(C) \cap R_2$. By Lemma 5.4(ii) and the surjectivity of (5) it suffices to treat the case where f vanishes on X. But then $f = \xi f'$ for some $f' \in I(C) \cap R_{d-1}$. The proposition now follows by induction on d. □

We say that curves $C, C' \subset \mathbb{P}^{n-1}$ are projectively equivalent if there exists $\alpha \in \mathrm{PGL}_n$ with $\alpha(C) = C'$.

Lemma 5.6. *(i) Genus one normal curves $C, C' \subset \mathbb{P}^{n-1}$ are projectively equivalent if and only if they have the same j-invariant.*
(ii) Any two rational nodal curves $C, C' \subset \mathbb{P}^{n-1}$ are projectively equivalent.

Proof: (i) Let C and C' have hyperplane sections H and H'. If C and C' are isomorphic as curves then composing with a translation map we can find an isomorphism $\alpha : C \cong C'$ with $\alpha^* H' \sim H$.
(ii) This is clear from Remark 5.2. □

Lemma 5.7. *Let $C \subset \mathbb{P}^{n-1}$ be either a genus one normal curve or a rational nodal curve. Then there are only finitely many $\alpha \in \mathrm{PGL}_n$ with $\alpha(C) = C$.*

Proof: We first treat the case C is a genus one normal curve, say with hyperplane section H. We are interested in the automorphisms α of C with $\alpha^* H \sim H$. The automorphism group of C sits in an exact sequence

$$0 \to E \to \mathrm{Aut}(C) \to \mathrm{Aut}(E, 0) \to 0$$

where E is the Jacobian of C. The first map is $P \mapsto \tau_P$ where τ_P is translation by P. Since H is a divisor of degree n we have $\tau_P^* H \sim H$ if and only if $nP = 0$. The lemma follows from the fact that $E[n]$ and $\mathrm{Aut}(E, 0)$ are both finite.

If C is a rational nodal curve then without loss of generality it is the image of

$$\mathbb{P}^1 \mapsto \mathbb{P}^{n-1}; \quad (s : t) \mapsto (s^n + t^n : st^{n-1} : \ldots : s^{n-1}t).$$

The group of automorphisms of $\mathbb{P}^1$ that extend to automorphisms of $\mathbb{P}^{n-1}$ form a copy of the dihedral group generated by $(s : t) \mapsto (t : s)$ and $(s : t) \mapsto (\zeta s : t)$ for ζ an nth root of unity. □

5.2. **Minimal free resolutions.** We recall that a genus one model of degree $n = 3, 4, 5$ is a collection of homogeneous polynomials in $R = K[x_1, \ldots, x_n]$. Splitting into the cases $n = 3, 4, 5$ we now use $\phi \in X_n$ to define an ideal $I_\phi \subset R$ and a complex of graded free R-modules $\mathcal{F}_\bullet(\phi)$. We write $R(d)$ for the graded R-module with $R(d)_e = R_{d+e}$.

If $n = 3$ then ϕ consists of a single polynomial $f \in R$. This polynomial generates an ideal $I_\phi \subset R$ and defines a complex

$$\mathcal{F}_\bullet(\phi) : \qquad 0 \longrightarrow R(-3) \xrightarrow{\ f\ } R \longrightarrow 0.$$

If $n = 4$ then ϕ consists of polynomials q_1, q_2. These polynomials generate an ideal $I_\phi \subset R$ and define a complex

$$\mathcal{F}_\bullet(\phi) : \qquad 0 \longrightarrow R(-4) \xrightarrow{\begin{pmatrix} -q_2 \\ q_1 \end{pmatrix}} R(-2)^2 \xrightarrow{\begin{pmatrix} q_1 & q_2 \end{pmatrix}} R \longrightarrow 0.$$

If $n = 5$ then ϕ is a 5×5 alternating matrix of linear forms. The Pfaffian of a 4×4 alternating matrix is

$$\operatorname{pf}\begin{pmatrix} 0 & a_1 & a_2 & a_3 \\ & 0 & b_3 & b_2 \\ & & 0 & b_1 \\ & & & 0 \end{pmatrix} = a_1b_1 - a_2b_2 + a_3b_3.$$

We write $\phi^{\{i\}}$ for the submatrix of ϕ obtained by deleting the ith row and ith column. Then the vector of submaximal Pfaffians of ϕ is $P = (p_1, \ldots, p_5)$ where

$$p_i = (-1)^{i+1}\operatorname{pf}(\phi^{\{i\}}).$$

These polynomials generate an ideal $I_\phi \subset R$ and define a complex

$$\mathcal{F}_\bullet(\phi): \quad 0 \longrightarrow R(-5) \xrightarrow{P^T} R(-3)^5 \xrightarrow{\phi} R(-2)^5 \xrightarrow{P} R \longrightarrow 0.$$

In each case $n = 3, 4, 5$, the variety $C_\phi \subset \mathbb{P}^{n-1}$ is that defined by the ideal $I_\phi \subset R$. We say that $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ if it is exact at every term except the final copy of R where the homology is R/I_ϕ.

Lemma 5.8. *Let $n = 3, 4, 5$ and let $\phi \in X_n$.*
(i) Every component of C_ϕ has dimension at least 1.
(ii) If every component of C_ϕ has dimension 1 then $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ.

PROOF: (i) This is clear for $n = 3, 4$. For $n = 5$ we recall that the 4×4 Pfaffians of a generic 5×5 alternating matrix define the image of the Plucker embedding $\operatorname{Gr}(2, 5) \to \mathbb{P}^9$. Then C_ϕ is the intersection of this Grassmannian with a linear subspace $\mathbb{P}^4$. Since $\operatorname{Gr}(2, 5)$ has dimension 6 we are done by [15, I, Theorem 7.2].
(ii) If $n = 3, 4$ then our claim is that f is non-zero, respectively that q_1, q_2 are coprime. This is clear. The case $n = 5$ is an application of the Buchsbaum-Eisenbud acyclicity criterion, for which we refer to [4, Theorem 1.4.13] or [10, Theorem 20.9]. □

We recall that if A is a finitely generated graded K-algebra, say $A = \oplus_{d \geq 0} A_d$, then there is a polynomial $h_A(t)$, called the Hilbert polynomial, with the property that $h_A(d) = \dim(A_d)$ for all $d \gg 0$.

Lemma 5.9. *(i) Let $n = 3, 4, 5$ and let $\phi \in X_n$. If the complex $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ then*

$$h_{R/I_\phi}(t) = nt.$$

(ii) If $C \subset \mathbb{P}^{n-1}$ is a curve of arithmetic genus g and degree d then

$$h_{R/I(C)}(t) = dt + (1 - g).$$

Proof: (i) We compute the Hilbert polynomial from the minimal free resolution in the usual way. For example in the case $n = 5$,

$$h(t) = \binom{t+4}{4} - 5\binom{t+2}{4} + 5\binom{t+1}{4} - \binom{t-1}{4} = 5t.$$

(ii) This is a definition. See for example [15, I, §7]. □

Proposition 5.10. *Let $n = 3, 4, 5$ and let $\phi \in X_n$.*
(i) If $C_\phi \subset \mathbb{P}^{n-1}$ is a smooth curve of genus one then it is a genus one normal curve of degree n.
(ii) If $C_\phi \subset \mathbb{P}^{n-1}$ is a rational curve with a single node then it is a rational nodal curve of degree n.

Proof: By Lemma 5.8 the complex $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ. Since $I_\phi \subset I(C_\phi)$, a comparison of Hilbert polynomials as described in Lemma 5.9 shows that C_ϕ has degree $d \le n$. If $C_\phi \subset \mathbb{P}^{n-1}$ spans a linear subspace of dimension $m-1$ it follows by Riemann-Roch that $3 \le m \le d \le n$. We must show that $m = n$. In the case $n = 3$ this is already clear. If $n = 4, 5$ then C_ϕ is defined by quadrics. This enables us to rule out the unwanted possibilities for (m, d), with the exception of $(m, d) = (4, 4)$ in the case $n = 5$. This possiblity is excluded by the following lemma. □

Lemma 5.11. *Let $C \subset \mathbb{P}^3$ be either a genus one normal curve or a rational nodal curve. Then C cannot be defined by the 4×4 Pfaffians of a 5×5 alternating matrix of linear forms on $\mathbb{P}^3$.*

Proof: Let ϕ be such a matrix, with vector of submaximal Pfaffians $P = (p_1, \ldots, p_5)$. Let C be defined by quadrics q_1, q_2. By Proposition 5.3 we have $\langle p_1, \ldots, p_5 \rangle = \langle q_1, q_2 \rangle$. Replacing ϕ by $A^T \phi A$ for suitable $A \in \mathrm{GL}_5$ we may suppose that $P = (q_1, q_2, 0, 0, 0)$. Since $P\phi = 0$, and q_1, q_2 are coprime, it follows that the first two rows of ϕ are zero. But then every 4×4 Pfaffian of ϕ vanishes, which is a contradiction. □

Lemma 5.12. *Let $n = 3, 4, 5$ and let $\phi \in X_n$. If $C_\phi \subset \mathbb{P}^{n-1}$ is either a genus one normal curve or a rational nodal curve then I_ϕ is a radical ideal, equivalently $I(C_\phi) = I_\phi$.*

Proof: By Lemma 5.8 the complex $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ. If $n = 3$ then $I_\phi = (f)$ where f is an irreducible cubic. If $n = 4, 5$ then I_ϕ is generated by a vector space of quadrics of dimension $d = 2, 5$. Since $I_\phi \subset I(C_\phi)$ we are done by Proposition 5.3. □

Lemma 5.13. *Let $n = 3, 4, 5$ and let $\phi, \phi' \in X_n$. Suppose that*
(i) there exists $\alpha \in \mathrm{PGL}_n$ with $\alpha(C_\phi) = C_{\phi'}$,
(ii) $\mathcal{F}_\bullet(\phi)$ and $\mathcal{F}_\bullet(\phi')$ are minimal free resolutions of R/I_ϕ and $R/I_{\phi'}$,
(iii) the ideals I_ϕ and $I_{\phi'}$ are radical ideals.
Then ϕ and ϕ' are equivalent.

Proof: By (i) we may assume $C_\phi = C_{\phi'}$. Then (iii) gives $I_\phi = I_{\phi'}$. The cases $n = 3, 4$ are now clear. If $n = 5$ then there is an isomorphism of complexes

$$\begin{tikzcd}
0 \arrow[r] & R(-5) \arrow[r, "P^T"] \arrow[d, "c"] & R(-3)^5 \arrow[r, "\phi"] \arrow[d, "B"] & R(-2)^5 \arrow[r, "P"] \arrow[d, "A"] & R \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & R(-5) \arrow[r, "P'^T"] & R(-3)^5 \arrow[r, "\phi'"] & R(-2)^5 \arrow[r, "P'"] & R \arrow[r] & 0
\end{tikzcd}$$

The matrices $A, B \in \mathrm{GL}_5$ are uniquely determined. Comparing this diagram with its dual gives $B = cA^{-T}$. So $\phi' = [A, c^{-1}I_5]\phi$. □

Lemma 5.14. *Let $n = 3, 4, 5$ and let $\phi \in X_n$. Suppose that*
(i) there are only finitely many $\alpha \in \mathrm{PGL}_n$ with $\alpha(C_\phi) = C_\phi$,
(ii) $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ,
(iii) the ideal I_ϕ is a radical ideal.
Then the stabiliser of ϕ for the action of G_n on $\mathbb{P}(X_n)$ is finite.

Proof: This is clear for $n = 3, 4$. In the case $n = 5$ it suffices to show that if $[A, I_5]\phi = \lambda\phi$ for some $A \in \mathrm{GL}_5$ and $\lambda \in K^*$, then A is a scalar matrix. Taking submaximal Pfaffians we obtain $P \operatorname{adj} A = \lambda^2 P$. By (ii) the components of P are linearly independent. It follows that $\operatorname{adj} A$ and hence A is a scalar matrix. □

Proof of Proposition 4.6: (For $n = 3, 4, 5$.) We are given $\phi, \phi' \in X_n$ with C_ϕ and $C_{\phi'}$ either smooth curves of genus one or rational curves with a single node. By Proposition 5.10 these are either genus one normal curves or rational nodal curves. The hypotheses of Lemmas 5.13 and 5.14 are satisfied by Lemmas 5.6, 5.7, 5.8 and 5.12. □

5.3. **The generic model.** We show that the generic genus one model of degree $n = 3, 4, 5$ defines a smooth curve of genus one.

Definition 5.15. Let $n = 3, 4, 5$. The Jacobian matrix J_ϕ of a genus one model $\phi \in X_n$ is

$$\begin{array}{lll} n = 3 & \phi = (f) & J_\phi = \left(\frac{\partial f}{\partial x_j}\right) \\ n = 4 & \phi = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} & J_\phi = \left(\frac{\partial q_i}{\partial x_j}\right) \\ n = 5 & p_i = (-1)^{i+1} \operatorname{pf}(\phi^{\{i\}}) & J_\phi = \left(\frac{\partial p_i}{\partial x_j}\right). \end{array}$$

Lemma 5.16. *Let $n = 3, 4, 5$ and let $\phi \in X_n$.*
(i) If $P \in C_\phi$ then $\operatorname{rank} J_\phi(P) \leq n - 2$.
(ii) If $\operatorname{rank} J_\phi(P) = n - 2$ *for every $P \in C_\phi$ then C_ϕ is a smooth curve of genus one.*

PROOF: (i) We saw in Lemma 5.8(i) that every component of C_ϕ has dimension at least 1. Therefore $\dim T_P(C_\phi) \geq 1$. Since $I_\phi \subset I(C_\phi)$ it follows that $\operatorname{rank} J_\phi(P) \leq n - 2$.
(ii) The argument used in (i) shows that every component of C_ϕ has dimension 1. So by Lemma 5.8(ii) the complex $\mathcal{F}_\bullet(\phi)$ is a minimal free resolution of R/I_ϕ. In particular R/I_ϕ is Cohen-Macaulay. It follows by Serre's criterion (see [10, §18.3]) that I_ϕ is a prime ideal. Hence C_ϕ is an irreducible smooth curve and $I(C_\phi) = I_\phi$. It only remains to check that C_ϕ has genus 1. We do this by computing the Hilbert polynomial as described in Lemma 5.9. □

We define some "bad" subsets $B_n \subset X_n$.

Definition 5.17. (i) Let $B_3 \subset X_3$ consist of all models of the form

$$\phi = \big(x_1 f_1(x_2, x_3) + f_2(x_2, x_3)\big) .$$

(ii) Let $B_4 \subset X_4$ consist of all models of the form

$$\phi = \begin{pmatrix} x_1 x_2 + g_1(x_2, x_3, x_4) \\ g_2(x_2, x_3, x_4) \end{pmatrix} .$$

(iii) Let $B_5 \subset X_5$ consist of all models ϕ with $\phi_{ij}(1, 0, 0, 0, 0) = 0$ for all $\{i, j\} \neq \{1, 2\}$, and $\phi_{45}(x_1, \ldots, x_5) \equiv 0$.

Lemma 5.18. *Let $n = 3, 4, 5$ and let $\phi \in X_n$. The following are equivalent.*
(i) C_ϕ is not a smooth curve of genus one.
(ii) $\operatorname{rank} J_\phi(P) < n - 2$ *for some $P \in C_\phi$.*
(iii) ϕ is equivalent to a model in B_n.

PROOF: (i) ⇒ (ii). This is a restatement of Lemma 5.16.
(ii) ⇒ (i). This follows from Proposition 5.10(i), Lemma 5.12 and the Jacobian criterion for smoothness.
(iii) ⇒ (ii). Without loss of generality $\phi \in B_n$. Then the point $P =$

$(1:0:\ldots:0)$ belongs to C_ϕ and $\operatorname{rank} J_\phi(P) < n-2$.
(ii) $\Rightarrow$ (iii). This is clear for $n = 3, 4$. We take $n = 5$. Since $P \in C_\phi$ the 4×4 Pfaffians of $\phi(P)$ vanish. So $\operatorname{rank} \phi(P) = 0$ or 2.

If $\operatorname{rank} \phi(P) = 2$ then we may assume $P = (1:0:\ldots:0)$ and

$$\phi = \begin{pmatrix} 0 & x_1 & \phi_{13} & \phi_{14} & \phi_{15} \\ & 0 & \phi_{23} & \phi_{24} & \phi_{25} \\ & & 0 & \ell_3 & -\ell_2 \\ & - & & 0 & \ell_1 \\ & & & & 0 \end{pmatrix}$$

for some $\phi_{ij}, \ell_k \in \langle x_2, x_3, x_4, x_5 \rangle$. Since $\operatorname{rank} J_\phi(P) < 3$ the linear forms ℓ_1, ℓ_2, ℓ_3 are linearly dependent. Replacing ϕ by $A\phi A^T$ for suitable $A \in \mathrm{GL}_5$ we may suppose that $\ell_1 = 0$. Then $\phi \in B_5$ as required.

If $\operatorname{rank} \phi(P) = 0$ then we may assume

$$\phi = \begin{pmatrix} 0 & \phi_{12} & \phi_{13} & \phi_{14} & \ell_1 \\ & 0 & \phi_{23} & \phi_{24} & \ell_2 \\ & & 0 & \phi_{34} & \ell_3 \\ & - & & 0 & \ell_4 \\ & & & & 0 \end{pmatrix}$$

for some $\phi_{ij} \in \langle x_2, x_3, x_4, x_5 \rangle$ and $\ell_j \in \langle x_3, x_4, x_5 \rangle$. It is clear that $\ell_1, \ldots, \ell_4$ are linearly dependent. Replacing ϕ by $A\phi A^T$ for suitable $A \in \mathrm{GL}_5$ we may suppose that $\ell_4 = 0$. Then $\phi \in B_5$ as required. □

Proof of Proposition 4.5: (For $n = 3, 4, 5$.) Let X_n^{sing} be the set of all models $\phi \in X_n$ which do not define a smooth curve of genus one. We consider the projective variety

$$Z_n = \{(\phi, P) \in \mathbb{P}(X_n) \times \mathbb{P}^{n-1} | P \in C_\phi \text{ and } \operatorname{rank} J_\phi(P) < n-2\}.$$

Let $\mathrm{pr}_1 : Z_n \to \mathbb{P}(X_n)$ be the first projection. Lemma 5.18 identifies $\mathrm{pr}_1(Z_n) = \mathbb{P}(X_n^{\text{sing}})$. Since the image of a projective variety is again projective it follows that $X_n^{\text{sing}} \subset X_n$ is a Zariski closed subset.

Lemma 5.18 also identifies X_n^{sing} as the image of a morphism

$$\mathcal{G}_n \times B_n \to X_n.$$

Since $\mathcal{G}_n$ and B_n are irreducible it follows that X_n^{sing} is irreducible. □

5.4. **The invariant differential.** We continue to work over an algebraically closed field K. In the case $n = 5$ we further suppose that $\operatorname{char}(K) \neq 2$.

Let $\phi \in X_n$ with C_ϕ a smooth of curve genus one. We use ϕ to define an invariant differential ω_ϕ on C_ϕ. In the cases $n = 1, 2$ we put

$$\begin{array}{lll} n = 1 & \phi = (a_1, a_2, a_3, a_4, a_6) & \omega_\phi = \frac{dx}{2y+a_1x+a_3} \\ n = 2 & \phi = (p(x,z), q(x,z)) & \omega_\phi = \frac{z^2 d(x/z)}{2y+p(x,z)}. \end{array}$$

In the cases $n = 3, 4, 5$ we start with the complex

$$\mathcal{F}_\bullet(\phi) \; : \quad 0 \longrightarrow R \xrightarrow{\phi_{n-2}} \mathcal{F}_{n-3} \longrightarrow \ldots \longrightarrow \mathcal{F}_1 \xrightarrow{\phi_1} R \longrightarrow 0$$

defined in §5.2. We identify the maps ϕ_i with the matrices of homogeneous polynomials that represent them. Then we define

$$\omega_\phi = \frac{x_1^2 d(x_2/x_1)}{\frac{\partial \phi_1}{\partial x_3} \circ \ldots \circ \frac{\partial \phi_{n-2}}{\partial x_n}}$$

where the partial derivative of a matrix is the matrix of partial derivatives. In the cases $n = 3, 4$ this formula works out as

$$\omega_\phi = \frac{x_1^2 d(x_2/x_1)}{\frac{\partial f}{\partial x_3}} \quad \text{ and } \quad \omega_\phi = \frac{x_1^2 d(x_2/x_1)}{\frac{\partial q_1}{\partial x_4}\frac{\partial q_2}{\partial x_3} - \frac{\partial q_1}{\partial x_3}\frac{\partial q_2}{\partial x_4}}.$$

Proposition 5.19. *Let $\phi \in X_n$ with C_ϕ a smooth curve of genus one. If $\phi' = g\phi$ for some $g \in \mathcal{G}_n$ then the isomorphism $\gamma : C_{\phi'} \cong C_\phi$ determined by g satisfies*

$$\gamma^* \omega_\phi = (\det g)\omega_{\phi'}.$$

PROOF: If the proposition holds for $g_1, g_2 \in \mathcal{G}_n$ then it holds for g_1g_2. So we only need to consider g running over a set of generators for $\mathcal{G}_n$. Since the cases $n = 1, 2$ are well known we take $n = 3, 4, 5$. The result is clear for g of the form $[1, B]$ with

$$B = \begin{pmatrix} \mu_1 & \lambda & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_n \end{pmatrix}.$$

If $n = 3$ and $g = [\mu, I_3]$ then the result is again clear. If $n = 4$ and $g = [A, I_4]$ then there is an isomorphism of complexes

$$\begin{tikzcd} 0 \arrow[r] & R(-4) \arrow[r, "\phi_2'"] \arrow[d, "\det A"] & R(-2)^2 \arrow[r, "\phi_1'"] \arrow[d, "A^T"] & R \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & R(-4) \arrow[r, "\phi_2"] & R(-2)^2 \arrow[r, "\phi_1"] & R \arrow[r] & 0 \end{tikzcd}$$

We deduce

$$\gamma^* \omega_\phi = (\det A)\omega_{\phi'} = (\det g)\omega_{\phi'}.$$

If $n = 5$ and $g = [A, I_5]$ then there is an isomorphism of complexes

$$\begin{tikzcd}
0 \arrow[r] & R(-5) \arrow[r, "\phi_3'"] \arrow[d, "(\det A)^2"] & R(-3)^5 \arrow[r, "\phi_2'"] \arrow[d, "(\det A)A^T"] & R(-2)^5 \arrow[r, "\phi_1'"] \arrow[d, "\operatorname{adj} A"] & R \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & R(-5) \arrow[r, "\phi_3"] & R(-3)^5 \arrow[r, "\phi_2"] & R(-2)^5 \arrow[r, "\phi_1"] & R \arrow[r] & 0
\end{tikzcd}$$

We deduce

$$\gamma^* \omega_\phi = (\det A)^2 \omega_{\phi'} = (\det g) \omega_{\phi'}.$$

It only remains to prove the proposition for $g = [1, B]$ with B a permutation matrix. This in turn reduces to checking the result for a set of transpositions generating the symmetric group S_n. The symmetry (12) is already clear from the identity

$$x_1^2 d(x_2/x_1) + x_2^2 d(x_1/x_2) = 0.$$

Since the entries of ϕ_1 belong to $I(C_\phi)$ we have

$$\sum_{i=2}^{n} \frac{\partial \phi_1}{\partial x_i} d(x_i/x_1) = 0. \tag{6}$$

If $n = 3$ then (6) gives the symmetry (23). If $n = 4$ then the symmetry (34) is clear. By (6) we have

$$\begin{vmatrix} \frac{\partial q_1}{\partial x_2} & \frac{\partial q_1}{\partial x_4} \\ \frac{\partial q_2}{\partial x_2} & \frac{\partial q_2}{\partial x_4} \end{vmatrix} d(x_2/x_1) + \begin{vmatrix} \frac{\partial q_1}{\partial x_3} & \frac{\partial q_1}{\partial x_4} \\ \frac{\partial q_2}{\partial x_3} & \frac{\partial q_2}{\partial x_4} \end{vmatrix} d(x_3/x_1) = 0$$

and this establishes the symmetry (23).

If $n = 5$ then the symmetry (35) is clear. Differentiating $\phi_1 \phi_2 = 0$ and $\phi_2 \phi_3 = 0$ we find

$$\frac{\partial \phi_1}{\partial x_3} \frac{\partial \phi_2}{\partial x_4} \frac{\partial \phi_3}{\partial x_5} + \frac{\partial \phi_1}{\partial x_3} \frac{\partial \phi_2}{\partial x_5} \frac{\partial \phi_3}{\partial x_4} = \phi_1 \frac{\partial \phi_2}{\partial x_3} \frac{\partial^2 \phi_3}{\partial x_4 \partial x_5}. \tag{7}$$

This establishes the symmetry (45). Using (6) we get

$$\sum_{i=2}^{5} \frac{\partial \phi_1}{\partial x_i} \frac{\partial \phi_2}{\partial x_4} \frac{\partial \phi_3}{\partial x_5} d(x_i/x_1) = 0.$$

The terms for $i = 4, 5$ vanish since char$\,(K) \neq 2$ and analogous to (7) we have

$$2 \frac{\partial \phi_1}{\partial x_4} \frac{\partial \phi_2}{\partial x_4} \frac{\partial \phi_3}{\partial x_5} = \frac{\partial^2 \phi_1}{\partial x_4^2} \frac{\partial \phi_2}{\partial x_5} \phi_3 \,.$$

This establishes the symmetry (23). □

Lemma 5.20. *Let $\phi = \pi_n(\phi_1)$ be a Weierstrass model with C_ϕ a smooth curve of genus one. Then the natural isomorphism $\gamma : C_{\phi_1} \cong C_\phi$ satisfies $\gamma^* \omega_\phi = \omega_{\phi_1}$.*

Proof: We check this by direct calculation using the definition of ω_ϕ and the formulae of §6. □

Lemma 5.21. *Let $\phi \in X_n$ with C_ϕ a smooth curve of genus one. Then ω_ϕ is an invariant differential on C_ϕ.*

Proof: Our claim is that ω_ϕ is a non-zero regular 1-form. By Propositions 4.6, 4.7 and 5.19 it suffices to prove this for ϕ a Weierstrass model. Then Lemma 5.20 reduces us to the case $n = 1$, and in this case the result is well known. □

We recall from Definition 4.12 that models $\phi, \phi' \in X_n$ are properly equivalent if there exists $g \in \mathcal{G}_n$ with $g\phi = \phi'$ and $\det(g) = 1$.

Lemma 5.22. *Let $\phi, \phi' \in X_1$ with C_ϕ and $C_{\phi'}$ smooth curves of genus one. Then ϕ and ϕ' are properly equivalent if and only if $\pi_n(\phi)$ and $\pi_n(\phi')$ are properly equivalent.*

Proof: One implication is clear from Proposition 4.7. For the converse we suppose $\pi_n(\phi)$ and $\pi_n(\phi')$ are properly equivalent. Then by Proposition 5.19 and Lemma 5.20 there is an isomorphism $\gamma : C_\phi \cong C_{\phi'}$ with $\gamma^* \omega_{\phi'} = \omega_\phi$. Composing with a translation we may suppose that γ is determined by some $g \in \mathcal{G}_1$. It follows that ϕ and ϕ' are properly equivalent. □

Proof of Proposition 4.13: Let $\phi \in X_n$ with C_ϕ a smooth curve of genus one. We must show that ϕ is properly equivalent to a Weierstrass model $\pi_n(0, 0, 0, A, B)$ for some unique $A, B \in K$. The existence is already clear from Propositions 4.6 and 4.7. To prove uniqueness we use Lemma 5.22 to reduce to the case $n = 1$. In this case the result is well known. □

In the proof of Theorem 4.4(iii) we used

Proposition 5.23. *Let $\phi \in X_n$ with C_ϕ a smooth curve of genus one. Then the geometric invariants of (C_ϕ, ω_ϕ) are $c_4(\phi)$ and $c_6(\phi)$.*

Proof: We are free to replace ϕ by any properly equivalent model. So we may assume that ϕ is a Weierstrass model. Then Lemma 5.20 reduces us to the case $n = 1$. In this case the result is a tautology. □

6. Weierstrass models

Let E be an elliptic curve with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

In the notation of §3 we have $E = C_\phi$ where $\phi = (a_1, a_2, a_3, a_4, a_6)$. The complete linear system $|n.0|$ determines a morphism $E \to \mathbb{P}^{n-1}$

$$\begin{array}{lrcl} n = 2 & (x, y) & \mapsto & (x : 1) \\ n = 3 & (x, y) & \mapsto & (1 : x : y) \\ n = 4 & (x, y) & \mapsto & (1 : x : y : x^2) \\ n = 5 & (x, y) & \mapsto & (1 : x : y : x^2 : xy). \end{array}$$

The image is defined by a genus one model

$$\begin{aligned} \pi_2(\phi) &= (a_1xz + a_3z^2, x^3z + a_2x^2z^2 + a_4xz^3 + a_6z^4) \\ \pi_3(\phi) &= (y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3) \\ \pi_4(\phi) &= \begin{pmatrix} x_1x_4 - x_2^2 \\ x_3^2 + a_1x_2x_3 + a_3x_1x_3 - x_2x_4 - a_2x_2^2 - a_4x_1x_2 - a_6x_1^2 \end{pmatrix} \\ \pi_5(\phi) &= \begin{pmatrix} 0 & \ell & x_5 & x_4 & x_3 \\ & 0 & x_4 & x_3 & x_2 \\ & & 0 & -x_2 & 0 \\ & - & & 0 & x_1 \\ & & & & 0 \end{pmatrix} \end{aligned}$$

where $\ell = a_1x_5 - a_2x_4 + a_3x_3 - a_4x_2 - a_6x_1$.

These formulae define a morphism $\pi_n : X_1 \to X_n$. A morphism $\gamma_n : \mathcal{G}_1 \to \mathcal{G}_n$ with the properties specified in Proposition 4.7 is given by

$$\begin{aligned} \gamma_2([u; r, s, t]) &= \left[u^{-3}, (0, u^2s, t), \begin{pmatrix} u^2 & 0 \\ r & 1 \end{pmatrix} \right] \\ \gamma_3([u; r, s, t]) &= \left[u^{-6}, \begin{pmatrix} 1 & r & t \\ 0 & u^2 & u^2s \\ 0 & 0 & u^3 \end{pmatrix} \right] \\ \gamma_4([u; r, s, t]) &= \left[\begin{pmatrix} u^{-4} & 0 \\ u^{-6}r & u^{-6} \end{pmatrix}, \begin{pmatrix} 1 & r & t & r^2 \\ 0 & u^2 & u^2s & 2u^2r \\ 0 & 0 & u^3 & 0 \\ 0 & 0 & 0 & u^4 \end{pmatrix} \right] \end{aligned}$$

and $\gamma_5([u;r,s,t]) = [A_5, B_5]$ where

$$A_5 = u^{-2}\begin{pmatrix} 1 & -s & 2r-s^2 & rs-t & -r^2+rs^2-st \\ 0 & u & 2us & -ur & u(-2rs+t) \\ 0 & 0 & u^2 & 0 & -u^2r \\ 0 & 0 & 0 & u^3 & u^3s \\ 0 & 0 & 0 & 0 & u^4 \end{pmatrix}$$

and

$$B_5 = u^{-3}\begin{pmatrix} 1 & r & t & r^2 & rt \\ 0 & u^2 & u^2s & 2u^2r & u^2(rs+t) \\ 0 & 0 & u^3 & 0 & u^3r \\ 0 & 0 & 0 & u^4 & u^4s \\ 0 & 0 & 0 & 0 & u^5 \end{pmatrix}.$$

7. Formulae

We recall some formulae for the invariants in the cases $n = 2, 3, 4$. In each case we scale the invariants so as to give the usual formulae when restricted to the Weierstrass family. As noted in Remark 4.16 these are also the scalings, unique up to sign, for which c_4, c_6 and Δ are primitive integer coefficient polynomials. We assume for simplicity that $\mathrm{char}\,(K) \neq 2, 3$.

7.1. **Formulae for the invariants: case $n = 2$.** The invariants in the case $n = 2$ are classical. Here is one way to compute them. We start with the binary quartic

$$f = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

and compute (a scalar multiple of) its Hessian

$$\begin{aligned} H \;=\; & (8ac-3b^2)x^4 + (24ad-4bc)x^3z + (48ae+6bd-4c^2)x^2z^2 \\ & +(24be-4cd)xz^3 + (8ce-3d^2)z^4. \end{aligned}$$

We then turn f into a differential operator by substituting $\partial/\partial z$ and $-\partial/\partial x$ for x and z. Letting this operator act on f and H gives the invariants

$$\begin{aligned} c_4 &= 2^4(12ae - 3bd + c^2) \\ c_6 &= 2^5(72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3). \end{aligned}$$

The discriminant $\Delta = (c_4^3 - c_6^2)/1728$ is 16 times the usual discriminant of a degree 4 polynomial. If the cross terms $\alpha_0, \alpha_1, \alpha_2$ are included (by computing the square) then c_4, c_6 and Δ are primitive integer coefficient polynomials in $\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e$.

7.2. **Formulae for the invariants: case $n = 3$.** The invariants in the case $n = 3$ are again classical. The ternary cubic

$$\begin{aligned} U(x,y,z) &= ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z \\ &\qquad + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz \end{aligned}$$

has Hessian

$$H(U) = (-1/2) \times \begin{vmatrix} \frac{\partial^2 U}{\partial x^2} & \frac{\partial^2 U}{\partial x \partial y} & \frac{\partial^2 U}{\partial x \partial z} \\ \frac{\partial^2 U}{\partial x \partial y} & \frac{\partial^2 U}{\partial y^2} & \frac{\partial^2 U}{\partial y \partial z} \\ \frac{\partial^2 U}{\partial x \partial z} & \frac{\partial^2 U}{\partial y \partial z} & \frac{\partial^2 U}{\partial z^2} \end{vmatrix} .$$

Putting $c_4 = c_4(U)$, $c_6 = c_6(U)$ and $H = H(U)$ we find

$$H(\lambda U + \mu H) = 3(c_4\lambda^2\mu + 2c_6\lambda\mu^2 + c_4^2\mu^3)U + (\lambda^3 - 3c_4\lambda\mu^2 - 2c_6\mu^3)H.$$

This formula is classical: see [16, §II.7] or [22, §225]. It is easily verified by restricting to any family of plane cubics covering the j-line, for example the Weierstrass family defined in §6. We solve to find

$$\begin{aligned} c_4 &= -216abcm + 144abc_1c_2 + 144acb_1b_3 - 48ab_1c_2^2 + \ldots \\ &\qquad \ldots + 24a_3b_1c_2m - 8a_3b_3m^2 + 16b_1^2c_1^2 - 8b_1c_1m^2 + m^4 \\ c_6 &= 5832a^2b^2c^2 - 3888a^2bcb_3c_2 + 864a^2bc_2^3 + 864a^2cb_3^3 + \ldots \\ &\qquad \ldots + 12a_3b_3m^4 + 64b_1^3c_1^3 - 48b_1^2c_1^2m^2 + 12b_1c_1m^4 - m^6 \end{aligned}$$

where the full expressions have 25 terms and 103 terms respectively. These polynomials are written out completely in [1], [9, §10.3], [22, §§220,221] and [25, §§4.4,4.5].

We may compute the discriminant as $\Delta = (c_4^3 - c_6^2)/1728$. An alternative, taken from [22, §241], is the following. We compute the partial derivatives of U and $H = H(U)$, and arrange the coefficients of these quadrics in a 6×6 matrix. Then this matrix has determinant $\pm 1728\Delta$.

7.3. **Formulae for the invariants: case $n = 4$.** We identify a genus one model of degree 4 with a pair of 4×4 symmetric matrices. Explicitly

$$\phi = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \equiv \begin{pmatrix} A \\ B \end{pmatrix}$$

where

$$q_1(x_1, \ldots, x_4) = \tfrac{1}{2}\mathbf{x}^T A \mathbf{x} \quad \text{and} \quad q_2(x_1, \ldots, x_4) = \tfrac{1}{2}\mathbf{x}^T B \mathbf{x}.$$

The invariants are found by computing the binary quartic

$$\det(sA + tB) = as^4 + bs^3t + cs^2t^2 + dst^3 + et^4$$

and then using the formulae for $n = 2$. The correct scalings are

$$\begin{aligned} c_4 &= 12ae - 3bd + c^2 \\ c_6 &= \tfrac{1}{2}(72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3). \end{aligned}$$

Since $b, d \in 2\mathbb{Z}[X_4]$ the coefficients of c_4 and c_6 are indeed integers as predicted by Lemma 4.15

We may compute the discriminant as $\Delta = (c_4^3 - c_6^2)/1728$. An alternative is the following. Let T_1 and T_2 be the symmetric matrices defined in [1], [20] by

$$\operatorname{adj}(s(\operatorname{adj} A) + t(\operatorname{adj} B)) \quad = \quad a^2 A s^3 + a T_1 s^2 t + e T_2 s t^2 + e^2 B t^3.$$

The corresponding quadrics are

$$q_1'(x_1, \dots x_4) \quad = \quad \tfrac{1}{2}\mathbf{x}^T T_1 \mathbf{x} \quad \text{and} \quad q_2'(x_1, \dots x_4) \quad = \quad \tfrac{1}{2}\mathbf{x}^T T_2 \mathbf{x}.$$

For a permutation $\pi \in S_4$ we define

$$\Omega_{\pi(1),\pi(2)} \quad = \quad \operatorname{sign}(\pi) \left(\frac{\partial q_1}{\partial x_{\pi(3)}} \frac{\partial q_2}{\partial x_{\pi(4)}} - \frac{\partial q_1}{\partial x_{\pi(4)}} \frac{\partial q_2}{\partial x_{\pi(3)}} \right).$$

Then we arrange the coefficients of the quadrics q_1, q_2, q_1', q_2' and $\Omega_{r,s}$ for $1 \le r < s \le 4$ in a 10×10 matrix. The determinant of this matrix turns out to be $\pm 16\Delta$. As seen in §5.4, the quadrics $\Omega_{r,s}$ arise naturally in the construction of an invariant differential ω_ϕ on C_ϕ.

8. An evaluation algorithm

In the case $n = 5$ the invariants c_4 and c_6 are homogeneous polynomials of degrees 20 and 30 in 50 variables. They are therefore too large to write down as explicit polynomials. Nonetheless we have found a practical algorithm for evaluating them. We assume throughout this section that $\operatorname{char}(K) \neq 2, 3, 5$.

We identify $X_5 = \wedge^2 V \otimes W$ where V and W are 5-dimensional vector spaces. Explicitly

$$(\phi_{ij}(x_1, \dots, x_5))_{i,j=1,\dots,5} \equiv \sum_{i<j} (v_i \wedge v_j) \otimes \phi_{ij}(x_1, \dots, x_5)$$

where $v_1, \dots, v_5$ and $x_1, \dots, x_5$ are fixed bases for V and W. The action of $\mathcal{G}_5 = \mathrm{GL}(V) \times \mathrm{GL}(W)$ is the natural one. The commutator subgroup of $\mathcal{G}_5$ is $G_5 = \mathrm{SL}(V) \times \mathrm{SL}(W)$.

Definition 8.1. Let (ρ, Y) be a rational representation of $\mathcal{G}_5$. A covariant is a polynomial map $F : \wedge^2 V \otimes W \to Y$ such that $F \circ g = \rho(g) \circ F$ for all $g \in G_5$.

Notice that the invariants are the covariants in the case of the trivial representation. For a fixed representation (ρ, Y) the covariants form a module over the ring of invariants.

The 4×4 Pfaffians of ϕ are quadrics $p_1, \dots, p_5$ satisfying

$$\phi \wedge \phi \wedge v_i = p_i(x_1, \dots, x_5)\ v_1 \wedge \ldots \wedge v_5.$$

We may therefore define covariants

$$\begin{array}{ll} P : \wedge^2 V \otimes W \to V^* \otimes S^2 W\,; & \phi \mapsto \sum_{i=1}^5 v_i^* \otimes p_i(x_1,\ldots,x_5) \\ S : \wedge^2 V \otimes W \to S^5 W\,; & \phi \mapsto \det(\frac{\partial p_i}{\partial x_j}) \end{array}$$

where $v_1^*,\ldots,v_5^*$ is the basis for V^* dual to $v_1,\ldots,v_5$.

Our method for evaluating the invariants relies on the following geometric "accident".

Lemma 8.2. *Let $\phi \in X_5$ with C_ϕ a smooth curve of genus one and let $p_1,\ldots,p_5$ be the 4×4 Pfaffians of ϕ.*
(i) The secant variety of C_ϕ is the hypersurface defined by $S(\phi) = 0$.
(ii) The partial derivatives $\frac{\partial}{\partial x_i} S(\phi)$ are quadrics in $p_1,\ldots,p_5$.

Proof: (i) See [12, Lemma 6.7] or [17, VIII.2.5].
(ii) The lemma may be checked by direct computation on any family of models covering the j-line, for example the Weierstrass family defined in §6. A more illuminating proof is given in [11, Corollary 7.5]. □

Lemma 8.2(ii) is accompanied by the following uniqueness statement.

Lemma 8.3. *Let $\phi \in X_5$ with 4×4 Pfaffians $p_1,\ldots,p_5$. If $S(\phi) \neq 0$ then the quartics $\{p_i p_j : 1 \leq i \leq j \leq 5\}$ are linearly independent.*

Proof: The condition $S(\phi) \neq 0$ gives that $p_1,\ldots,p_5$ are linearly independent. Now suppose $q(v_1,\ldots,v_5)$ is a quadric in 5 variables with $q(p_1,\ldots,p_5) = 0$. We differentiate with respect to x_j to obtain

$$\textstyle\sum_{i=1}^5 \frac{\partial q}{\partial v_i}(p_1,\ldots,p_5)\frac{\partial p_i}{\partial x_j}(x_1,\ldots,x_5) = 0.$$

Our assumption $S(\phi) \neq 0$ then gives $\frac{\partial q}{\partial v_i}(p_1,\ldots,p_5) = 0$ for all i. Since $p_1,\ldots,p_5$ are linearly independent, it follows that all partial derivatives of q are identically zero, and hence that q itself is identically zero. □

Lemma 8.4. *There is a covariant*

$$Q : \wedge^2 V \otimes W \to S^2 V \otimes W\,; \quad \phi \mapsto \textstyle\sum q_i(v_1,\ldots,v_5) \otimes x_i$$

with the property that if $\phi \in X_5$ with 4×4 Pfaffians $p_1,\ldots,p_5$ then

$$\frac{\partial}{\partial x_i} S(\phi) \quad = \quad q_i(p_1,\ldots,p_5)$$

for all i. Moreover Q is uniquely determined by this property.

Proof: Let $\phi \in X_5(\mathbb{K})$ be the generic model defined over the function field $\mathbb{K} = K(X_5)$. By Proposition 4.5 we know that C_ϕ is a smooth curve of genus one. Then by Lemma 8.2 we can solve for quadrics $q_1,\ldots,q_5$ with the required property. These quadrics define a rational map

$$Q : \wedge^2 V \otimes W - \to S^2 V \otimes W.$$

By Lemma 8.3 the quadrics $q_1, \ldots, q_5$ are uniquely determined. So the covariance property is clear. We must show that Q is regular, and for this we may work over an algebraically closed field.

We first claim that Q is regular at all $\phi \in X_5$ with $S(\phi) \neq 0$. The coefficients of the quartics $\{p_i p_j : 1 \leq i \leq j \leq 5\}$ may be arranged in a 15×70 matrix. Let $h_1, \ldots, h_N \in K[X_5]$ be the 15×15 minors of this matrix. If $\phi \in X_5$ with $S(\phi) \neq 0$ then Lemma 8.3 gives $h_i(\phi) \neq 0$ for some i. Our claim follows since Q is regular on each of the open sets $\{h_i \neq 0\}$.

Now let $F \in K[X_5]$ be a homogeneous polynomial of least degree such that FQ is regular. Then Q is regular at ϕ if and only if $F(\phi) \neq 0$. The above claim gives $F(\phi) \neq 0$ whenever $S(\phi) \neq 0$. But we know by Lemma 8.2(i) that $S(\phi) \neq 0$ for C_ϕ a smooth curve of genus one. By Theorem 4.4(ii) and the irreducibility of Δ (which is inherited from the case $n = 1$) it follows that F is a power of Δ. To complete the proof it only remains to show that S is not divisible by Δ. Since S has degree 10 and Δ has degree 60, this is clear. □

Starting from P and Q we compute covariants M and N_λ taking values in $S^5 V^*$ and $S^5 V$. We then use the natural identification $S^5 V^* = (S^5 V)^*$ to contract these covariants, and hence compute the invariants. We arrive at the following algorithm.

Algorithm 8.5. *Assume* char $(K) \neq 2, 3, 5$.
INPUT: A genus one model $\phi \in X_5 = \wedge^2 V \otimes W$.
OUTPUT: The invariants $c_4(\phi)$, $c_6(\phi)$, $\Delta(\phi)$.

(1) *Compute the* 4×4 *Pfaffians* $p_1, \ldots, p_5$ *of* ϕ.
(2) *Check that the quartics* $\{p_i p_j : 1 \leq i \leq j \leq 5\}$ *are linearly independent. If not return* $0, 0, 0$.
(3) *Compute the secant quintic* $s = \det(\frac{\partial p_i}{\partial x_j})$.
(4) *Solve for the auxiliary quadrics* $q_1, \ldots, q_5$ *satisfying*

$$\frac{\partial s}{\partial x_i} \;=\; q_i(p_1, \ldots, p_5).$$

(5) *Compute the quintic* $M = \det(\sum_{k=1}^{5} \frac{\partial^2 p_k}{\partial x_i \partial x_j} v_k^*) \in S^5 V^*$.
(6) *Compute the quintic* $N_\lambda = \det(\lambda \frac{\partial q_i}{\partial v_j} + \sum_{k=1}^{5} \frac{\partial \phi_{jk}}{\partial x_i} v_k) \in S^5 V$.
(7) *Contract* M *and* N_λ *to obtain*

$$\langle M, N_\lambda \rangle = 40 c_4 \lambda - 320 c_6 \lambda^3 + 128 c_8 \lambda^5.$$

(8) *Check that* $c_8 = c_4^2$.
(9) *Return* c_4, c_6, $(c_4^3 - c_6^2)/1728$.

It is easy to show that the quantities c_4 and c_6 computed are invariants of weights 4 and 6. By Theorem 4.4 the invariants of weights 4 and 6 each form a 1-dimensional vector space. So it only remains to check that the invariants computed are not identically zero, and that they are correctly scaled. We did this by computing their restriction to the Weierstrass family, but in fact it would suffice to compute a single numerical example.

To complete the justification of Algorithm 8.5 we must show that if the quartics in Step 2 are linearly dependent then the invariants are necessarily zero. By Lemma 8.3 we have $S(\phi) = 0$. Then $\Delta(\phi) = 0$ by Lemma 8.2(i). Since $c_4^3 - c_6^2 = 1728\Delta$ it only remains to show that $c_4(\phi) = 0$. We do this by constructing a covariant

$$T : \wedge^2 V \otimes W \to S^5 W^*$$

of degree 30 with $\langle S, T \rangle = c_4^2$. We omit the (lengthy) details, since our main interest is in applying Algorithm 8.5 in the case C_ϕ is a smooth curve of genus one.

An alternative method for computing the discriminant is the following. Let $\phi \in X_5$ with 4×4 Pfaffians $p_1, \ldots, p_5$. For a permutation $\pi \in S_5$ we define

$$\Omega_{\pi(1),\pi(2)} \quad = \quad \operatorname{sign}(\pi) \textstyle\sum_{i,j=1}^5 \frac{\partial p_i}{\partial x_{\pi(3)}} \frac{\partial \phi_{ij}}{\partial x_{\pi(4)}} \frac{\partial p_j}{\partial x_{\pi(5)}}.$$

The calculations of §5.4 show that $\Omega_{r,s}$ is well-defined up to the addition of quadrics in the space spanned by $p_1, \ldots, p_5$. We arrange the coefficients of $p_1, \ldots, p_5$ and $\Omega_{r,s}$ for $1 \le r < s \le 5$ in a 15×15 matrix. Then the determinant of this matrix is an invariant of degree 60, and hence weight 12. We claim it is $\pm 32\Delta$. Since the invariants of weight 12 form a 2-dimensional vector space, our claim is verified by computing two (suitably chosen) numerical examples. This method for computing the discriminant is in practice much faster than using Algorithm 8.5.

9. Computing the geometric invariants

Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n \ge 3$, and let ω be an invariant differential on C, both defined over a field K. The geometric invariants c_4 and c_6 of the pair (C, ω) were defined in §2. We are interested in computing geometric invariants for the following two reasons.

Computing the Jacobian. Given equations defining a genus one normal curve $C \subset \mathbb{P}^{n-1}$ of degree n, we aim to compute a Weierstrass equation for its Jacobian. The first step is to compute an invariant differential ω on C. We can do this using either the method of §2 or the method of §5.4. Proposition 2.3 then reduces the problem of computing the Jacobian to that of computing the geometric invariants.

Minimisation. Let K be a local field with discrete valuation $\mathrm{ord} : K^* \to \mathbb{Z}$. If $n \le 5$ then by minimisation we mean the task of finding an integer coefficient genus one model equivalent to a given one, with $\mathrm{ord}(\Delta)$ minimal. We refer to [8] for a treatment of this problem in the case $n = 2$. In general the same question can be asked provided we have a notion of genus one model with the following properties:

- a (non-singular) genus one model defines a pair (C, ω),
- it is possible to decide whether a genus one model has integer coefficients.

We will not discuss the possible definitions of genus one model for $n > 5$, but merely note that if we are to keep track of our progress in minimising, we must be able to compute geometric invariants.

We have compiled the following list of methods for computing geometric invariants. By Lemma 2.2 we are free to rescale ω at any stage (provided we keep track of the scalars).

9.1. **The invariants method.** We assume that C has degree $n \le 5$. The first step is to compute a genus one model $\phi \in X_n$ with $C = C_\phi$. For $n \le 4$ this is trivial. For $n = 5$ we use the algorithm described in [12]. Then the formulae and algorithms of §§7,8 are used to compute $c_4(\phi)$ and $c_6(\phi)$. By Proposition 5.23 these are the geometric invariants of (C_ϕ, ω_ϕ).

The main disadvantage of the invariants method is that we are currently restricted to $n \le 5$.

9.2. **The projection method.** Extending our field (if necessary) we first find a rational point $P \in C(K)$. For instance we might find P by intersecting our curve with a random hyperplane, or by taking the generic point defined over the function field. Then we project away from P to obtain a genus one normal curve $C_P \subset \mathbb{P}^{n-2}$ of degree $n-1$. Explicitly, we change co-ordinates on $\mathbb{P}^{n-1}$ so that $P = (0 : 0 : \ldots : 0 : 1)$ and the tangent line at P is $x_1 = \ldots = x_{n-2} = 0$. Then the projection map

$$\mathbb{P}^{n-1} - \to \mathbb{P}^{n-2} ; \quad (x_1 : \ldots : x_{n-1} : x_n) \mapsto (x_1 : \ldots : x_{n-1})$$

restricts to an isomorphism $\pi : C \cong C_P$ with $\pi(P) = (0 : 0 : \ldots : 0 : 1)$. We eliminate x_n from the quadrics generating $I(C)$ by linear algebra. If $n \ge 5$ then by Proposition 5.3 the remaining quadrics are sufficient to generate $I(C_P)$. The invariant differential ω on C is specified by an $n \times n$ matrix of quadrics, as described in §2. The corresponding invariant differential on C_P is obtained by deleting the last row and column of this matrix. We eliminate x_n from the remaining entries by subtracting suitable elements of $I(C)$.

At this stage we may either project away from $\pi(P)$ or switch to another method. If we keep projecting away from a rational point, then eventually we obtain a curve in Weierstrass form. (The final stages of this process are described in [7, §8].) Alternatively if a method for computing Riemann-Roch spaces is available, then we may pass directly to a Weierstrass equation by computing $\mathcal{L}(mP)$ for $m = 1, 2, 3$.

The main disadvantage of the projection method is that it requires a field extension.

9.3. **The covering method.** Suppose we are given pairs (C_1, ω_1) and (C_2, ω_2), and a morphism $\pi : C_1 \to C_2$. Further suppose that π is a twist of the multiplication-by-m map on an elliptic curve. Then $(C_1, \pi^*\omega_2)$ and $(C_2, m\omega_2)$ have the same geometric invariants. This enables us to compute the geometric invariants of (C_1, ω_1) from those of (C_2, ω_2).

The main disadvantage of the covering method is that we need to know a suitable map $\pi : C_1 \to C_2$. However if the curve C_1 is found by a descent calculation then it is likely that such a map will be known. In this setting we already know the Jacobian, and the application we have in mind is minimisation.

9.4. **The Wronskian method.** The invariant differential ω determines a derivation $f \mapsto df/\omega$ on the function field $K(C)$. Anderson [2] gives a formula in terms of Wronskian determinants for the covering map of degree n^2 from C to its Jacobian. From this data it is easy to read off the geometric invariants.

The main disadvantage of the Wronskian method is that it requires extensive calculations in the function field.

An example. Wuthrich [27] has constructed an element of order 5 in the Tate-Shafarevich group of an elliptic curve E over $\mathbb{Q}$, where the elliptic curve E does not admit any rational 5-isogenies. Written as a genus one normal quintic his example has equations

$$\begin{aligned}
p_1 &= 3x_1^2 + x_1x_5 - x_2x_4 - x_3^2 \\
p_2 &= 17x_1^2 - 10x_1x_3 + 7x_1x_5 - 7x_2x_4 - 4x_2x_5 + 4x_3x_4 \\
p_3 &= 215x_1^2 - 16x_1x_2 - 80x_1x_3 + 16x_1x_4 + 81x_1x_5 - 49x_2x_4 \\
&\quad -28x_2x_5 - 16x_3x_5 - 16x_4^2 \\
p_4 &= 60x_1^2 + 48x_1x_2 - 34x_1x_3 - 24x_1x_4 + 20x_1x_5 - 8x_2^2 - 5x_2x_3 \\
&\quad -12x_2x_4 + 16x_2x_5 - 14x_3x_5 - 8x_4x_5 \\
p_5 &= 18x_1^2 + 9x_1x_3 - 4x_1x_4 - 4x_1x_5 - 4x_2x_3 - 8x_2x_4 - 6x_2x_5 \\
&\quad +8x_3x_5 - 4x_5^2.
\end{aligned}$$

We use the algorithm in [12] to write these quadrics as the 4×4 Pfaffians of a matrix of linear forms:

$$\begin{pmatrix} 0 & 310x_1 + 3x_2 + 162x_5 & -34x_1 - 5x_2 - 14x_5 & 10x_1 + 28x_4 + 16x_5 & 80x_1 - 32x_4 \\ & 0 & 6x_1 + 3x_2 + 2x_5 & -6x_1 + 7x_3 - 4x_4 & -14x_2 - 8x_3 \\ & & 0 & -x_3 & 2x_2 \\ & - & & 0 & -4x_1 \\ & & & & 0 \end{pmatrix}$$

Algorithm 8.5 then computes the invariants

$$c_4 = 2^{44} \times 151009, \qquad c_6 = -2^{66} \times 34871057.$$

Thus the Jacobian is the elliptic curve of conductor 1 289 106 508 910 with minimal Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - 3146x + 39049.$$

According to MAGMA [19] this elliptic curve has rank 0 and the analytic order of its Tate-Shafarevich group is 25. It is also the only elliptic curve in its isogeny class.

We were also able to compute this example using the projection and Wronskian methods. In our current implementation (written in MAGMA [19], and available from the author's website) the invariants method is slightly faster than the projection method, each taking around a second. The Wronskian method is much slower, taking around 30 seconds in this case, but has the advantage of giving equations for the covering map. These timings are of course heavily dependent on details of the implementation we have not described here.

10. Invariants in characteristics 2 and 3

In §4 we showed that there is an injective homomorphism of graded rings

$$\pi_n^* : K[X_n]^{G_n} \to K[X_1]^{G_1}.$$

We also recalled the usual formulae for b_2, b_4, b_6, b_8 and c_4, c_6, Δ as polynomials in

$$K[X_1] = K[a_1, a_2, a_3, a_4, a_6].$$

In Lemma 4.9 we saw that if $\mathrm{char}\,(K) \neq 2, 3$ then $K[X_1]^{G_1} = K[c_4, c_6]$. The analogue of this result in characteristics 2 and 3 is the following.

Lemma 10.1. *The ring of invariants is*

$$K[X_1]^{G_1} = \begin{cases} K[a_1, \Delta] & \textit{if}\ \mathrm{char}\,(K) = 2 \\ K[b_2, \Delta] & \textit{if}\ \mathrm{char}\,(K) = 3. \end{cases}$$

PROOF: It is easy to show that a_1 and Δ, respectively b_2 and Δ, are invariants. We must show that they generate the ring of invariants. As in the proof of Lemma 4.9, this is deduced from the existence of a suitable normal form.

Case char $(K) = 2$. We start with the general Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

One easily computes $j = a_1^{12}/\Delta$. We assume $j \neq 0$ and following [24, Appendix A] make substitutions $x = x' + r$ and $y = y' + t$ so that $a_3 = a_4 = 0$. We are free to suppose that K is algebraically closed. Then a further substitution $y = y' + sx'$ gives $a_2 = 0$. We arrive at the normal form

$$y^2 + a_1 xy = x^3 + a_6$$

with $\Delta = a_1^6 a_6$. It follows that every invariant is a polynomial in a_1 and Δ/a_1^6. We are done since a_1 does not divide Δ.

Case char $(K) = 3$. We start with a general Weierstrass equation and complete the square to obtain

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6.$$

One easily computes $j = a_2^6/\Delta$. We assume $j \neq 0$ and following [24, Appendix A] make a substitution $x = x' + r$ so that $a_4 = 0$. We arrive at the normal form

$$y^2 = x^3 + a_2 x^2 + a_6$$

with $b_2 = a_2$ and $\Delta = -a_2^3 a_6$. It follows that every invariant is a polynomial in b_2 and Δ/b_2^3. We are done since b_2 does not divide Δ. $\square$

Theorem 10.2. *Let $n = 2, 3, 4, 5$. Then the map $\pi_n^* : K[X_n]^{G_n} \rightarrow K[X_1]^{G_1}$ is an isomorphism in all characteristics.*

PROOF: In §4 we saw that $c_4, c_6, \Delta \in K[X_1]^{G_1}$ extend to invariants $c_4, c_6, \Delta \in K[X_n]^{G_n}$. So it only remains to show that in characteristics 2 and 3 there are invariants in $K[X_n]^{G_n}$ of weights 1 and 2.

If char $(K) = 2$ or 3 then $c_4^3 - c_6^2 = 1728\Delta = 0$. So an invariant of weight 2 exists by unique factorization in $K[X_n]$.

We now take char $(K) = 2$ and split into the cases $n = 2, 3, 4, 5$. In the cases $n = 2, 3$ the coefficient of xyz is an invariant of weight 1. In the case $n = 4$ we write

$$\begin{array}{rcl} q_1(x_1, \ldots, x_4) & = & \sum_{i \leq j} a_{ij} x_i x_j \\ q_2(x_1, \ldots, x_4) & = & \sum_{i \leq j} b_{ij} x_i x_j \end{array}$$

and find

$$a_1 = a_{12} b_{34} + a_{13} b_{24} + a_{14} b_{23} + a_{23} b_{14} + a_{24} b_{13} + a_{34} b_{12}.$$

If $n = 5$ then our genus one model is a matrix of linear forms, say $\phi = (\phi_{ij}(x_1, \ldots, x_5))$. Let T be a set of left coset representatives for $D_5 = \langle (12345), (25)(34) \rangle$ as a subgroup of S_5. Then a_1 is the coefficient of $\prod_{i=1}^5 x_i$ in $\sum_{\sigma \in T} \prod_{i=1}^5 \phi_{\sigma(i)\,\sigma(i+1)}$. □

Remark 10.3. If char $(K) = 2$ or 3 then the invariants do not suffice to compute the Jacobian. For example the elliptic curves $y^2 + xy = x^3 + 1$ and $y^2 + xy = x^3 + x^2 + 1$ over $\mathbb{F}_2$ have invariants $a_1 = \Delta = 1$, but are not isomorphic. Similarly the elliptic curves $y^2 = x^3 - x \pm 1$ over $\mathbb{F}_3$ have invariants $b_2 = 0$ and $\Delta = 1$, but are not isomorphic. These examples should be seen as a consequence of the failure of Lemma 2.4 in characteristics 2 and 3.

As we noted in the introduction, it should instead be possible to find a formula for the Jacobian that works in all characteristics by modifying the formulae in characteristic 0. This has been carried out by Artin, Rodriguez-Villegas and Tate [3] in the case $n = 3$.

Acknowledgements. I would like to thank Nick Shepherd-Barron for introducing me to this problem. The computer calculations in support of this work were performed using MAGMA [19] and PARI [21].

References

[1] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* **90** (2001), no. 2, 304–315.

[2] G.W. Anderson, Lacunary Wronskians on genus one curves, *J. Number Theory* **115** (2005), no. 2, 197–214.

[3] M. Artin, F. Rodriguez-Villegas and J. Tate, On the Jacobians of plane cubics, *Adv. Math.* **198** (2005), no. 1, 366–382.

[4] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, Cambridge, 1993.

[5] D.A. Buchsbaum and D. Eisenbud, Gorenstein ideals of height 3, *Seminar D. Eisenbud/B. Singh/W. Vogel*, Vol. 2, pp. 30–48, Teubner-Texte zur Math., **48**, Teubner, Leipzig, 1982.

[6] D.A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, *Amer. J. Math.* **99** (1977) 447-485.

[7] J.W.S. Cassels, *Lectures on elliptic curves*, CUP, Cambridge, 1991.

[8] J.E. Cremona, M. Stoll, Minimal models for 2-coverings of elliptic curves, *LMS J. Comput. Math.* **5** (2002), 220–243.

[9] I. Dolgachev, *Lectures on invariant theory*, LMS Lecture Note Series **296**, Cambridge University Press, Cambridge, 2003.

[10] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, GTM **150**, Springer-Verlag, New York, 1995.

[11] T.A. Fisher, *The higher secant varieties of an elliptic normal curve*, preprint.

[12] T.A. Fisher, *Genus one curves defined by Pfaffians*, preprint.

[13] W. Fulton and J. Harris, *Representation theory*, GTM **129**, Springer-Verlag, New York, 1991.

[14] J.H. Grace and A. Young, *The algebra of invariants*, Cambridge University Press, Cambridge, 1903.

[15] R. Hartshorne, *Algebraic geometry*, GTM **52**, Springer-Verlag, New York-Heidelberg, 1977.

[16] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993.

[17] K. Hulek, *Projective geometry of elliptic curves*, Soc. Math. de France, Astérisque **137** (1986).

[18] G. Kempf, Some quotient surfaces are smooth, *Michigan Math. J.* **27** (1980), no. 3, 295–299.

[19] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comb.* **24**, 235-265 (1997). (See also the Magma home page at `http://magma.maths.usyd.edu.au/magma/`.)

[20] J.R. Merriman, S. Siksek, N.P. Smart, Explicit 4-descents on an elliptic curve, *Acta Arith.* **77** (1996), no. 4, 385–404.

[21] PARI/GP is developped by the PARI Group, University of Bordeaux. (See also the PARI home page at `http://pari.math.u-bordeaux.fr/`.)

[22] G. Salmon, *A treatise on the higher plane curves*, Third edition, Hodges, Foster and Figgis, Dublin, 1879.

[23] I.R. Shafarevich, *Basic algebraic geometry. 1. Varieties in projective space*, Springer-Verlag, Berlin, 1994.

[24] J.H. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag, New York, 1986.

[25] B. Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993.

[26] A. Weil, Remarques sur un mémoire d'Hermite, *Arch. Math.* **5** (1954), 197–202.

[27] C. Wuthrich, Une quintique de genre 1 qui contredit le principe de Hasse, *Enseign. Math.* (2) 47 (2001), no. 1-2, 161–172.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`