Invariants for the elliptic normal quintic

Tom Fisher

June 21, 2002

Abstract

Let k be a field with char $k \neq 2, 3, 5$. Let C be a smooth curve of genus one defined over k. Suppose that C admits a k-rational divisor of degree n. For $n = 2, 3, 4$ classical invariant theory allows us to compute the Jacobian of C without making any field extensions. We extend to the case $n = 5$, where although the corresponding invariants are too large to write down as polynomials, we have found a practical algorithm for computing them.

Introduction

Let C be a smooth projective curve of genus one defined over a field k. We would like to compute the Jacobian of C, giving the answer in Weierstrass form. We recall that the Jacobian is a certain twist of C that is soluble over k. One approach is to work over an extension field, chosen to make C soluble. This reduces the problem to that of putting a curve in Weierstrass form. But there are two objections to this method. Firstly extending our field may not be practical. Secondly one has to be extremely careful not to accidently write down a quadratic twist of the Jacobian.

Another approach, described by Weil [26], makes use of classical invariant theory. This avoids the need to make any field extensions, but is limited to curves of small degree. To make this last statement precise we take D a k-rational divisor on C of degree n. It is well known that

- If $n = 1$ then C has a k-rational point. In particular C is its own Jacobian.

- If $n \geq 2$ then the linear system associated to D defines a morphism $C \to \mathbf{P}^{n-1}$. We identify $\mathbf{P}^{n-1} = \mathbf{P}(W^*)$ where $W = H^0(C, \mathcal{O}_C(D))$.

- If $n \geq 3$ then this morphism is an embedding. We refer to the geometric configuration $C \subset \mathbf{P}^{n-1}$ as an elliptic normal curve.

- If $n \geq 4$ then $C \subset \mathbf{P}^{n-1}$ is defined by quadrics. The space of quadrics $V = H^0(\mathbf{P}^{n-1}, \mathcal{I}_C(2))$ has dimension $n(n-3)/2$ and generates the homogeneous ideal of C.

From now on we assume that char $k \nmid 6n$. Classical invariant theory gives formulae for the Jacobian in the cases $n = 2, 3, 4$. A unified account is given in [2]. The vector spaces V and W introduced above provide a convenient notation for describing the group actions involved. We take projective equations for C

$$\begin{array}{lll} n=2 & y^2 x_1^2 = U(x_0, x_1) & (U \text{ a quartic}) \\ n=3 & U(x_0, x_1, x_2) = 0 & (U \text{ a cubic}) \\ n=4 & U(x_0, x_1, x_2, x_3) = U'(x_0, x_1, x_2, x_3) = 0 & (U,\, U' \text{ quadrics}) \end{array} \qquad (1)$$

and view these equations as elements of S^4W, S^3W respectively $V^* \otimes S^2W$. Then $\mathrm{SL}(W)$, respectively $\mathrm{SL}(V) \times \mathrm{SL}(W)$, acts on each affine space, and so on the polynomial rings $k[S^4W]$, $k[S^3W]$ and $k[V^* \otimes S^2W]$. In each case the invariant subring is generated by polynomials c_4 and c_6. Labelling these invariants correctly, it turns out that C has Jacobian $y^2 = x^3 - 27c_4x - 54c_6$. Moreover the equations (1) describe a smooth curve of genus one precisely whenever the discriminant $\Delta = (c_4^3 - c_6^2)/1728$ is non-zero.

For $n = 2$ the invariants may be found in [2], [7], [26] or virtually any text on classical invariant theory. For $n = 3$ the invariants are rather more cumbersome, but may still be found written out in [2], [20] or [23]. For $n = 4$ we view the quadrics U, U' as 4×4 symmetric matrices and reduce to the case $n = 2$ by considering the quartic $\det(U + tU')$. We refer to [2], [18] for details.

In this article we extend to the case $n = 5$. Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic. In other words C is a smooth curve of genus one and degree 5 spanning $\mathbf{P}^4$. It is known that C is defined by 5 quadrics, but that 5 quadrics do not in general define an elliptic normal quintic. However it follows from work of Buchsbaum and Eisenbud [5] that the quadrics defining an elliptic normal quintic may be written as the 4×4 Pfaffians of a 5×5 skew-symmetric matrix with entries linear forms on $\mathbf{P}^4$. A geometric argument recalled in [11,

§2] shows that generically this construction gives rise to an elliptic normal quintic. We view these matrices as elements of $\wedge^2 V \otimes W$ and write $C(\phi) \subset \mathbf{P}^4$ for the subscheme defined by the 4×4 Pfaffians of $\phi \in \wedge^2 V \otimes W$.

Theorem 1 *Let V and W be 5-dimensional vector spaces over k. Then the invariant subring for the action of* $\mathrm{SL}(V) \times \mathrm{SL}(W)$ *on* $k[\wedge^2 V \otimes W]$ *is generated by homogeneous polynomials c_4 and c_6 of degrees 20 and 30 respectively. If we set $\Delta = (c_4^3 - c_6^2)/1728$ then*
(i) $C(\phi) \subset \mathbf{P}^4$ is an elliptic normal quintic if and only if $\Delta(\phi) \neq 0$.
(ii) If (i) holds then $C(\phi)$ has Jacobian $y^2 = x^3 - 27c_4(\phi)x - 54c_6(\phi)$.

Given what is classically known in the cases $n = 2, 3, 4$ the statement of Theorem 1 is not a surprise. However it should be stressed that prior to the work of Buchsbaum and Eisenbud it was not possible even to pose the problem correctly.

We define the size $|p|$ of a polynomial p to be the number of monomials appearing in p. The size of the covariants c_4 and c_6 (this is independent of the bases chosen for V and W) grows rapidly with n.

n	Group action	$\lvert c_4\rvert$	$\lvert c_6\rvert$
2	$\mathrm{SL}(W)$ acts on S^4W	3	5
3	$\mathrm{SL}(W)$ acts on S^3W	25	103
4	$\mathrm{SL}(V) \times \mathrm{SL}(W)$ acts on $V^* \otimes S^2W$	4003	81547
5	$\mathrm{SL}(V) \times \mathrm{SL}(W)$ acts on $\wedge^2 V \otimes W$	?	?

As the reader might well surmise from this table, the invariants in the case $n = 5$ are too large to write down as explicit polynomials. See Appendix B for a more careful estimate. Instead we give a practical algorithm for computing the Jacobian. It has 2 steps

- Given 5 quadrics defining an elliptic normal quintic $C \subset \mathbf{P}^4$ we compute $\phi \in \wedge^2 V \otimes W$ such that $C = C(\phi)$.
- Given $\phi \in \wedge^2 V \otimes W$ we compute $c_4(\phi)$ and $c_6(\phi)$.

The first step follows from the work of Buchsbaum and Eisenbud. Indeed the matrix ϕ may be extracted from the syzygies between the original quadrics, and this reduces the problem to linear algebra. The second step is more involved and should be regarded as our main result.

We were inspired to find such an algorithm by the following observation on plane cubics. We take $C \subset \mathbf{P}^2$ a plane cubic with equation $U(x_0, x_1, x_2) = 0$. The Hessian is $H = \det(\partial^2 U/\partial x_i \partial x_j)$. Salmon [20, Chapter V. Art. 241] observes that if we write the quadrics $\partial U/\partial x_i$ and $\partial H/\partial x_i$ in terms of the basis x_0^2, x_1^2, x_2^2, x_0x_1, x_1x_2, x_0x_2 then we obtain a 6×6 matrix whose determinant is a non-zero multiple of the discriminant. He gives equally simple recipes for c_4 and c_6.

We take from this two lessons. Firstly that there are practical algorithms for computing the invariants, far more elegant than the invariants themselves written out as explicit polynomials. Secondly that we should make a definition of covariant sufficiently general to include both the original curve U and the invariants we seek. Each step of our algorithm will then construct new covariants from the ones we already know.

To check that the above algorithm for Δ is correct, it suffices to work over an algebraically closed field. Then making an appropriate choice of co-ordinates our plane cubic takes the form

$$U(x_0, x_1, x_2) = a(x_0^3 + x_1^3 + x_2^3) - 3bx_0x_1x_2. \tag{2}$$

This curve is non-singular provided $D = a(a^3 - b^3)$ is non-zero. The discriminant is $\Delta = D^3$. The Hessian works out as

$$\frac{1}{18}H(x_0, x_1, x_2) = \frac{\partial D}{\partial b}(x_0^3 + x_1^3 + x_2^3) + 3\frac{\partial D}{\partial a}x_0x_1x_2. \tag{3}$$

So the 6×6 determinant may be put in block diagonal form, with each 2×2 block proportional to

$$\det\begin{pmatrix} a & b \\ -\partial D/\partial b & \partial D/\partial a \end{pmatrix} = 4D.$$

It follows that the 6×6 determinant is a non-zero multiple of Δ.

We should regard $(a : b)$ as co-ordinates on $X(3) \simeq \mathbf{P}^1$ and (2) as the universal family $\mathcal{X}(3) \to X(3)$. So we could at this point present our algorithm for computing the invariants in the case $n = 5$, observe that it works for the family $\mathcal{X}(5) \to X(5)$ and thus reduce the length of this article considerably. However we have decided also to explain the methods we used to find our algorithm.

As the above example shows, there are huge computational savings to be made if we are willing to restrict our covariants to $X(n)$. So it is natural to ask how one might recognise a covariant from its restriction to $X(n)$. But to identify $C \subset \mathbf{P}^{n-1}$ as a fibre of $\mathcal{X}(n) \to X(n)$ we must pick a basis $P, Q \in \mathrm{Jac}(C)[n]$ such that the Weil pairing $e_n(P,Q)$ is a fixed primitive nth root of unity. Two such choices differ by an element of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$. So the restriction of a covariant to $X(n)$ satisfies an invariance property under $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$. We call the forms on $X(n)$ satisfying this invariance property the discrete covariants. Since $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ is a finite group the discrete covariants may essentially be read off from the character table. Carrying this programme through in the case $n = 3$ we would for instance learn that (3) is an interesting expression to consider, even if we did not know that it could be computed as the determinant of the matrix of second partial derivatives.

In §1 we recall from [11] some preliminaries on elliptic normal quintics and make our definition of covariant. From §2 until the end of §11 we work over an algebraically closed field. We begin by classifying the orbits of codimension 1 for the action of $\mathrm{GL}(V) \times \mathrm{GL}(W)$ on $\wedge^2 V \otimes W$. This shows that the invariants c_4, c_6 and Δ exist, but neither gives a way of computing them, nor explains the link with the Jacobian.

In §§3,4,5 we develop the theory of discrete covariants. Theorem 2 and its corollary give practical necessary and sufficient conditions for a discrete covariant to come from a covariant. This leads to an improved description of the ring of invariants, and in particular to a proof of Theorem 1 in the case k is algebraically closed. In §7 we give a complete classification of the discrete covariants. Then in §8 we use this classification to write down some non-trivial covariants. It was this prior knowledge of the covariants, albeit restricted to the family $\mathcal{X}(5) \to X(5)$, that enabled us to find our algorithm for computing the invariants. We present the algorithm itself in §9. Its verification does not depend on Theorem 2. In §§10,11 we construct further covariants of geometric interest. These correspond to the invariant differential and quintic hypersurfaces respectively.

In §12 we drop our assumption that k is algebraically closed and make the necessary modifications to the proof of Theorem 1. Then in §13 we implement our algorithm for computing the Jacobian and give some examples in the case $k = \mathbf{Q}$. In §14 we add to our examples by comparing our algorithm with that found by C. O'Neil [19] in the special case where the Jacobian is assumed to have a k-rational point of order 5. There are two appendices. Appendix A gives the character table for $\Gamma = \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$. Appendix B gives an estimate for the size of the invariant c_4.

Some notation

Let V be a vector space over a field k. Let $V^* = \mathrm{Hom}(V,k)$. We write $k[V] = k \oplus V^* \oplus S^2V^* \oplus \ldots$ for the ring of polynomial functions on V, and $k(V)$ for its field of fractions. The Grassmannian $\mathrm{Gr}(r,V)$ is the set of r-dimensional subspaces of V. We write $\mathbf{P}(V) = \mathrm{Gr}(1,V)$. The pairing between a vector space and its dual, or any pairing derived from it, is denoted $\langle\ ,\ \rangle$. If $\pi : G \to \mathrm{GL}(V)$ is a linear representation then we sometimes write $\pi = \pi_V$ or $V = V_\pi$. We write $x \propto y$ to mean $x = cy$ for some $c \in k^*$.

While working with curves of degree n we assume $\mathrm{char}\, k \nmid 6n$. For most of this article $n = 5$ and k is algebraically closed. We write μ_n for the nth roots of unity and ζ_n for a generator. The vector spaces V and W introduced in §1 have bases $v_0, \ldots, v_4$ and $x_0, \ldots, x_4$. The dual bases for V^* and W^* are $v_0^*, \ldots, v_4^*$ and $x_0^*, \ldots, x_4^*$. We identify $\mathbf{P}^4 = \mathbf{P}(W^*)$ so that $x_0, \ldots, x_4$ are co-ordinates on $\mathbf{P}^4$.

1 The space of elliptic normal quintics

Let k be a field with $\mathrm{char}\, k \neq 2,3,5$. Let V and W be 5-dimensional vector spaces over k. We agree to view an element $\phi \in \wedge^2 V \otimes W$ as a 5×5 as skew-symmetric matrix whose entries are linear forms on $\mathbf{P}^4 := \mathbf{P}(W^*)$. We write $C(\phi) \subset \mathbf{P}^4$ for the subscheme defined by the 4×4 Pfaffians of ϕ. Our starting point is

Proposition 1.1 *(i) Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic defined over k. Then $C = C(\phi)$ for some $\phi \in \wedge^2 V \otimes W$.*
(ii) The elliptic normal quintics are Zariski dense in $\wedge^2 V \otimes W$.

(i) We gave two different proofs in [11][1]. The first interprets V^* as the global sections of the unique indecomposable rank 2 vector bundle over C with determinant the hyperplane section. The second, which depends on a description of Gorenstein ideals in codimension 3 due to Buchsbaum and Eisenbud, interprets V as the space of quadrics containing C.
(ii) This follows from properties of the Grassmannian $\mathrm{Gr}(2,V)$. For details see [11, §2]. □

We call the 50-dimensional affine space $\wedge^2 V \otimes W$ the space of elliptic normal quintics. Theorem 1 describes the invariant subring for the action of

[1] Our notation differs in that we have replaced V by V^*.

$\mathrm{SL}(V) \times \mathrm{SL}(W)$ on $k[\wedge^2 V \otimes W]$. More generally for $\rho : \mathrm{GL}(V) \times \mathrm{GL}(W) \to \mathrm{GL}(Y)$ a linear representation we define

Definition 1.2 *A polynomial function $F : \wedge^2 V \otimes W \to Y$ is a* covariant *of weight $(p, q) \in \mathbf{Z}^2$ if*

$$F \circ (g_V, g_W) = (\det g_V)^p (\det g_W)^q \rho(g_V, g_W) \circ F \tag{4}$$

for all $(g_V, g_W) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$. If $Y = k$ is the trivial representation then F is called an invariant.

Remark 1.3 The only algebraic characters of $\mathrm{GL}(V) \times \mathrm{GL}(W)$ are of the form $(g_V, g_W) \mapsto (\det g_V)^p (\det g_W)^q$. So the invariants of Definition 1.2 are precisely the homogeneous polynomials in $k[\wedge^2 V \otimes W]$ invariant under the action of $\mathrm{SL}(V) \times \mathrm{SL}(W)$.

The main reason for considering covariants, and not just invariants, is that certain covariants are easy to write down. By manipulating these we construct further covariants, and if all goes well, eventually arrive at the invariants we seek. We shall take Y to be a homogeneous subspace of the tensor algebra generated by V, W, V^* and W^*. By homogeneous we mean that there are integers r and s such that $\rho(\lambda I_V, \mu I_W) = \lambda^r \mu^s I_Y$ for all $\lambda, \mu \in k^*$. It follows from (4) that

$$\begin{array}{rcl} 2 \deg F & = & 5p + r \\ \deg F & = & 5q + s. \end{array} \tag{5}$$

The most obvious example of a covariant is the identity map $U : \wedge^2 V \otimes W \to \wedge^2 V \otimes W$. It has degree 1 and weight (0,0). Identifying $\wedge^4 V = V^*$ there is a natural squaring map $P : \wedge^2 V \otimes W \to V^* \otimes S^2 W$. We call this the Pfaffian map, since the quadrics $\langle P(\phi), v \rangle$ for $v \in V$ are the 4×4 Pfaffians of ϕ. By definition these are also the quadrics defining $C(\phi)$. It is easy to see that P is a covariant of degree 2 and weight $(1, 0)$.

2 Orbits of codimension 1

Let $n \geq 3$ be an integer. Let k be an algebraically closed field with $\mathrm{char}\, k \nmid 6n$. We make some observations about elliptic normal curves of degree n and certain of their degenerations. We then return to the case $n = 5$ and, as a first step towards understanding the invariants, describe the orbits of codimension 1 for the action of $\mathrm{GL}(V) \times \mathrm{GL}(W)$ on $\wedge^2 V \otimes W$. Our assumptions on k will remain in force until the end of §11.

Definition 2.1 *(i) An* elliptic normal curve $C \subset \mathbf{P}^{n-1}$ *is a smooth curve of genus one and degree n spanning* $\mathbf{P}^{n-1}$.
(ii) A rational nodal curve $C \subset \mathbf{P}^{n-1}$ *is a rational curve of degree n, with a single node, spanning* $\mathbf{P}^{n-1}$.
(iii) A Néron polygon $C \subset \mathbf{P}^{n-1}$ *is the union of n lines $\ell_0, \ldots, \ell_{n-1}$, spanning $\mathbf{P}^{n-1}$ and arranged such that ℓ_i meets ℓ_j if and only if $i - j \equiv \pm 1 \pmod{n}$.*

Lemma 2.2 *The automorphisms of $\mathbf{P}^{n-1}$ act transitively on (i) the isomorphism classes of elliptic normal curves, (ii) the rational nodal curves and (iii) the Néron polygons.*

Proof. (i) Let $C, C' \subset \mathbf{P}^{n-1}$ be elliptic normal curves with $C \simeq C'$. We pick $0 \in C$ with $n.0$ linearly equivalent to the hyperplane section. Similarly we pick $0' \in C'$. Composing with a translation, if necessary, our isomorphism maps $0 \mapsto 0'$ and so extends to $\mathbf{P}^{n-1}$.
(ii) The linear system $\{f \in H^0(\mathbf{P}^1, \mathcal{O}_{\mathbf{P}^1}(n)) \mid f(0) = f(\infty)\}$ defines a morphism $\mathbf{P}^1 \to \mathbf{P}^{n-1}$ with image a rational nodal curve. It suffices to observe that every rational nodal curve arises in this way.
(ii) A Néron polygon is uniquely determined by its n vertices. The lemma reduces to a well known result. $\square$

Lemma 2.3 *Let $C \subset \mathbf{P}^{n-1}$ be either (i) an elliptic normal curve or (ii) a rational nodal curve. Then there are only finitely many automorphisms of C that extend to automorphisms of $\mathbf{P}^{n-1}$.*

Proof. (i) We say that $P \in C$ is a flex if $n.P$ is linearly equivalent to the hyperplane section. It is well known that C has n^2 flexes and that these span $\mathbf{P}^{n-1}$. An automorphism of C extends to $\mathbf{P}^{n-1}$ if and only if it permutes the flexes, and is uniquely determined by this permutation. A more careful argument gives the number of automorphisms as dn^2 where $d = 2, 4$ or 6.
(ii) Let C be the image of $(a : b) \mapsto (a^n + b^n : ab^{n-1} : \ldots : a^{n-1}b)$. The automorphisms that extend to $\mathbf{P}^{n-1}$ belong to the dihedral group generated by $(a : b) \mapsto (b : a)$ and $(a : b) \mapsto (a : \zeta_n b)$. $\square$

We return to the case $n = 5$. The curves of Definition 2.1 will be called elliptic normal quintics, rational nodal quintics and Néron pentagons respectively. In §1 we introduced 5-dimensional vector spaces V and W and identified $\wedge^2 V \otimes W$ as the space of elliptic normal quintics.

Proposition 2.4 *Let $G := \mathrm{GL}(V) \times \mathrm{GL}(W)$ act on $\wedge^2 V \otimes W$. Then there is an orbit of codimension 1 for each isomorphism class of elliptic curves, as determined by the j-invariant, and exactly one further orbit of codimension 1 corresponding to the rational nodal quintics.*

We need some lemmas.

Lemma 2.5 *Let $C(\phi) \subset \mathbf{P}^4$ satisfy one of the conditions of Definition 2.1.*
(i) If $C(\phi) = C(\phi')$ as subschemes of $\mathbf{P}^4$ then $\phi' = (g_V, 1)\phi$ for some $g_V \in \mathrm{GL}(V)$. Furthermore g_V is unique up to sign.
(ii) If $C(\phi) \simeq C(\phi')$ as curves then $\phi' = (g_V, g_W)\phi$ for some $(g_V, g_W) \in G$.
(iii) If $C(\phi)$ is either an elliptic normal quintic or a rational nodal quintic then the stabiliser of ϕ has finite image in $\mathrm{PGL}(V) \times \mathrm{PGL}(W)$.

Proof. (i) For an elliptic normal quintic this is [11, Prop. 9.4]. The alternative proof given at the end of [11, §10] immediately carries over to the degenerate case.
(ii) We apply Lemma 2.2 and the existence part of (i).
(iii) We apply Lemma 2.3 and the uniqueness part of (i). The corresponding statement for a Néron pentagon is false. □

Lemma 2.6 *Let $C(\phi)$ be either an elliptic normal quintic or a rational nodal quintic. Then the orbit of ϕ under the action of G has codimension 1 in $\wedge^2 V \otimes W$. In particular the closure of the orbit of ϕ is the zero locus of an irreducible invariant.*

Proof. The first statement follows from Proposition 2.5(iii) on counting dimensions. For the second statement we note that the only algebraic characters of G are of the form $(g_V, g_W) \mapsto (\det g_V)^p (\det g_W)^q$. □

Lemma 2.7 *Let $Z' \subset \mathrm{Gr}(5, \wedge^2 V)$ be the set of 4-planes $\Pi \subset \mathbf{P}(\wedge^2 V)$ for which $\mathrm{Gr}(2, V) \cap \Pi$ is not an elliptic normal quintic. Then Z' is closed and irreducible.*

Proof. According to the proof of Proposition 1.1(ii), $Z' \subset \mathrm{Gr}(5, \wedge^2 V)$ is the set of Π for which $\mathrm{Gr}(2, V) \cap \Pi$ is not a smooth curve. So it suffices to prove a form of Bertini's theorem [13, II.8.18]. For $x \in \mathrm{Gr}(2, V)$ let $B_x \subset \mathrm{Gr}(5, \wedge^2 V)$ be the set of 4-planes Π satisfying (i) $x \in \Pi$, and (ii) $\dim T_x \mathrm{Gr}(2, V) \cap T_x \Pi > 1$. These are the bad points with respect to x. Let

$$B = \{(x, \Pi) \in \mathrm{Gr}(2, V) \times \mathrm{Gr}(5, \wedge^2 V) \mid \Pi \in B_x\}.$$

We write p_1 and p_2 for the first and second projections. Since $p_1(B) = \mathrm{Gr}(2, V)$ and each fibre B_x is irreducible, it follows that B is irreducible. We deduce that $Z' = p_2(B)$ is closed and irreducible. $\square$

Lemma 2.8 *Let $Z \subset \wedge^2 V \otimes W$ be the set of ϕ for which $C(\phi)$ is not an elliptic normal quintic. Then Z is closed and irreducible.*

Proof. There is a rational map $\kappa : \wedge^2 V \otimes W \dashrightarrow \mathrm{Gr}(5, \wedge^2 V)$ that associates to ϕ the corresponding subspace $\Pi \subset \wedge^2 V$. Let $Z_1 \subset \wedge^2 V \otimes W$ be the set of ϕ that fail to span W. It follows by Definition 1.2 that all invariants of positive degree vanish on Z_1. On the complement of Z_1, κ is a morphism with irreducible fibres. We write Z_2 for the closure of $\kappa^{-1}(Z')$, so that $Z_2 \subset \wedge^2 V \otimes W$ is closed and irreducible. Then $Z = Z_1 \cup Z_2$ and it suffices to show that $Z = Z_2$. But applying Lemma 2.6 in the case of a rational nodal quintic shows that Z_2 is the zero locus of an invariant. Thus $Z_1 \subset Z_2$ and $Z = Z_2$ as required. $\square$

Proof of Proposition 2.4. According to Lemmas 2.5 and 2.6 there are orbits of codimension 1 as specified. Let $Z \subset \wedge^2 V \otimes W$ be the subset defined in Lemma 2.8. Since the rational nodal quintics are dense in Z, there is no room left for any further orbits of codimension 1. $\square$

We prove a weak form of Theorem 1.

Proposition 2.9 *There are irreducible invariants c_4, c_6 and Δ such that*
(i) $C(\phi) \subset \mathbf{P}^4$ is an elliptic normal quintic if and only if $\Delta(\phi) \neq 0$.
(ii) If (i) holds then

$$\begin{array}{lcl} j(C(\phi)) = 0 & \iff & c_4(\phi) = 0 \\ j(C(\phi)) = 1728 & \iff & c_6(\phi) = 0. \end{array}$$

Proof. We construct c_4 and c_6 by applying Lemma 2.6 with ϕ an elliptic normal quintic of the appropriate j-invariant. Likewise Δ is constructed from the rational nodal quintics. The remaining statements follow by Proposition 2.4 and Lemma 2.8. $\square$

This construction sheds no light on the following important questions.

- How are c_4, c_6 and Δ related?
- What are the degrees and weights?
- Given ϕ, how might one practically compute $c_4(\phi)$, $c_6(\phi)$ and $\Delta(\phi)$?

For $n = 2, 3, 4$ we may answer these questions by writing down c_4, c_6 and Δ as explicit polynomials. However in the case $n = 5$ we believe that the invariants are too large to write down. To make explicit computations feasible we restrict our covariants to the modular curve $X(5) \subset \mathbf{P}(\wedge^2 V \otimes W)$. Over the next three sections we develop a practical method for deciding which forms on $X(5)$ arise in this way.

3 Some modular curves

We review the facts we need about the modular curve $X(n)$, with special attention to the case $n = 5$.

Let $n \geq 3$ be an integer, and let $\zeta_n \in k$ be a primitive nth root of unity. The Heisenberg group H_n is the subgroup of GL_n generated by

$$\theta(\sigma) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix}, \qquad \theta(\tau) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}. \tag{6}$$

As our notation indicates, we prefer to view H_n as an abstract group with generators σ and τ. Then (6) defines a faithful representation $\theta : H_n \to \mathrm{GL}_n$ called the Schrödinger representation. We write $\overline{\theta} : H_n \to \mathrm{PGL}_n$ for the corresponding projective representation, and also put

$$\overline{\nu}(-I) \propto \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \end{pmatrix}. \tag{7}$$

The modular curve $Y(n)$ parametrises the isomorphism classes of triples (E, P, Q), where E is an elliptic curve and $P, Q \in E[n]$ satisfy $e_n(P, Q) = \zeta_n$. We write τ_P and τ_Q for the translation maps by P and Q respectively.

Lemma 3.1 *Let $n \geq 3$ be an odd integer and let (E, P, Q) be a triple as above. If we embed $E \subset \mathbf{P}^{n-1}$ via the complete linear system $|n.0|$ then there is a unique choice of co-ordinates on $\mathbf{P}^{n-1}$ such that τ_P, τ_Q and $[-1]$ are given by $\overline{\theta}(\sigma)$, $\overline{\theta}(\tau)$ and $\overline{\nu}(-I)$.*

Proof. This is well known. See for example [8], [9]. □

For $n \geq 5$ we obtain an embedding $X(n) \subset \mathbf{P}^{n-1}$, given on the open subset $Y(n)$ by $(E, P, Q) \mapsto 0$. In fact $X(n) \subset \mathbf{P}(A)$ where

$$A = \{(0, a_1, a_2, \ldots, -a_2, -a_1)\} \subset k^n$$

is an eigenspace for the action of $\overline{\nu}(-I)$. We write $(x_0 : x_1 : \ldots : x_{n-1})$ for our co-ordinates on $\mathbf{P}^{n-1}$ and agree to read all subscripts mod n.

Definition 3.2 *(i) Let $A(n) \subset \mathbf{P}(A)$ be the subscheme defined by the 4×4 Pfaffians of the matrix $(a_{i-j}a_{i+j})_{i,j=0}^{n-1}$.*
(ii) Let $\mathcal{A}(n) \subset A(n) \times \mathbf{P}^{n-1}$ be the subscheme defined by the 4×4 Pfaffians of the matrix $(a_{i-j}x_{i+j})_{i,j=0}^{n-1}$.

Proposition 3.3 *Let $n \geq 5$ be an odd integer and let (E, P, Q) be a triple as above. If we embed $E \subset \mathbf{P}^{n-1}$ as described in Lemma 3.1 then*
(i) $E \cap \mathbf{P}(A) = \{0\}$, and
(ii) E is the fibre of $\mathcal{A}(n) \to A(n)$ above 0.

Proof. See [8], [11]. □

We obtain equations for $X(n)$ for some small values of n

$$X(5) = \mathbf{P}^1 \qquad\qquad X(7) = \{a^3b + b^3c + c^3a = 0\} \subset \mathbf{P}^2$$

$$X(9) = \left\{ \begin{array}{rcl} a^2b + b^2c + c^2a & = & 0 \\ ab^2 + bc^2 + ca^2 & = & d^3 \end{array} \right\} \subset \mathbf{P}^3.$$

In the case $n = p$ is prime, Vélu [24] has shown that $X(p) = A(p)$. Accordingly we write $\mathcal{X}(p) \to X(p)$ instead of $\mathcal{A}(p) \to A(p)$.

There is an action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ on $X(n)$ given by relabelling torsion. Explicitly $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ acts on $Y(n)$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : (E, P, Q) \mapsto (E, aP + bQ, cP + dQ). \tag{8}$$

It is well known that the quotient of $X(n)$ by this action is the j-line, and that the cusps of $X(n)$ are the points above $j = \infty$. It follows by Lemma 3.1 that $\overline{\nu}(-I)$ extends uniquely to a projective representation

$$\overline{\nu} : \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{PGL}_n$$

satisfying

$$\overline{\nu}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \ \overline{\theta}(\sigma^u \tau^v) \ \overline{\nu}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \propto \ \overline{\theta}(\sigma^{au+cv}\tau^{bu+dv}). \tag{9}$$

By construction, $\overline{\nu}$ acts on $\mathbf{P}(A)$ and its restriction to $Y(n) \subset \mathbf{P}(A)$ is given by (8). Fixing generators

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{10}$$

for $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ we find

$$\overline{\nu}(S) \propto (\zeta_n^{ij})_{i,j=0}^{n-1}, \qquad \overline{\nu}(S^{-1}TS) \propto (\zeta_n^{i^2/2}\delta_{ij})_{i,j=0}^{n-1}. \tag{11}$$

This defines an action of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ on the family $\mathcal{A}(n) \to A(n)$. In [8] we used this action both to find the cusps of $X(n)$ and to describe the degenerate fibres. The formulae (11) could also be used to show that the action of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ on $\mathbf{P}(A)$ is irreducible, and hence that $X(n)$ spans $\mathbf{P}(A)$. In this article we use the action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ to help recover the covariants from their restrictions to $X(5)$.

Specialising to the case $n = 5$ we identify $X(5) = \mathbf{P}(A)$ where

$$A = \{(0, a, b, -b, -a)\} \subset k^5.$$

The family of curves $\mathcal{X}(5) \to X(5)$ is defined by quadrics

$$p_i := abx_i^2 + b^2 x_{i+1}x_{i+4} - a^2 x_{i+2}x_{i+3}.$$

These are the 4×4 Pfaffians of the matrix

$$\begin{pmatrix} 0 & bx_3 & -ax_1 & ax_4 & -bx_2 \\ -bx_3 & 0 & bx_4 & -ax_2 & ax_0 \\ ax_1 & -bx_4 & 0 & bx_0 & -ax_3 \\ -ax_4 & ax_2 & -bx_0 & 0 & bx_1 \\ bx_2 & -ax_0 & ax_3 & -bx_1 & 0 \end{pmatrix}.$$

We rewrite this matrix in the notation of §1. In terms of bases $v_0, \ldots, v_4$ and $x_0, \ldots, x_4$ for V and W it is given by[2]

$$u(a,b) \quad = \quad a \sum (v_1 \wedge v_4)x_0 + b \sum (v_2 \wedge v_3)x_0.$$

This defines a linear map $u : A \to \wedge^2 V \otimes W$ with the property that the fibre $C(\phi)$ of $\mathcal{X}(5) \to X(5)$ above $(a:b)$ is given by $\phi = u(a,b)$. The action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ tells us that the cusps are the roots of

$$D(a,b) = ab(a^{10} - 11a^5b^5 - b^{10}) \tag{12}$$

and that the fibre at each cusp is a Néron pentagon.

To bridge the gap between the rational nodal quintics and the Néron pentagons we consider

$$u_1(\lambda_0, \ldots, \lambda_4) \quad = \quad \sum \lambda_0 (v_1 \wedge v_4)x_0 + \sum (v_2 \wedge v_3)x_0. \tag{13}$$

This family of curves was studied in [8], [9]. We restate [9, Lemma 2.9] in the language of invariants.

Lemma 3.4 *Let $F \in k[\wedge^2 V \otimes W]$ be an invariant. Then $f_1 = F \circ u_1$ is a polynomial in $\lambda := \prod \lambda_i$.*

Proof. Putting $g_V = \mathrm{Diag}(1, \alpha, 1, 1, \alpha)$ and $g_W = \mathrm{Diag}(\alpha, 1, 1, 1, 1)$ we find

$$(g_V, g_W)\, u_1(\lambda_0, \ldots, \lambda_4) = \alpha\, u_1(\alpha^2 \lambda_0, \alpha^{-1}\lambda_1, \lambda_2, \lambda_3, \alpha^{-1}\lambda_4). \tag{14}$$

[2]The summations are over all cyclic permutations of the subscripts.

The formulae (5) with $r = s = 0$ give $2p + q = \deg F$. By (4) we have

$$f_1(\lambda_0, \ldots, \lambda_4) = f_1(\alpha^2\lambda_0, \alpha^{-1}\lambda_1, \lambda_2, \lambda_3, \alpha^{-1}\lambda_4).$$

If $\lambda \neq 0$ then repeated application of this identity, and its cyclic permutes, shows that $f_1(\lambda_0, \ldots, \lambda_4)$ only depends on λ. The lemma follows. $\square$

Since $\phi = u_1(0, 0, 0, 0, 0)$ is a Néron pentagon and $\phi' = u_1(0, 1, 1, 1, 1)$ is a rational nodal quintic, we deduce

Corollary 3.5 *Let $F \in k[\wedge^2 V \otimes W]$ be an invariant. Then $F(\phi) \neq 0$ for ϕ a Néron pentagon if and only if $F(\phi') \neq 0$ for ϕ' a rational nodal quintic.*

The next lemma will help us describe the ring of invariants.

Lemma 3.6 *Let $F \in k(\wedge^2 V \otimes W)$ be a rational invariant, i.e. a rational function satisfying (4). Then F is regular if and only if $f = F \circ u$ is regular.*

Proof. Suppose that f is regular and write $F = R/S$ where R and S are coprime invariants. We suppose for a contradiction that S has positive degree. Then $S(\phi) = 0$ for some $\phi = u(a, b)$ and $R(\phi) = f(a, b)S(\phi) = 0$. If ϕ is an elliptic normal quintic then it follows by Lemma 2.6 that R and S have a common factor. This is a contradiction. It remains to consider ϕ a Néron pentagon. But in that case Corollary 3.5 gives $R(\phi') = S(\phi') = 0$ for ϕ' a rational nodal quintic. We use Lemma 2.6 to conclude as before. $\square$

The analogue of Lemma 3.6 for covariants is false. However the technique of Lemma 3.4 is still useful. We record the necessary formulae.

Lemma 3.7 *Let $F : \wedge^2 V \otimes W \to Y$ be a covariant. We put $f = F \circ u$ and $f_1 = F \circ u_1$. Let $\lambda_0, \ldots, \lambda_4 \in k$ with $\prod \lambda_i = a^5$ and $\alpha_0, \ldots, \alpha_4 \in k$ with $\prod \alpha_i = 1$. Suppose that the λ_i and α_i are related via*

$$\alpha_i^2/(\alpha_{i+1}\alpha_{i+4}) = \lambda_i/a \qquad (15)$$

$$\alpha_i^5 = \lambda_i^2/(\lambda_{i+2}\lambda_{i+3}). \qquad (16)$$

Then

$$f_1(\lambda_0, \ldots, \lambda_4) = \rho_Y(g_V, g_W) f(a, 1) \qquad (17)$$

where $g_V = \mathrm{Diag}(\alpha_1\alpha_4, \alpha_0\alpha_2, \ldots, \alpha_0\alpha_3)$ and $g_W = \mathrm{Diag}(\alpha_0, \ldots, \alpha_4)$.

Proof. We apply the definition (4) to (14) and its cyclic permutes. $\square$

Remark 3.8 In practice we are given f and wish to compute f_1. We use (15) to eliminate α_2, α_3, α_4 from the right hand side of (17). Then we use (16) to eliminate α_0 and α_1.

4 The extended Heisenberg group

We introduce more of the technical machinery needed to recover a covariant from its restriction to $X(5)$.

Let $n \geq 3$ be an odd integer. The Heisenberg group $H_n \subset \mathrm{SL}_n$ is the subgroup generated by the matrices $\theta(\sigma)$ and $\theta(\tau)$ of §3. It is a non-abelian group of order n^3 with centre generated by $\zeta := \sigma\tau\sigma^{-1}\tau^{-1}$. Let $\overline{H}_n$ be the quotient of H_n by its centre. There is an exact sequence

$$0 \longrightarrow \mu_n \longrightarrow H_n \longrightarrow \overline{H}_n \longrightarrow 0$$

and a bilinear pairing on $\overline{H}_n$ defined by $e_n(\overline{x}, \overline{y}) = xyx^{-1}y^{-1}$. It is easy to see that e_n is alternating and non-degenerate. Taking $\overline{\sigma}, \overline{\tau}$ as our basis for $\overline{H}_n$ there is a natural group homomorphism $\beta : \mathrm{Aut}(H_n) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$. The kernel of β is the group of inner automorphisms of H_n, *i.e.* a copy of $\overline{H}_n$.

Let N_n be the normaliser of H_n in SL_n. Then N_n acts on H_n via conjugation, and the corresponding action on $\overline{H}_n$ preserves the pairing e_n. Conversely, Lemma 3.1 tells us that every such automorphism of $\overline{H}_n$ arises in this way. We obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_n & \longrightarrow & N_n & \stackrel{\alpha}{\longrightarrow} & \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \overline{H}_n & \longrightarrow & \mathrm{Aut}(H_n) & \stackrel{\beta}{\longrightarrow} & \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & 0. \end{array} \tag{18}$$

The group N_5 was used by Horrocks and Mumford [14] in their construction of an indecomposable rank 2 vector bundle on $\mathbf{P}^4$. In fact the number $|N_5| = 15,000$ appears in the title of their paper.

We make a choice of involution $\iota \in \mathrm{Aut}(H_n)$ with $\beta(\iota) = -I$. The second row of (18) allows us to identify $\mathrm{Aut}(H_n)$ as a group of affine transformations. Since n is odd, our choice of ι uniquely determines a section[3] s_β for β with

[3]We require that our sections are group homomorphisms.

$s_\beta(-I) = \iota$. Indeed the image of s_β is the centraliser of ι in $\mathrm{Aut}(H_n)$. The middle vertical map of (18) factors through $\overline{N}_n$, the image of N_n in PGL_n. So the restriction of s_β to $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ determines a projective representation

$$\overline{\omega} : \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{PGL}_n\,.$$

The extended Heisenberg group is the semi-direct product

$$H_n^+ := H_n \ltimes \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$$

with group law $(h,\gamma)(h',\gamma') = (h\, s_\beta(\gamma)h', \gamma\gamma')$. The inclusion of H_n^+ in GL_n will be called the extended Schrödinger representation. But in order to identify $H_n^+ = N_n$ we must first fix a section for the map α compatible with s_β. More precisely

Lemma 4.1 *The following objects are in natural 1-1 correspondence.*
(i) Sections s_α for α compatible with s_β.
(ii) Lifts of $\overline{\omega} : \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{PGL}_n$ to $\omega : \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{GL}_n$.
(iii) Extensions of $\theta : H_n \to \mathrm{GL}_n$ to $\theta^+ : H_n^+ \to \mathrm{GL}_n$.

Proof. The projective representation $\overline{\omega}$ is defined by the requirement

$$\overline{\omega}(\gamma)\ h\ \overline{\omega}(\gamma)^{-1} = s_\beta(\gamma)h \qquad \text{for all } h \in H_n,\ \gamma \in \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}). \tag{19}$$

But to say that s_α is a section for the map α compatible with s_β means

$$s_\alpha(\gamma)\ h\ s_\alpha(\gamma)^{-1} = s_\beta(\gamma)h \qquad \text{for all } h \in H_n,\ \gamma \in \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}). \tag{20}$$

The correspondence between (i) and (ii) is clear. Now given s_α compatible with s_β we define $\theta^+(h,\gamma) = hs_\alpha(\gamma)$ and check using (20) that θ^+ is a homomorphism. Conversely, given θ^+ we set $s_\alpha(\gamma) = \theta^+(1,\gamma)$. This gives the correspondence between (i) and (iii). $\square$

We fix, once and for all, our choice of involution $\iota \in \mathrm{Aut}(H_n)$. We take $\iota(\sigma) = \sigma^{-1}$ and $\iota(\tau) = \tau^{-1}$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ it follows that

$$s_\beta(\gamma) : \sigma \mapsto \zeta^{-ac/2}\sigma^a\tau^c;\ \tau \mapsto \zeta^{-bd/2}\sigma^b\tau^d.$$

Substituting in (19) we see that $\overline{\omega}(\gamma)$ is uniquely determined by

$$\begin{aligned} \overline{\omega}(\gamma)\theta(\sigma)\overline{\omega}(\gamma)^{-1} &= \zeta_n^{-ac/2}\theta(\sigma^a\tau^c) \\ \overline{\omega}(\gamma)\theta(\tau)\overline{\omega}(\gamma)^{-1} &= \zeta_n^{-bd/2}\theta(\sigma^b\tau^d). \end{aligned}$$

Comparison with (9) shows that the projective representations $\overline{\nu}$ and $\overline{\omega}$ differ only by the automorphism $\gamma \mapsto (\gamma^T)^{-1} = S^{-1}\gamma S$ of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$. In particular we have explicit expressions (11) for $\overline{\omega}(S)$ and $\overline{\omega}(T)$.

We temporarily adopt the notation $\mathbf{P}^{n-1} = \mathbf{P}(U)$ where U is an n-dimension vector space. The action of $\overline{\omega}(-I)$ gives an eigenspace decomposition $U = U_+ \oplus U_-$ with $\dim U_\pm = (n \pm 1)/2$. We use this decomposition to give criteria for $\overline{\omega}$ to lift to GL_n.

Lemma 4.2 *Suppose we are given lifts $\omega(S)$ and $\omega(T)$ for $\overline{\omega}(S)$ and $\overline{\omega}(T)$, and characters $\chi_\pm : \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \to k^*$ such that $\omega(S)$ and $\omega(T)$ restricted to $U_\pm$ have determinants $\chi_\pm(S)$ and $\chi_\pm(T)$. Then ω extends uniquely to a lifting of $\overline{\omega}$.*

Proof. Let $\gamma \in \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$. We claim that there is a unique lifting $\omega(\gamma)$ of $\overline{\omega}(\gamma)$ whose restriction to $U_\pm$ has determinant $\chi_\pm(\gamma)$. The existence follows from our assumptions in the cases $\gamma = S, T$. The uniqueness relies on the fact that $\dim U_+$ and $\dim U_-$ are coprime. It is evident that ω, so defined, is a group homomorphism. $\square$

Lemma 4.3 *The group $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ has $\gcd(3, n)$ 1-dimensional characters. Moreover each character is uniquely determined by its value at T.*

Proof. This follows from the relations $(ST)^3 = S^4 = T^n = I$. The characters in the case $3 \mid n$ factor through $\mathrm{PSL}_2(\mathbf{Z}/3\mathbf{Z}) \simeq A_4$. $\square$

Lemma 4.4 *The projective representation $\overline{\omega}$ lifts to GL_n. The number of such liftings is $\gcd(3, n)$.*

Proof. Since $3(1^2 + 2^2 + \ldots + (\frac{n-1}{2})^2) \equiv 0 \pmod{n}$ it follows from (11) and Lemma 4.3 that we may choose $\omega(T)$ and $\chi_\pm$ satisfying the hypotheses of Lemma 4.2. We scale $\omega(S)$ such that

$$\omega(S)\omega(T)^{-1}\omega(S) = \omega(T)\omega(S)\omega(T). \tag{21}$$

We check the remaining hypotheses of Lemma 4.2 by restricting to $U_\pm$ and taking determinants in (21). This proves the existence of a lifting ω. Since any two liftings differ by a 1-dimensional character, the number of liftings is determined by Lemma 4.3. $\square$

Remark 4.5 Explicit calculations show that $\omega(S) = g_n^{-1}(\zeta_n^{ij})_{i,j=0}^{n-1}$ where the Gauss sum $g_n = \sum_{i=0}^{n-1} \zeta_n^{-i^2/2}$ satisfies $g_n^2 = (-1)^{(n-1)/2}n$.

Remark 4.6 For $n = p$ is a prime it is known [16, V, Satz 25.5] that the group of Schur multipliers $H^2(\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}), k^*)$ is trivial. This gives an alternative proof of Lemma 4.4.

Corollary 4.7 *The Schrödinger representation $\theta : H_n \to \mathrm{GL}_n$ extends to a representation $\theta^+ : H_n^+ \to \mathrm{GL}_n$. If n is prime to 6 then θ^+ is unique.*

Proof. We combine Lemmas 4.1 and 4.4. $\square$

Remark 4.8 We say that two representations of H_n are conjugate if they differ by an automorphism of H_n. The Schrödinger representation has $\phi(n)$ conjugates, one for each primitive nth root of unity. We may apply Corollary 4.7 to any one of these representations.

5 The discrete covariants

We return to the case $n = 5$. In §3 we considered the family of curves

$$u(a, b) \quad = \quad a \sum (v_1 \wedge v_4)x_0 + b \sum (v_2 \wedge v_3)x_0.$$

We choose conjugates of the Schrödinger representation that make $u(a, b)$ Heisenberg invariant

$$\begin{array}{lll} \theta_V : H_5 \to \mathrm{GL}(V)\,; & \sigma : v_i \mapsto \zeta_5^{2i} v_i\,; & \tau : v_i \mapsto v_{i+1} \\ \theta_W : H_5 \to \mathrm{GL}(W)\,; & \sigma : x_i \mapsto \zeta_5^{i} x_i\,; & \tau : x_i \mapsto x_{i+1}. \end{array} \tag{22}$$

We continue to write θ_V and θ_W for the extensions of these representations to H_5^+ as determined by Corollary 4.7.

Let $\mathrm{Stab}(\phi) \subset \mathrm{SL}(V) \times \mathrm{SL}(W)$ be the stabiliser of $\phi \in \wedge^2 V \otimes W$. If ϕ is an elliptic normal quintic, we write $H(\phi) \subset \mathrm{Stab}(\phi)$ for the subgroup[4] acting on $C(\phi)$ by translations. We also write $N(\phi)$ for the normaliser of $H(\phi)$ in $\mathrm{SL}(V) \times \mathrm{SL}(W)$. In the case $\phi = u(a, b)$ we relate these groups to the exact sequence

$$0 \longrightarrow H_5 \longrightarrow H_5^+ \longrightarrow \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) \longrightarrow 0. \tag{23}$$

[4]In fact we shall see in Lemma 12.2 that $H(\phi) = \mathrm{Stab}(\phi)$.

Lemma 5.1 *Let $\phi = u(a,b)$ be an elliptic normal quintic. Then*
(i) $H(\phi) = \{(\theta_V(h), \theta_W(h)) \mid h \in H_5\}$.
(ii) $N(\phi) = \{(\zeta_V \theta_V(h^+), \zeta_W \theta_W(h^+)) \mid \zeta_V, \zeta_W \in \mu_5,\ h^+ \in H_5^+\}$.

Proof. (i) We saw in §3 that the translation automorphisms of $C(\phi)$ extending to $\mathbf{P}^4$ are described by the Heisenberg group. Notice that by working with $\mathrm{SL}(V) \times \mathrm{SL}(W)$ we have removed the sign ambiguity of Lemma 2.5(i).
(ii) The inclusion "$\supset$" is clear from (23). So let $(g_V, g_W) \in N(\phi)$. Then g_V belongs to the normaliser of H_5 in $\mathrm{SL}(V)$. The construction of the extended Heisenberg group shows that $g_V = \theta_V(h^+)$ for some $h^+ \in H_5^+$. This reduces us to the case $g_V = I_V$. But now g_W belongs to the centraliser of H_5 in $\mathrm{SL}(W)$. It follows that g_W is a scalar matrix as required. □

The representations θ_V and θ_W, or more precisely their extensions to H_5^+, define actions of $\Gamma := \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on $A \subset W^*$ and on $(\wedge^2 V \otimes W)^{H_5}$.

Lemma 5.2 *The linear map $u : A \to (\wedge^2 V \otimes W)^{H_5}$ is an isomorphism of Γ-modules.*

Proof. We compute the character of the H_5-representation $\wedge^2 V \otimes W$. It is constant on the centre of H_5 and zero elsewhere. Thus $\dim(\wedge^2 V \otimes W)^{H_5} = 2$ and u is an isomorphism of vector spaces. Now suppose that $\gamma \in \Gamma$ maps $\phi = u(a,b)$ to $\phi' = u(a',b')$. Then γ acts on $\mathbf{P}(A) \subset \mathbf{P}^4$ but maps $C(\phi) \subset \mathbf{P}^4$ to $C(\phi') \subset \mathbf{P}^4$. By Lemma 3.3(i) we have

$$\gamma : (0 : a : b : -b : -a) \mapsto (0 : a' : b' : -b' : -a').$$

So $\gamma(a,b) \propto (a',b')$ and the lemma holds up to scalars. We are done since Γ has no 1-dimensional characters. □

The action of Γ on $A \subset W^*$ is given by $\chi : \Gamma \to \mathrm{GL}(A)$ where

$$\begin{aligned} \chi(S) : &\quad (a,b) \mapsto (\phi a + b, a - \phi b)/(\zeta_5^4 - \zeta_5) \\ \chi(T) : &\quad (a,b) \mapsto (\zeta_5^2 a, \zeta_5^3 b) \end{aligned}$$

and $\phi = (\zeta_5 - \zeta_5^4)/(\zeta_5^2 - \zeta_5^3)$. Up to equivalence this is a lifting of the action (8) of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5) = \mathbf{P}(A)$. If we use the exact sequence (23) to extend χ to H_5^+ then Lemma 5.2 takes the form

$$u \circ \chi(h^+) = (\theta_V(h^+), \theta_W(h^+)) \circ u \quad \text{for all } h^+ \in H_5^+. \tag{24}$$

Now let $F : \wedge^2 V \otimes W \to Y$ be a covariant and let $f = F \circ u$ be the restriction of F to $X(5)$. We give Y the structure of H_5^+-module via

$$\pi(h^+) = \rho_Y(\theta_V(h^+), \theta_W(h^+)) \quad \text{for all } h^+ \in H_5^+. \tag{25}$$

Then

$$\begin{aligned} f \circ \chi(h^+) &= F \circ u \circ \chi(h^+) & \\ &= F \circ (\theta_V(h^+), \theta_W(h^+)) \circ u & \text{by (24)} \\ &= \rho_Y(\theta_V(h^+), \theta_W(h^+)) \circ F \circ u & \text{by Definition 1.2} \\ &= \pi(h^+) \circ f & \text{by (25)} \end{aligned}$$

We obtain a Γ-equivariant map $f : A \to Y^{H_5}$. More generally for $\pi : \Gamma \to \mathrm{GL}(Z)$ a linear representation we define

Definition 5.3 *A homogeneous polynomial function $f : A \to Z$ is a* discrete covariant *if $f \circ \chi(\gamma) = \pi(\gamma) \circ f$ for all $\gamma \in \Gamma$. If $Z = k$ is the trivial representation then f is called a* discrete invariant.

The discrete covariants are easy to compute. In §7 we give a complete classification, by first reducing to the case where π is irreducible.

Lemma 5.4 *A covariant $F : \wedge^2 V \otimes W \to Y$ is uniquely determined by its corresponding discrete covariant $f = F \circ u : A \to Y^{H_5}$.*

Proof. In §§1,2 we saw that $\mathrm{GL}(V) \times \mathrm{GL}(W)$ acts transitively on each isomorphism class of elliptic curves and that the elliptic normal quintics are dense in $\wedge^2 V \otimes W$. We are done since $X(5)$ covers the j-line. □

It is therefore reasonable to make the definition

Definition 5.5 *Let $f : A \to Y^{H_5}$ be a discrete covariant. We say that f is a* covariant *if $f = F \circ u$ for some covariant $F : \wedge^2 V \otimes W \to Y$.*

There are essentially two different ways in which a discrete covariant may fail to be a covariant.

Fractional weights. Given f a discrete covariant, we may compute its weights using (5). If these fail to be integers then f is not a covariant.

Example. The discrete invariant $D(a, b) = ab(a^{10} - 11a^5b^5 - b^{10})$ has degree 12. By (5) it has weights (24/5,12/5) and so cannot be an invariant. Another example, this time with $Y = S^5W$, is

$$(a, b) \mapsto ab \sum x_0^5 - 5b^2 \sum x_0^3 x_1 x_4 + 5a^2 \sum x_0^3 x_2 x_3 - 30ab \prod x_0.$$

By (5) it has weights $(4/5, -3/5)$ and so cannot be a covariant.

Denominators. We generalise the notion of covariant to that of *rational covariant*, by which we mean a rational map $F : \wedge^2 V \otimes W - \to Y$ satisfying (4). Let $f = F \circ u$ be the corresponding rational discrete covariant. It may happen that f is regular even when F is not. In such cases the proof of Lemma 5.4 shows that f is not a covariant.

Example. Decomposing $(S^{10}W)^{H_5}$ as an Γ-module (see §11) we find that the trivial representation appears. So there is a discrete covariant of degree zero. But clearly there are no covariants of degree zero.

We prove that these are the only two obstructions.

Theorem 2 *Let $\rho : \mathrm{GL}(V) \times \mathrm{GL}(W) \to \mathrm{GL}(Y)$ be a homogeneous representation and let $f : A \to Y^{H_5}$ be an integer weight discrete covariant. Then there is a rational covariant $F : \wedge^2 V \otimes W - \to Y$ such that $f = F \circ u$.*

Proof. We are assuming that $\rho_Y(\lambda I_V, \mu I_W) = \lambda^r \mu^s I_Y$ for all $\lambda, \mu \in k^*$ and that there are integers p, q with

$$\begin{aligned} 2 \deg f &= 5p + r \\ \deg f &= 5q + s. \end{aligned} \tag{26}$$

Let $\phi \in \wedge^2 V \otimes W$ be an elliptic normal quintic. Then $\phi = (g_V, g_W) u(a, b)$ for some $(g_V, g_W) \in \mathrm{SL}(V) \times \mathrm{SL}(W)$ and $(a, b) \in A$. We define a rational map $F : \wedge^2 V \otimes W - \to Y$ via

$$F(\phi) = \rho_Y(g_V, g_W) f(a, b).$$

We must check that F is well defined. So suppose that $\phi' = (g_V, g_W)\phi$ with $\phi = u(a, b)$, $\phi' = u(a', b')$ and $(g_V, g_W) \in \mathrm{SL}(V) \times \mathrm{SL}(W)$. We aim to show that $f(a', b') = \rho_Y(g_V, g_W) f(a, b)$. By Lemma 5.1(i) we have $H(\phi) = H(\phi')$. So $(g_V, g_W) \in N(\phi)$ and Lemma 5.1(ii) tells us that

$$(g_V, g_W) = (\zeta_V \theta_V(h^+), \zeta_W \theta_W(h^+)) \tag{27}$$

for some $\zeta_V, \zeta_W \in \mu_5$, $h^+ \in H_5^+$. We compute

$$\begin{array}{rcll}
\phi' & = & \zeta_V^2 \zeta_W (\theta_V(h^+), \theta_W(h^+))\phi & \text{by (27)} \\
\Longrightarrow \quad (a', b') & = & \zeta_V^2 \zeta_W \chi(h^+)(a,b) & \text{by (24)} \\
\Longrightarrow \quad f(a', b') & = & \zeta_V^r \zeta_W^s f(\chi(h^+)(a,b)) & \text{by (26)} \\
& = & \zeta_V^r \zeta_W^s \pi(h^+) f(a,b) & \text{by Definition 5.3} \\
& = & \rho_Y(g_V, g_W) f(a,b) & \text{by (25) and (27).}
\end{array}$$

Thus F is a well defined rational map. It is clear from our construction that F satisfies (4) and that $f = F \circ u$. $\square$

Let Δ be the irreducible invariant introduced in §1. We recall that $C(\phi)$ is an elliptic normal quintic if and only if $\Delta(\phi) \neq 0$. In the case of a specific covariant, such as Δ, we shall use the same symbol both for the covariant and for its discrete covariant. This should not cause any confusion.

Corollary 5.6 *Let $\rho : \mathrm{GL}(V) \times \mathrm{GL}(W) \to \mathrm{GL}(Y)$ be a homogeneous representation and let $f : A \to Y^{H_5}$ be an integer weight discrete covariant. Let F be the rational covariant constructed in Theorem 2. Then*
(i) $\Delta^m f$ is a covariant for m sufficiently large,
(ii) f is a covariant if and only if $f_1 := F \circ u_1$ is regular.
Furthermore an integer weight discrete invariant is an invariant.

Proof. (i) By construction F is regular outside $\{\Delta = 0\}$. It follows that $\Delta^m F$ is regular for m sufficiently large.
(ii) It is clear that f_1 is regular whenever F is regular. For the converse we recall from §2 that $\phi = u_1(0, 1, 1, 1, 1)$ is a rational nodal quintic, and that the rational nodal quintics are dense in $\{\Delta = 0\}$. The statement concerning invariants follows from Lemma 3.6. $\square$

Remark 5.7 We use the formulae of Proposition 3.7 to construct f_1 directly from f. Thus Corollary 5.6 gives a practical method for deciding which discrete covariants are covariants. We give examples in §§8,10,11.

Remark 5.8 Let $f : A \to Y^{H_5}$ be a discrete covariant with weights (p, q). If $Y^{H_5} \neq 0$ then $2r + s \equiv 0 \pmod 5$. It follows by (26) that p is an integer if and only if q is an integer. In other words to demand that a discrete covariant has integer weights is really only one condition. This condition is a congruence mod 5 on the degree.

6 The invariants

We continue to assume that k is algebraically closed, and give a proof of Theorem 1 in this case.

Proposition 6.1 *The ring of invariants is generated by invariants c_4 and c_6 of degrees 20 and 30 respectively. If we set $\Delta = (c_4^3 - c_6^2)/1728$ then*
(i) $C(\phi) \subset \mathbf{P}^4$ is an elliptic normal quintic if and only if $\Delta(\phi) \neq 0$.
(ii) If (i) holds then $C(\phi)$ has Weierstrass equation

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

We begin by describing the discrete invariants. Since $\Gamma = \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ has no 1-dimensional characters, a homogeneous polynomial $f \in k[A]$ is a discrete invariant if and only if its roots are invariant under the action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z}) \simeq A_5$ on $X(5) \simeq \mathbf{P}(A)$. We recognise this as a classical problem and recall from [17, Part I, Chapter II, §13] the discrete invariants

$$\begin{aligned} D(a,b) &= ab(a^{10} - 11a^5b^5 - b^{10}) \\ c_4(a,b) &= -\tfrac{1}{121} \begin{vmatrix} \frac{\partial^2 D}{\partial a^2} & \frac{\partial^2 D}{\partial a \partial b} \\ \frac{\partial^2 D}{\partial a \partial b} & \frac{\partial^2 D}{\partial b^2} \end{vmatrix} \\ &= a^{20} + 228a^{15}b^5 + 494a^{10}b^{10} - 228a^5b^{15} + b^{20} \\ c_6(a,b) &= \tfrac{1}{20} \begin{vmatrix} \frac{\partial D}{\partial a} & \frac{\partial D}{\partial b} \\ \frac{\partial c_4}{\partial a} & \frac{\partial c_4}{\partial b} \end{vmatrix} \\ &= -a^{30} + 522a^{25}b^5 + 10005a^{20}b^{10} + 10005a^{10}b^{20} - 522a^5b^{25} - b^{30}. \end{aligned}$$

The roots of these polynomials correspond under stereographic projection to the vertices, faces and edges of an icosahedron. They are also the ramification points of the quotient map $j : X(5) \to \mathbf{P}^1$. We must have

$$j \propto c_4^3/D^5 \quad \text{and} \quad j - 1728 \propto c_6^2/D^5. \tag{28}$$

In particular D^5, c_4^3 and c_6^2 satisfy a linear dependence relation. Comparing a few coefficients we find $1728D^5 = c_4^3 - c_6^2$ and in fact this gives equality in (28). We arrive at the discrete analogue of Proposition 6.1.

Proposition 6.2 *The ring of discrete invariants is generated by D, c_4 and c_6 subject to the single relation $1728D^5 = c_4^3 - c_6^2$.*

(i) $\phi = u(a,b)$ is an elliptic normal quintic if and only if $D(a,b) \neq 0$.
(ii) If (i) holds then $C(\phi)$ has Weierstrass equation

$$y^2 = x^3 - 27c_4(a,b)x - 54c_6(a,b). \tag{29}$$

Proof. The orbits for the action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5)$ are the roots of the polynomials c_4, c_6, D and $c_4^3 - jD^5$ for $j \neq 0, 1728$. The discrete invariants are products of these polynomials.
(i) We saw in §3 that the cusps of $X(5)$ are the roots of D.
(ii) Since we are working over an algebraically closed field, it suffices to compare the j-invariants. The above discussion shows that $C(\phi)$ has j-invariant $1728c_4^3/(c_4^3 - c_6^2)$. This is also the j-invariant of (29). □

Proof of Proposition 6.1. The ring of discrete invariants is $k[D, c_4, c_6]$. The formulae (5) with $r = s = 0$ tell us that a discrete invariant has integer weights if and only if it has degree $d \equiv 0 \pmod 5$. So the ring of integer weight discrete invariants is $k[D^5, c_4, c_6] = k[c_4, c_6]$. By Corollary 5.6 this is the ring of invariants. We now set $\Delta = D^5$ and use Proposition 6.2 to identify c_4, c_6 and Δ as non-zero multiples of the invariants of the same name introduced in §2. This proves (i). For (ii) we reduce to the case $\phi = u(a,b)$ and apply Proposition 6.2(ii). □

Remark 6.3 We recall from §3 that the curves $C(\phi)$ for $\phi = u(a,b)$ have rational point $(0 : a : b : -b : -a)$. This makes it possible to prove Proposition 6.2 without the assumption that k is algebraically closed. Indeed in the notation of [8], [9], [10] we recognise $C(\phi)$ as the elliptic curve C_λ for $\lambda = a^5/b^5$. Then starting with the isogenous curve

$$D_\lambda : \quad y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2$$

we used Vélu's formulae [25] to compute a Weierstrass equation for C_λ. Substituting $\lambda = a^5/b^5$ gives (29) as required.

In §9 we give a practical algorithm for computing the invariants. Then in §12 we complete the proof of Theorem 1 by showing that over a non-algebraically closed field the invariants describe the Jacobian.

7 Computing the discrete covariants

Let $\Gamma = \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$. In §5 we defined a 2-dimensional irreducible representation $\chi : \Gamma \to \mathrm{GL}(A)$ and so an action of Γ on $k[A] = k[a, b]$. Let

$$R = k[A]^\Gamma = k[D, c_4, c_6]$$

be the ring of discrete invariants. The discrete covariants attached to the representation $\pi : \Gamma \to \mathrm{GL}(Z)$ form a graded R-module

$$M_\pi = \oplus_{d \geq 0} M_{\pi,d} = (k[A] \otimes Z_\pi)^\Gamma$$

where the grading is by degree. The aim of this section is to compute M_π for all representations π. We immediately reduce to the case where π is irreducible.

The character table for Γ is given in Appendix A. There are 5 even characters labelled $\psi_1, \ldots, \psi_5$ and 4 odd characters labelled $\chi_1, \ldots, \chi_4$. Naturally we use the same symbol both for a representation and its character. We have arranged that $\psi_1 = 1$ and that $\chi_1 = \chi$. We use the recurrence relation $S^{r+1}\chi \oplus S^{r-1}\chi \simeq S^r\chi \otimes \chi$ to compute the symmetric powers of χ.

$$\chi_1, \quad \psi_4, \quad \chi_3, \quad \psi_3, \quad \chi_4, \quad \psi_2 \oplus \psi_5, \quad \chi_2 \oplus \chi_4, \quad \psi_2 \oplus \psi_3, \quad \ldots$$

The integers $\dim M_{\pi,d}$ may be read off from this list. However we require more detailed information. We fix a basis $z_1, \ldots, z_m$ for Z_π and accordingly write $\Pi : \Gamma \to \mathrm{GL}_m$ for the representation satisfying

$$\pi(\gamma)[z_1, \ldots, z_m] \quad = \quad [\textstyle\sum_i \Pi(\gamma)_{i1} z_i, \ldots, \sum_i \Pi(\gamma)_{im} z_i].$$

A discrete covariant takes the form $[f_1, \ldots, f_m].[z_1, \ldots, z_m] := \sum f_i z_i$ where the $f_i \in k[A]$ are homogeneous polynomials of the same degree satisfying

$$[f_1, \ldots, f_m] \circ \chi(\gamma) \quad = \quad [\textstyle\sum_i \Pi(\gamma)_{1i} f_i, \ldots, \sum_i \Pi(\gamma)_{mi} f_i].$$

Since we assume that π is irreducible, the f_i are linearly independent and we may recover the matrices $\Pi(\gamma)$ from $[f_1, \ldots, f_m]$. We write computer algebra routines that

- Given $[f_1, \ldots, f_m]$ compute the matrices $\Pi(S)$ and $\Pi(T)$.
- Given matrices $\Pi(S)$ and $\Pi(T)$ compute a basis for $M_{\pi,d}$, writing each basis element in the form $[f_1, \ldots, f_m]$.

We specify a preferred choice of basis for Z_π by listing a single discrete covariant for each irreducible representation π. The matrices $\Pi(S)$ and $\Pi(T)$ may then be recovered using the first of the above routines. The notation we use to label the discrete covariants will be explained later.

ψ_1	$[1]$
ψ_2	$\partial \otimes E = [5a^2b^4, -a(a^5+2b^5), b(2a^5-b^5), -5a^4b^2]$
ψ_3	$U^4 = [a^4, 4a^3b, 6a^2b^2, 4ab^3, b^4]$
ψ_4	$U^2 = [a^2, 2ab, b^2]$
ψ_5	$\partial_E^2 c_4 \propto [(3a^5+b^5)b, -10a^3b^3, a(a^5-3b^5)]$
χ_1	$U = [a, b]$
χ_2	$E = [a^2(a^5+7b^5), (7a^5-b^5)b^2]$
χ_3	$U^3 = [a^3, 3a^2b, 3ab^2, b^3]$
χ_4	$U^5 = [a^5, 5a^4b, 10a^3b^2, 10a^2b^3, 5ab^4, b^5]$

The above routines allow us to compute the vector spaces $M_{\pi,d}$ one at a time. Indeed this is sufficient for many applications. However we shall go further and give generators for each M_π as an R-module.

Proposition 7.1 *Let $R = k[D, c_4, c_6]$ and let M be a finitely generated torsion free graded R-module. The following are equivalent.*
(i) M is Cohen-Macaulay as an R-module, i.e. $\operatorname{depth}(R_+, M) = 2$.
(ii) M is a free $k[D, c_4]$-module.
(iii) M is a free $k[D, c_6]$-module.
(iv) M is a free $k[c_4, c_6]$-module.

Proof. This is a special case of [4, Theorem 4.3.5]. □

Our next result is an application of [4, Theorem 4.3.6] originally due to Hochster and Eagon.

Proposition 7.2 *Let $\pi : \Gamma \to \mathrm{GL}(Z_\pi)$ with $m = \dim(Z_\pi)$. Then*
(i) M_π is a free $k[D, c_4]$-module of rank $2m$.
(ii) M_π is a free $k[D, c_6]$-module of rank $3m$.
(iii) M_π is a free $k[c_4, c_6]$-module of rank $5m$.
Furthermore, if $M_\pi(r) \subset M_\pi$ is the direct sum of the graded pieces $M_{\pi,d}$ with $d \equiv r \pmod 5$, then $M_\pi(r)$ is a free $k[c_4, c_6]$-module of rank m.

Proof. The polynomial ring $k[A]$ is Cohen-Macaulay as an R-module, say on account of the regular sequence c_4, c_6. By Proposition 7.1, $k[A]$ is a free

$k[c_4, c_6]$-module and the same goes for $k[A] \otimes Z_\pi$. The projection map

$$\tfrac{1}{|\Gamma|} \textstyle\sum_{\gamma \in \Gamma} \gamma : \quad k[A] \otimes Z_\pi \longrightarrow M_\pi$$

shows that M_π is a projective $k[c_4, c_6]$-module. By [4, Theorem 4.1.1] it is therefore a free $k[c_4, c_6]$-module. The equivalent conditions of Proposition 7.1 are satisfied. So it only remains to compute the ranks. Let $K = k(A)^\Gamma$ be the field of fractions of R. By the normal basis theorem the $K[\Gamma]$-module $k(A)$ is a copy of the regular representation. Thus

$$K \otimes Z_\pi \simeq (k(A) \otimes Z_\pi)^\Gamma = K \otimes M_\pi.$$

In particular $m = \dim_K(K \otimes M_\pi)$. Statements (i)-(iii) now follow from

$$\begin{aligned} [K : k(D, c_4)] &= 2 \\ [K : k(D, c_6)] &= 3 \\ [K : k(c_4, c_6)] &= 5. \end{aligned}$$

For the final statement we observe that $M_\pi(r)$ is free of rank m_r with $5m = \sum_{r=0}^4 m_r$. But multiplication by D shows that $m_r \leq m_{r+2}$ for all r. So $m_0 = \ldots = m_4 = m$ as required. □

We use Molien's theorem [4, Theorem 2.5.2] to compute the Poincaré series of M_π

$$p(M_\pi, t) := \sum_{d=0}^{\infty} (\dim_k M_{\pi,d}) t^d = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \frac{\operatorname{Tr} \pi(\gamma)}{1 - \operatorname{Tr} \chi(\gamma) t + t^2}. \tag{30}$$

For example taking $\pi = \chi$ we find

$$\begin{aligned} p(M_\chi, t) &= \frac{t + t^{11} + t^{19} + t^{29}}{(1 - t^{12})(1 - t^{20})} \\ &= \frac{t + t^{11} + t^{19} + t^{21} + t^{29} + t^{39}}{(1 - t^{12})(1 - t^{30})} \\ &= \frac{(t + t^{11}) + (t^{13} + t^{23}) + (t^{25} + t^{35}) + (t^{37} + t^{47}) + (t^{19} + t^{29})}{(1 - t^{20})(1 - t^{30})}. \end{aligned}$$

A basis for M_χ as a $k[D, c_4]$-module is

$$\begin{aligned} U &= [a, b] & \partial c_4 &= [\partial c_4/\partial b, -\partial c_4/\partial a] \\ \partial D &= [\partial D/\partial b, -\partial D/\partial a] & \partial c_6 &= [\partial c_6/\partial b, -\partial c_6/\partial a]. \end{aligned} \tag{31}$$

To give a basis for M_χ as a $k[D,c_6]$-module we need two further generators, namely c_4U and $c_4\partial c_4$. Finally the $k[c_4,c_6]$-modules $M_\chi(r)$ have bases

$$\begin{array}{ll} D^sU,\ D^s\partial D & \text{for } r=2s+1,\ s=0,1,2,3 \\ \partial c_4,\ \partial c_6 & \text{for } r=4. \end{array}$$

In order to construct new covariants from old, we adopt the notation

$$\begin{aligned} [f_1,\dots,f_m]\otimes[g_1,\dots,g_n] &= [f_1g_1,\dots,f_mg_1,f_1g_2,\dots,f_mg_n] \\ [f_1,\dots,f_m][g_1,\dots,g_n] &= [f_1g_1,f_1g_2+f_2g_1,\dots,f_mg_n] \\ \partial_{[f_1(a,b),\dots,f_m(a,b)]} &= [f_1(\tfrac{\partial}{\partial b},-\tfrac{\partial}{\partial a}),\dots,f_m(\tfrac{\partial}{\partial b},-\tfrac{\partial}{\partial a})]. \end{aligned} \tag{32}$$

We have already used the operator $\partial := \partial_U$ in the above example. To get started in the case $\pi=\chi_2$ we put

$$\begin{aligned} E &= [a^2(a^5+7b^5),b^2(7a^5-b^5)] \\ F &= [-b^3(26a^{10}+39a^5b^5-b^{10}),a^3(a^{10}+39a^5b^5-26b^{10})]. \end{aligned}$$

The degrees of the generators for M_π as a $k[D,c_4]$-module may be read off from the polynomial $p(M_\pi,t)(1-t^{12})(1-t^{20})$. We tabulate these polynomials, giving in each case a list of generators. We write our discrete covariants relative to the preferred basis for Z_π specified above.

$$\psi_1 \quad \begin{cases} 1+t^{30} \\ 1,c_6 \end{cases}$$

$$\psi_2 \quad \begin{cases} t^6+t^8+t^{12}+t^{14}+t^{16}+t^{18}+t^{22}+t^{24} \\ \partial\otimes E, U\otimes E, \partial\otimes F, U\otimes F, \\ \qquad \partial\otimes\partial_F c_6, U\otimes\partial_F c_6, \partial\otimes\partial_E c_6, U\otimes\partial_E c_6 \end{cases}$$

$$\psi_3 \quad \begin{cases} t^4+t^8+t^{10}+t^{12}+t^{14}+t^{16}+t^{18}+t^{20}+t^{22}+t^{26} \\ U^4,\partial^4 D, U\partial^3 D,\dots,U^3\partial D,\partial^4 c_4, U\partial^3 c_4,\dots,U^3\partial c_4,\partial^4 c_6 \end{cases}$$

$$\psi_4 \quad \begin{cases} t^2+t^{10}+t^{12}+t^{18}+t^{20}+t^{28} \\ U^2,\partial^2 D, U\partial D,\partial^2 c_4, U\partial c_4,\partial^2 c_6 \end{cases}$$

$$\psi_5 \quad \begin{cases} t^6+t^{10}+t^{14}+t^{16}+t^{20}+t^{24} \\ \partial_E^2 c_4,\partial_E\partial_F c_6, E^2,\partial_E^2 c_6, EF, E\partial_F c_6 \end{cases}$$

$$\chi_1 \quad \begin{cases} t + t^{11} + t^{19} + t^{29} \\ U, \partial D, \partial c_4, \partial c_6 \end{cases}$$

$$\chi_2 \quad \begin{cases} t^7 + t^{13} + t^{17} + t^{23} \\ E, F, \partial_F c_6, \partial_E c_6 \end{cases}$$

$$\chi_3 \quad \begin{cases} t^3 + t^9 + t^{11} + t^{13} + t^{17} + t^{19} + t^{21} + t^{27} \\ U^3, \partial^3 D, U\partial^2 D, U^2 \partial D, \partial^3 c_4, U\partial^2 c_4, U^2 \partial c_4, \partial^3 c_6 \end{cases}$$

$$\chi_4 \quad \begin{cases} t^5 + t^7 + t^9 + t^{11} + t^{13} + 2t^{15} + t^{17} + t^{19} + t^{21} + t^{23} + t^{25} \\ U^5, \partial^5 D, U\partial^4 D, \ldots, U^4 \partial D, \partial^5 c_4, U\partial^4 c_4, \ldots, U^4 \partial c_4, \partial^5 c_6 \end{cases}$$

Since our notation (32) tends to introduce large constants, we acknowledge that this table has been constructed under the assumption $\operatorname{char} k = 0$.

8 Computing the covariants

Let $\rho : \mathrm{GL}(V) \times \mathrm{GL}(W) \to \mathrm{GL}(Y)$ be a representation. Our method for computing the covariants $F : \wedge^2 V \otimes W \to Y$ is as follows. First we compute Y^{H_5} as a Γ-module. Then we use the work of §7 to give explicit expressions for the discrete covariants $f : A \to Y^{H_5}$. Finally we use Corollary 5.6 to decide which of these are covariants.

Before giving some examples, we recall from [15, Chap I, §2] the character table for the Heisenberg group H_p where p is an odd prime. There are p^2 1-dimensional characters indexed by $(u, v) \in (\mathbf{Z}/p\mathbf{Z})^2$ and $p-1$ conjugates of the Schrödinger representation indexed by $t \in (\mathbf{Z}/p\mathbf{Z})^*$.

$$\begin{array}{c|cc} & \zeta^i & \sigma^j \tau^k \\ \hline \lambda_{u,v} & 1 & \zeta_p^{ju+kv} \\ \theta_t & p\zeta_p^{it} & 0 \end{array} \tag{33}$$

Thus θ_t has dual θ_{-t}. We read off some further rules

Lemma 8.1 *Let $s, t \in (\mathbf{Z}/p\mathbf{Z})^*$. Then*

(i) $\theta_s \otimes \theta_t \simeq \begin{cases} p\theta_{s+t} & \text{if } s+t \not\equiv 0 \pmod p \\ \bigoplus_{u,v} \lambda_{u,v} & \text{if } s+t \equiv 0 \pmod p \end{cases}$

(ii) $\wedge^d \theta_t \simeq \begin{cases} \lambda_{0,0} & \text{if } d = 0 \text{ or } d = p \\ \frac{1}{p}\binom{p}{d}\theta_{dt} & \text{if } 1 \leq d \leq p-1 \end{cases}$

(iii) $S^d \theta_t \simeq \begin{cases} \frac{1}{p}\binom{p+d-1}{d}\theta_{dt} & \text{if } d \not\equiv 0 \pmod p \\ \lambda_{0,0} \oplus \frac{1}{p^2}\left(\binom{p+d-1}{d} - 1\right) \bigoplus_{u,v} \lambda_{u,v} & \text{if } d \equiv 0 \pmod p. \end{cases}$

We return to the case $p = 5$. By (22) the characters for V and W are θ_2 and θ_1 respectively. Lemma 8.1 gives a quick way of computing $\dim Y^{H_5}$. For example $Y = \wedge^2 V \otimes W$ has character

$$\wedge^2\theta_2 \otimes \theta_1 \quad \simeq \quad 2\theta_4 \otimes \theta_1 \quad \simeq \quad 2\textstyle\sum_{u,v} \lambda_{u,v}.$$

So $\dim Y^{H_5} = 2$. By inspection Y^{H_5} has basis $\sum(v_1 \wedge v_4)x_0$, $\sum(v_2 \wedge v_3)x_0$. Since

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \quad v_i \mapsto \zeta_5^{i^2} v_i\,; \quad x_i \mapsto \zeta_5^{3i^2} x_i$$

acts on Y^{H_5} with trace $\zeta_5^2 + \zeta_5^3$, reference to the character table for Γ (see Appendix A) shows that $Y^{H_5} \simeq \chi_1$ as a Γ-module. So the discrete covariants form a copy of M_χ. According to (5) a discrete covariant has integer weights if and only if it has degree $d \equiv 1 \pmod 5$. We recall from §7 that $M_\chi(1)$ is a free $k[c_4, c_6]$-module with generators U and ∂D. We arrive at integer weight discrete covariants

$$\begin{array}{rcl} U & = & a\sum(v_1 \wedge v_4)x_0 + b\sum(v_2 \wedge v_3)x_0 \\ H & = & (\partial D/\partial b)\sum(v_1 \wedge v_4)x_0 - (\partial D/\partial a)\sum(v_2 \wedge v_3)x_0. \end{array}$$

We use Corollary 5.6(ii) to check that U and H are covariants. The substitutions envisaged by Proposition 3.7 are $a^5 \mapsto \prod \lambda_i$, $b \mapsto 1$ and

$$\begin{array}{rcl} a\sum(v_1 \wedge v_4)x_0 & \mapsto & \sum \lambda_0(v_1 \wedge v_4)x_0 \\ \sum(v_2 \wedge v_3)x_0 & \mapsto & \sum(v_2 \wedge v_3)x_0. \end{array}$$

Since no denominators are introduced, U and H are covariants and indeed a basis for the $k[c_4, c_6]$-module of covariants for $Y = \wedge^2 V \otimes W$.

We recognise U as the identity map, corresponding to our original choice of elliptic normal quintic. The covariant H describes a second curve, invariant under the same representation of the Heisenberg group. By analogy with the case of plane cubics we call H the Hessian, and note that the linear span of U and H in $\mathbf{P}(\wedge^2 V \otimes W)$ is a twist of the modular curve $X(5)$.

We give another example, this time with $Y = S^2 V \otimes W$. It is immediate from Lemma 8.1 that $\dim Y^{H_5} = 3$. The action of T on the basis

$$\textstyle\sum v_0^2 x_0, \quad \sum v_1 v_4 x_0, \quad \sum v_2 v_3 x_0$$

shows that $Y^{H_5} \simeq \psi_5$ as a Γ-module. We recall from §7 that $M_{\psi_5}(1)$ is a free $k[c_4, c_6]$-module with generators $\partial_E^2 c_4$, $\partial_E^2 c_6$ and DE^2. We obtain integer weight discrete covariants

$$\begin{aligned}
Q_6 &= \textstyle\sum x_0(5a^3b^3v_0^2 + a(a^5 - 3b^5)v_1v_4 - b(3a^5 + b^5)v_2v_3) \\
Q_{16} &= \textstyle\sum x_0\big(25a^3b^3(a^{10} + b^{10})v_0^2 - a(a^{15} - 39a^{10}b^5 - 143a^5b^{10} + 3b^{15})v_1v_4 \\
&\qquad - b(3a^{15} + 143a^{10}b^5 - 39a^5b^{10} - b^{15})v_2v_3\big) \\
Q_{26} &= D\textstyle\sum x_0\big(a^2b^2(a^5 + 7b^5)(7a^5 - b^5)v_0^2 \\
&\qquad - b^4(7a^5 - b^5)^2v_1v_4 + a^4(a^5 + 7b^5)^2v_2v_3\big)
\end{aligned}$$

Again we use Corollary 5.6(ii) to check that these are covariants. This time the substitutions envisaged by Proposition 3.7 are $a^5 \mapsto \prod \lambda_i$, $b \mapsto 1$ and

$$\begin{array}{rcl}
a^3 \sum v_0^2 x_0 & \mapsto & \sum \lambda_0\lambda_1\lambda_4 v_0^2 x_0 \\
a \sum v_1v_4x_0 & \mapsto & \sum \lambda_0 v_1v_4x_0 \\
\sum v_2v_3x_0 & \mapsto & \sum v_2v_3x_0.
\end{array}$$

Since no denominators are introduced, Q_6, Q_{16} and Q_{26} are covariants and indeed a basis for the $k[c_4, c_6]$-module of covariants for $Y = S^2V \otimes W$.

We tabulate the results of these and similar calculations. In each case we give the character of Y^{H_5} as a Γ-module and the degrees of the generators for the $k[c_4, c_6]$-module of covariants for Y.

Y	Y^{H_5}	degrees
$\wedge^2 V \otimes W$	χ_1	$1, 11$
$V \otimes \wedge^2 W^*$	χ_2	$13, 23$
$\wedge^2 V^* \otimes W^*$	χ_1	$19, 29$
$V^* \otimes \wedge^2 W$	χ_2	$7, 17$
$V^* \otimes S^2 W$	ψ_4	$2, 12, 22$
$S^2 V \otimes W$	ψ_5	$6, 16, 26$
$V \otimes S^2 W^*$	ψ_4	$18, 28, 38$
$S^2 V^* \otimes W^*$	ψ_5	$14, 24, 34$

It would be interesting to find geometric interpretations for as many of these covariants as possible.

9 Computing the invariants

Let $C(\phi) \subset \mathbf{P}^4$ be an elliptic normal quintic. We give a practical algorithm for computing the invariants $c_4(\phi)$ and $c_6(\phi)$. We start with the covariants

$$\begin{array}{rcl} U : \wedge^2 V \otimes W & \to & \wedge^2 V \otimes W \\ u(a,b) & \mapsto & a \sum (v_1 \wedge v_4) x_0 + b \sum (v_2 \wedge v_3) x_0 \\ P : \wedge^2 V \otimes W & \to & V^* \otimes S^2 W \\ u(a,b) & \mapsto & \sum v_0^* (ab x_0^2 + b^2 x_1 x_4 - a^2 x_2 x_3) \end{array}$$

and write $p_i = \langle P(\phi), v_i \rangle$ for the quadrics defining $C(\phi)$. Then

$$S : \wedge^2 V \otimes W \to S^5 W; \quad \phi \mapsto \det(\partial p_i / \partial x_j)/2$$

is a covariant of degree 10. According to [15, VIII.2.5], [11, §12], $S(\phi)$ is an equation for the secant variety of $C(\phi)$. In the case $\phi = u(a,b)$ we find

$$p_i = ab x_i^2 + b^2 x_{i+1} x_{i+4} - a^2 x_{i+2} x_{i+3} \tag{34}$$

and

$$\begin{array}{rcl} S & = & a^5 b^5 \sum x_0^5 - a^4 b (a^5 - 3b^5) \sum x_0^3 x_1 x_4 + a^3 b^2 (a^5 + 2b^5) \sum x_0 x_1^2 x_4^2 \\ & & + a^2 b^3 (2a^5 - b^5) \sum x_0 x_2^2 x_3^2 - ab^4 (3a^5 + b^5) \sum x_0^3 x_2 x_3 \\ & & + (a^{10} - 16 a^5 b^5 - b^{10}) \prod x_0. \end{array}$$

A calculation reveals that the partial derivatives of S may be written as quadrics in the p_i. Explicitly

$$\partial S / \partial x_i = 5a^3 b^3 p_i^2 + a(a^5 - 3b^5) p_{i+1} p_{i+4} - b(3a^5 + b^5) p_{i+2} p_{i+3}. \tag{35}$$

We were led to this otherwise rather improbable looking identity by considering the covariant $Q = Q_6$ found in §8. The following lemma shows that it is practical to compute Q for general ϕ.

Lemma 9.1 *Let $C(\phi)$ be an elliptic normal quintic defined by quadrics $p_i = \langle P(\phi), v_i \rangle$. Then the quartics $p_i p_j$ for $i \leq j$ are linearly independent.*

Proof. It suffices to treat the case $\phi = u(a,b)$ with $ab \neq 0$. Then the p_i are given by (34). We suppose that there is a linear dependence relation

$$\textstyle\sum_{i \leq j} \lambda_{ij} p_i p_j = 0. \tag{36}$$

The coefficient of x_i^4 gives $\lambda_{ii} = 0$. Then the coefficient of $x_i^2 x_j^2$ gives $\lambda_{ij} = 0$ for all $i < j$. So (36) is the trivial relation and we are done. $\square$

We arrive at covariants

	Y	degree	weights
U	$\wedge^2 V \otimes W$	1	$(0,0)$
P	$V^* \otimes S^2 W$	2	$(1,0)$
Q	$S^2 V \otimes W$	6	$(2,1)$
M	$S^5 V^*$	10	$(5,2)$
N	$S^5 V$	5	$(1,1)$
N'	$S^5 V$	30	$(11,6)$

where M, N and N' are the following determinants

$$\begin{array}{rcll} V^* \otimes S^2 W & \subset & V^* \otimes \mathrm{Hom}(W^*, W) & \quad M = \det(P) \\ \wedge^2 V \otimes W & \subset & V \otimes \mathrm{Hom}(V^*, W) & \quad N = \det(U) \\ S^2 V \otimes W & \subset & V \otimes \mathrm{Hom}(V^*, W) & \quad N' = \det(Q). \end{array}$$

Now $\langle M, N \rangle$ and $\langle M, N' \rangle$ are invariants of degrees 15 and 40 respectively. By Proposition 6.1 we must have $\langle M, N \rangle = 0$. It even turns out that $N = 0$. However computing a single example shows that $\langle M, N' \rangle$ is non-zero, and so proportional to c_4^2. To compute both c_4 and c_6 we need one further idea. Let

$$N_t := \det(U + tQ)$$

where t is an indeterminate. Computing in the case $\phi = u(a,b)$ we find

$$\langle M, N_t \rangle = 20 c_4 t - 40 c_6 t^3 + 4 c_4^2 t^5.$$

We extract the invariants c_4 and c_6 as coefficients of this polynomial. Subject to completing the proof of Theorem 1, we now have a practical algorithm for computing the Jacobian of an elliptic normal quintic.

Remark 9.2 Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic. It is stated in [1, Example 22.6] (without proof or adequate reference) that C is the singular locus of its secant variety. The identity (35) together with [15, IV.5.6] makes it possible to give a computational proof of this result. We omit the details.

10 The invariant differential

Let $C = C(\phi)$ be an elliptic normal quintic. The aim of this section is to describe the invariant differential ω on C in terms of a covariant.

We begin by computing the covariants in the case $Y = \wedge^2 W^* \otimes S^2 W$. Lemma 8.1 gives

$$\wedge^2\theta_4 \otimes S^2\theta_1 \quad \simeq \quad 2\theta_3 \otimes 3\theta_2 \quad \simeq \quad 6\textstyle\sum_{u,v}\lambda_{u,v}$$

and so $\dim Y^{H_5} = 6$. A basis for Y^{H_5} is

$$\begin{array}{ccc} \sum(x_1^* \wedge x_4^*)x_0^2, & \sum(x_1^* \wedge x_4^*)x_1x_4, & \sum(x_1^* \wedge x_4^*)x_2x_3, \\ \sum(x_2^* \wedge x_3^*)x_0^2, & \sum(x_2^* \wedge x_3^*)x_1x_4, & \sum(x_2^* \wedge x_3^*)x_2x_3. \end{array}$$

Now $-I$ and T act with trace -6 and 1 respectively. Reference to the character table for Γ shows that $Y^{H_5} \simeq \chi_4$ as a Γ-module. We recall from §7 that $M_{\chi_4}(0)$ is a free $k[c_4, c_6]$-module with generators

$$U^5,\ U^4\partial D,\ \partial^5 c_4,\ \partial^5 c_6,\ DU^4\partial D,\ D^2U^3\partial^2 D. \tag{37}$$

These are the integer weight discrete covariants. We use Corollary 5.6(ii) to decide which are covariants. The substitutions envisaged by Proposition 3.7 are $a^5 \mapsto \prod \lambda_i$, $b \mapsto 1$ and

$$\begin{array}{rcl} a\sum(x_1^* \wedge x_4^*)x_0^2 & \mapsto & \sum \lambda_0(x_1^* \wedge x_4^*)x_0^2 \\ \sum(x_1^* \wedge x_4^*)x_1x_4 & \mapsto & \sum(x_1^* \wedge x_4^*)x_1x_4 \\ a^2\sum(x_1^* \wedge x_4^*)x_2x_3 & \mapsto & \sum \lambda_2\lambda_3(x_1^* \wedge x_4^*)x_2x_3 \\ a^4\sum(x_2^* \wedge x_3^*)x_0^2 & \mapsto & \sum \lambda_0^2\lambda_1\lambda_4(x_2^* \wedge x_3^*)x_0^2 \\ a^3\sum(x_2^* \wedge x_3^*)x_1x_4 & \mapsto & \sum \lambda_0\lambda_1\lambda_4(x_2^* \wedge x_3^*)x_1x_4 \\ \sum(x_2^* \wedge x_3^*)x_2x_3 & \mapsto & \sum(x_2^* \wedge x_3^*)x_2x_3. \end{array}$$

Invariance under T ensures that each discrete covariant has coefficient of $\sum(x_2^* \wedge x_3^*)x_0^2$ divisible by a^4. Arguing similarly for the other coefficients we see that no denominators are introduced. So for this choice of Y every integer weight discrete covariant is a covariant.

As in §9 we write $p_i = \langle P(\phi), v_i\rangle$ for the quadrics defining $C(\phi)$. Taking $\phi = u(a,b)$, the Jacobian matrix $(\partial p_i/\partial x_j)$ is

$$J(\phi) = \begin{pmatrix} 2abx_0 & b^2x_4 & -a^2x_3 & -a^2x_2 & b^2x_1 \\ b^2x_2 & 2abx_1 & b^2x_0 & -a^2x_4 & -a^2x_3 \\ -a^2x_4 & b^2x_3 & 2abx_2 & b^2x_1 & -a^2x_0 \\ -a^2x_1 & -a^2x_0 & b^2x_4 & 2abx_3 & b^2x_2 \\ b^2x_3 & -a^2x_2 & -a^2x_1 & b^2x_0 & 2abx_4 \end{pmatrix}$$

and the first of the covariants (37) works out as

$$\Omega(\phi) = \begin{pmatrix} 0 & \alpha_3 & \beta_1 & -\beta_4 & -\alpha_2 \\ -\alpha_3 & 0 & \alpha_4 & \beta_2 & -\beta_0 \\ -\beta_1 & -\alpha_4 & 0 & \alpha_0 & \beta_3 \\ \beta_4 & -\beta_2 & -\alpha_0 & 0 & \alpha_1 \\ \alpha_2 & \beta_0 & -\beta_3 & -\alpha_1 & 0 \end{pmatrix} \tag{38}$$

where

$$\begin{aligned} \alpha_i &= 5a^4bx_i^2 - 10a^3b^2x_{i-1}x_{i+1} + (a^5 - 3b^5)x_{i-2}x_{i+2} \\ \beta_i &= 5ab^4x_i^2 - (3a^5 + b^5)x_{i-1}x_{i+1} + 10a^2b^3x_{i-2}x_{i+2}. \end{aligned} \tag{39}$$

Lemma 10.1 *Let $C = C(\phi)$ be an elliptic normal quintic. Let $J = J(\phi)$ and $\Omega = \Omega(\phi)$ be the matrices defined above. Then*
(i) The matrix product $J\Omega$ vanishes in the function field $k(C)$.
(ii) The skew-symmetric matrix Ω has rank 2 at all points on C.

Proof. As usual it suffices to treat the case $\phi = u(a, b)$.
(i) This may be checked by direct calculation, preferably using Gröbner bases.
(ii) Since $C \subset \mathbf{P}^4$ is a smooth curve of codimension 3, the Jacobian matrix J has rank 3 on C. It follows by (i) that Ω has rank at most 2 on C. Alternatively we could observe that the 4×4 Pfaffians of Ω are the quartics $\partial S/\partial x_i$ and that by (35) these quartics vanish on C. It remains to show that Ω is non-zero on C. By (34) and (39) it suffices to show that

$$\det \begin{pmatrix} ab & b^2 & -a^2 \\ 5a^4b & -10a^3b^2 & a^5 - 3b^5 \\ 5ab^4 & -3a^5 - b^5 & 10a^2b^3 \end{pmatrix} = 18D(a, b) \tag{40}$$

is non-zero. But our assumption that $\phi = u(a, b)$ is an elliptic normal quintic gives $D(a, b) \neq 0$ as required. $\square$

Writing $\Omega = (\Omega_{ij})$, it follows that the invariant differential on C is

$$\omega = \frac{x_j^2 d(x_i/x_j)}{\Omega_{ij}} \qquad \text{for all } i \neq j. \tag{41}$$

According to (5) the covariant Ω has weights $(p, q) = (2, 1)$. This observation has some important consequences (see Remark 12.3).

We outline a method for computing the covariant Ω. Let $R = k[W^*] = k[x_0, \ldots, x_4]$. Let $I(\phi) \lhd R$ be the ideal generated by the quadrics $p_i = \langle P(\phi), v_i \rangle$ and let $I'(\phi) \lhd R$ be the ideal generated by the quartics $\partial S/\partial x_i$. We saw in Remark 9.2 that an elliptic normal quintic is the singular locus of its secant variety. Thus $I(\phi)$ is the radical of $I'(\phi)$ and both ideals have codimension 3.

Lemma 10.2 *Let $C(\phi) \subset \mathbf{P}^4$ be an elliptic normal quintic. Then the ideal $I'(\phi) \lhd R$ is Gorenstein of codimension 3.*

Proof. As usual it suffices to treat the case $\phi = u(a,b)$. As observed in the proof of Lemma 10.1, the quartics $\partial S/\partial x_i$ are the 4×4 Pfaffians of Ω. We obtain a complex of graded free R-modules

$$0 \longrightarrow R \xrightarrow{\partial S/\partial x_i} W^* \otimes R \xrightarrow{\Omega} W \otimes R \xrightarrow{\partial S/\partial x_i} R \longrightarrow 0. \qquad (42)$$

Since $I'(\phi)$ has codimension 3 it follows by the Buchsbaum-Eisenbud structure theorem [5], [11, §10] that (42) is a minimal free resolution for $R/I'(\phi)$ and that $I'(\phi)$ is Gorenstein. $\Box$

It follows that we may compute the covariant Ω from the minimal resolution for $R/I'(\phi)$. This gives a practical method for computing the discriminant Δ, analogous to Salmon's result for plane cubics cited in the introduction. Indeed the original 5 quadrics p_i together with the 10 quadrics ω_{ij} for $i < j$ give a total of 15 elements of S^2W. Since $\dim S^2W = 15$ we may form a 15×15 determinant. We claim that this determinant is a non-zero multiple of the discriminant. As usual it suffices to check in the case $\phi = u(a,b)$. But in that case the 15×15 matrix may be put in block diagonal form, with each 3×3 block a copy of (40). Our claim follows since $\Delta = D^5$. It should be pointed out that the work of §9 makes this algorithm obsolete.

Remark 10.3 In view of the relation $J\Omega = 0$ in $k(C)$ there is a much more direct way of computing $\Omega = (\omega_{ij})$. But working in the function field means that we would only determine the ω_{ij} up to addition of linear combinations of the quadrics p_i. It is interesting to note that the above algorithm for computing the discriminant is not affected by such changes.

11 The quintic covariants

In the cases $n = 2, 3, 4$ we recall [2] that classical invariant theory provides us with equations for the covering map of degree n^2 from a curve of genus one to its Jacobian. We would like to generalise this to the case $n = 5$. As a first step we compute the covariants in the case $Y = S^5 W$. Lemma 8.1 gives

$$S^5\theta_1 \quad \simeq \quad \lambda_{0,0} \oplus 5 \textstyle\sum_{u,v} \lambda_{u,v}$$

and so $\dim Y^{H_5} = 6$. A basis for Y^{H_5} is

$$\textstyle\sum x_0^5, \quad \sum x_0^3 x_1 x_4, \quad \sum x_0^3 x_2 x_3 \quad \sum x_0 x_1^2 x_4^2, \quad \sum x_0 x_2^2 x_3^2, \quad \prod x_0.$$

Since

$$R = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} : x_i \mapsto -x_{2i} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : x_i \mapsto \zeta_5^{3i^2} x_i$$

act on Y^{H_5} with trace -2 and 1, reference to the character table for Γ shows that $Y^{H_5} \simeq \psi_4 \oplus \psi_5$ as a Γ-module. So the integer weight discrete covariants form a copy of $M_{\psi_4}(0) \oplus M_{\psi_5}(0)$. Each summand is a free $k[c_4, c_6]$-module with generators in degrees 10, 20 and 30. In the notation of §7 they are labelled $\partial^2 D$, $U\partial c_4$, $D\partial^2 c_4$ and $\partial_E \partial_F c_6$, EF, $D^2 \partial_E^2 c_4$. We put

$$\begin{aligned} \mathcal{F} &= [\textstyle\sum x_0^5 - 30 \prod x_0, 10 \sum x_0^3 x_1 x_4, 10 \sum x_0^3 x_2 x_3] \\ \mathcal{G} &= [\textstyle\sum x_0^5 + 20 \prod x_0, 10 \sum x_0 x_1^2 x_4^2, 10 \sum x_0 x_2^2 x_3^2] \end{aligned}$$

and so obtain integer weight discrete covariants

$$\begin{aligned} F_{10} &= [a^{10} - 36a^5b^5 - b^{10}, 5a^4b(a^5 - 3b^5), 5ab^4(3a^5 + b^5)].\mathcal{F} \\ F_{20} &= [a^{20} + 114a^{15}b^5 + 114a^5b^{15} - b^{20}, \\ &\qquad -a^4b(a^{15} + 171a^{10}b^5 + 247a^5b^{10} - 57b^{15}), \\ &\qquad\quad -ab^4(57a^{15} + 247a^{10}b^5 - 171a^5b^{10} + b^{15})].\mathcal{F} \\ F_{30} &= D[10a^4b^4(9a^{10} + 26a^5b^5 - 9b^{10}), \\ &\qquad a^3(a^{15} + 126a^{10}b^5 + 117a^5b^{10} - 12b^{15}), \\ &\qquad\quad -b^3(12a^{15} + 117a^{10}b^5 - 126a^5b^{10} + b^{15})].\mathcal{F} \\ G_{10} &= [a^{10} + 14a^5b^5 - b^{10}, 5a^3b^2(a^5 + 2b^5), 5a^2b^3(2a^5 - b^5)].\mathcal{G} \\ G_{20} &= [a^{20} - 136a^{15}b^5 - 136a^5b^{15} - b^{20}, \\ &\qquad -a^3b^2(7a^{15} + 272a^{10}b^5 - 221a^5b^{10} + 26b^{15}), \\ &\qquad\quad -a^2b^3(26a^{15} + 221a^{10}b^5 + 272a^5b^{10} - 7b^{15})].\mathcal{G} \\ G_{30} &= 2D^2[10a^3b^3, a(a^5 - 3b^5), -b(3a^5 + b^5)].\mathcal{G}. \end{aligned}$$

We use Corollary 5.6(ii) to decide which of these are covariants. The substitutions envisaged by Proposition 3.7 are $a^5 \mapsto \prod \lambda_i$, $b \mapsto 1$ and

$$\begin{array}{rcl} a^5 \sum x_0^5 & \mapsto & \sum \lambda_0^3 \lambda_1 \lambda_4 x_0^5 \\ a^4 \sum x_0^3 x_1 x_4 & \mapsto & \sum \lambda_0^2 \lambda_1 \lambda_4 x_0^3 x_1 x_4 \\ a^3 \sum x_0 x_1^2 x_4^2 & \mapsto & \sum \lambda_0 \lambda_1 \lambda_4 x_0 x_1^2 x_4^2 \\ a^2 \sum x_0 x_2^2 x_3^2 & \mapsto & \sum \lambda_2 \lambda_3 x_0 x_2^2 x_3^2 \\ a \sum x_0^3 x_2 x_3 & \mapsto & \sum \lambda_0 x_0^3 x_2 x_3 \\ \prod x_0 & \mapsto & \prod x_0 \end{array}$$

Thus the condition for an integer weight discrete covariant to be a covariant is that the coefficient of $\sum x_0^5$ be divisible by a^5. In particular F_{10}, F_{20}, G_{10} and G_{20} are *not* covariants. We put

$$\begin{array}{rclcrcl} F_{40} & := & c_6 F_{10} + c_4 F_{20} & \qquad & G_{40} & := & c_6 G_{10} + c_4 G_{20} \\ F_{50} & := & c_4^2 F_{10} + c_6 F_{20} & & G_{50} & := & c_4^2 G_{10} + c_6 G_{20}. \end{array} \tag{43}$$

Then the quintic covariants form a free $k[c_4, c_6]$-module with basis

$$F_{10} - G_{10}, \quad F_{20} - G_{20}, \quad F_{30}, \quad G_{30}, \quad F_{40}, \quad F_{50}. \tag{44}$$

In particular the secant variety $S \propto F_{10} - G_{10}$ is the only quintic covariant of degree 10. A calculation in the case $\phi = u(a, b)$ confirms that the quintics (44) remain linearly independent when we specialise to ϕ an elliptic normal quintic. The quintic hypersurfaces through a fixed elliptic normal quintic have previously been studied by Hulek [15]. We give some examples to illustrate how our work with covariants picks out the quintic hypersurfaces to which Hulek was able to attach a geometric meaning.

Lemma 11.1 *Let $C(\phi) \subset \mathbf{P}^4$ be an elliptic normal quintic. Then*
(i) The Heisenberg invariant quintics vanishing on C have basis $F_{10} - G_{10}$, $F_{20} - G_{20}$, F_{30}, G_{30}, F_{40}.
(ii) The Heisenberg invariant quintics singular along C have basis $F_{10} - G_{10}$, $F_{20} - G_{20}$, $F_{30} - G_{30}$.

Proof. Hulek [15, VI] shows that these spaces have dimension 5 and 3 respectively. The latter has basis $\sum p_0^2 x_0$, $\sum p_1 p_4 x_0$, $\sum p_2 p_3 x_0$.
(i) We compute the covariants in the case $Y = V \otimes S^3 W$. We find $Y^{H_5} \simeq \chi_1 \oplus \psi_3$ as a Γ-module. By Molien's theorem the $k[c_4, c_6]$-module of integer weight discrete covariants is generated in degrees 13, 23 and 8, 18, 28, 28, 38. All

of these are covariants. Substituting $v_i \mapsto p_i$ we obtain quintic covariants vanishing on C. They have degrees 15, 25 and 10, 20, 30, 30, 40. Comparison with (44) shows the first two covariants must vanish. We conclude by a direct calculation in the case $\phi = u(a,b)$.
(ii) In §8 we computed the covariants for $Y = S^2V \otimes W$ and so obtained a free $k[c_4, c_6]$-module generated in degrees 6, 16 and 26. Substituting $v_i \mapsto p_i$ we obtain the quintic covariants singular along C. We conclude by a direct calculation in the case $\phi = u(a,b)$. □

Remark 11.2 The condition for a quintic covariant to vanish on C may be expressed in terms of a quintic contravariant (*i.e.* a covariant with $Y = S^5W^*$) of degree 10. The contraction of this contravariant with F_{50} is a non-zero multiple of the discriminant Δ.

Lemma 11.3 *Let $C = C(\phi)$ be an elliptic normal quintic. Let* $\operatorname{Tan} C$ *be the locus of tangent lines of C. Let F be the locus of singular lines of rank 3 quadrics containing C. Then*
(i) The quintics containing $\operatorname{Tan} C$ *have basis $F_{10} - G_{10}$, $F_{20} - G_{20}$, $F_{30} + G_{30}$.*
(ii) The quintics containing F have basis $F_{10} - G_{10}$, $F_{20} - G_{20}$, $F_{30} - G_{30}$.
(iii) $\operatorname{Tan} C \cup F$ *is the complete intersection $F_{10} - G_{10} = F_{20} - G_{20} = 0$.*

Proof. (i) We recall [15, VII] that $\operatorname{Tan} C$ is an irreducible surface of degree 10, and that the space of quintics containing $\operatorname{Tan} C$ has dimension 3. We compute a basis by working in the case $\phi = u(a,b)$. Evaluating the rows of (38) at the rational point $0 = (0 : a : b : -b : -a)$ we obtain 5 points on the tangent line to C at 0. The quintic covariants listed are the only ones to vanish at all these points.
(ii) We recall [15, IV.4.7] that F is an irreducible surface of degree 15. By [15, VIII.3.5] the quintics containing F are precisely the Heisenberg invariant quintics singular along C. We are done by Lemma 11.1(ii).
(iii) The proofs of (i) and (ii) show that $\operatorname{Tan} C \cup F$ is a surface of degree 25 contained in the complete intersection $F_{10} - G_{10} = F_{20} - G_{20} = 0$ also of degree 25. □

Remark 11.4 The character table for Γ gives $S^2\psi_4 \simeq S^2\psi_5 \simeq \psi_1 \oplus \psi_3$. But according to the table below, the trivial representation ψ_1 appears only once in the decomposition of $(S^{10}W)^{H_5}$ as a Γ-module. It follows that the quintic covariants satisfy a quadratic relation. We find

$$F_{10}F_{50} + 5F_{20}F_{40} + 3F_{30}^2 = G_{10}G_{50} + 5G_{20}G_{40} + 3G_{30}^2. \tag{45}$$

We return to the complete intersection of Lemma 11.3(iii). Substituting $F_{10} = G_{10}$ and $F_{20} = G_{20}$ in (45) and recalling our definitions (43) we find $(F_{30}+G_{30})(F_{30}-G_{30}) = 0$. These factors correspond to $\operatorname{Tan} C$ and F respectively.

As explained at the start of this section, we would like to find covariants describing the covering map from an elliptic normal quintic to its Jacobian. For this we would need a practical algorithm for computing certain covariants of order $r = 5$, 10 and 15. Unfortunately the dimension of $(S^rW)^{H_5}$ grows rapidly with r and this makes it difficult even to classify the discrete covariants. For example there are 41 covariants of order 10, all but 2 of which vanish on C.

Some hope is afforded by the work of Horrocks and Mumford [14, §2] who work directly[5] with characters of the extended Heisenberg group H_5^+. In fact they give an inductive procedure for computing (virtual) characters π_r of Γ such that

$$S^r\theta_1 \quad \simeq \quad \begin{cases} \pi_r \otimes \theta_r & \text{if } r \not\equiv 0 \pmod 5 \\ 1 \oplus \pi_r \otimes (\theta_1 \otimes \theta_1^*) & \text{if } r \equiv 0 \pmod 5. \end{cases}$$

Here we have used Corollary 4.7 to view θ_t as a character for H_5^+, and the exact sequence (23) to view characters of Γ as characters of H_5^+. For $5 \mid r$ it follows that $(S^rW)^{H_5} \simeq 1 \oplus \pi_r$ as a Γ-module. Implementing their algorithm we find

r	$\dim(S^rW)^{H_5}$	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	χ_1	χ_2	χ_3	χ_4
5	6	0	0	0	1	1	0	0	0	0
10	41	1	1	4	1	1	1	1	0	1
15	156	2	7	6	6	6	1	1	5	6
20	426	6	16	22	11	11	6	6	12	18
25	951	6	33	43	28	28	16	16	27	43
30	1856	21	68	83	48	48	27	27	59	86

This gives us partial information concerning the discrete covariants. But at present we do not know of any practical algorithm in the style of §9 giving equations for the covering map.

[5]This is in contrast with our approach of working with H_5 and Γ separately.

12 Computing the Jacobian

Let k be a field with $\operatorname{char} k \neq 2, 3, 5$. We drop our assumption that k is algebraically closed. To complete the proof of Theorem 1 we prove

Proposition 12.1 *Let $\phi \in \wedge^2 V \otimes W$ with $C(\phi) \subset \mathbf{P}^4$ an elliptic normal quintic. Then $C(\phi)$ has Jacobian*

$$y^2 = x^3 - 27c_4(\phi)x - 54c_6(\phi). \tag{46}$$

The invariants c_4 and c_6 were defined in §2. Their scalings were fixed §6. In the same section we gave a proof of Theorem 1 under the assumption that k is algebraically closed. So it remains to rule out the possibility that (46) might be a non-trivial quadratic twist[6] of the Jacobian. By analogy with the cases $n = 2, 3, 4$ the only issue here should be the appropriate scaling of the invariants.

Let E be the elliptic curve $y^2 = x^3 + Ax + B$. If we embed $E \subset \mathbf{P}^4$ via $(x_0 : x_2 : x_3 : x_4 : x_5) = (1 : x : y : x^2 : xy)$ then $E = C(\phi_{A,B})$ where

$$\phi_{A,B} = \begin{pmatrix} 0 & Bx_0 & x_5 & Ax_0 + x_4 & -x_3 \\ & 0 & -x_4 & -x_3 & x_2 \\ & & 0 & -x_2 & 0 \\ & - & & 0 & -x_0 \\ & & & & 0 \end{pmatrix}. \tag{47}$$

Running our algorithm, as described in §9, we find

$$c_4(\phi_{A,B}) = -48A \quad \text{and} \quad c_6(\phi_{A,B}) = -864B. \tag{48}$$

This proves Proposition 12.1 in the case $\phi = \phi_{A,B}$ and shows that our covariants are scaled appropriately. (See Remark 6.3 for an alternative approach.) As comparison of (46) and (48) reminds us, we are always free to rescale $(c_4, c_6) \mapsto (\lambda^4 c_4, \lambda^6 c_6)$ for any $\lambda \in k^*$.

Our proof of Proposition 12.1 relies on the following observation.

Lemma 12.2 *Let $C(\phi) \subset \mathbf{P}^4$ be an elliptic normal quintic. Then* $\operatorname{Stab}(\phi) \subset \operatorname{SL}(V) \times \operatorname{SL}(W)$ *acts on $C(\phi)$ as the 5-torsion of its Jacobian.*

[6] The reader should modify this statement as appropriate when $j = 0$, 1728

Proof. For the duration of the proof we assume that k is algebraically closed. Let $(g_V, g_W) \in \mathrm{SL}(V) \times \mathrm{GL}(W)$ with $(g_V, g_W)\phi = \phi$ and let α be the automorphism of $C(\phi)$ induced by g_W. We must show that α is a translation map if and only if $\det g_W = 1$. If α is a translation map we reduce to the case $\phi = u(a,b)$. In the notation of §5 we have $(g_V, g_W) = (\theta_V(h), \theta_W(h))$ for some $h \in H_5$. So $\det g_V = \det g_W = 1$ as required. If α is not a translation map then it has a finite number of fixed points. We reduce to the case $\phi = \phi_{A,B}$ with fixed point $0 = (0:0:0:0:1)$. The automorphism $[-1]$ is given by

$$g_V = \mathrm{Diag}(1,-1,1,-1,1) \qquad g_W = \mathrm{Diag}(-1,-1,1,-1,1).$$

If $A = 0$ or $B = 0$ there are additional automorphisms given by

$$g_V = \mathrm{Diag}(\zeta^2, \zeta, 1, \zeta^{-1}, \zeta^{-2}) \qquad g_W = \mathrm{Diag}(\zeta^3, \zeta, 1, \zeta^{-1}, \zeta^{-2})$$

with $\zeta^6 = 1$ or $\zeta^4 = 1$. In each case we find $\det g_V = 1$ and $\det g_W \neq 1$. $\square$

Remark 12.3 In §10 we gave a description of the invariant differential in terms of a covariant Ω. Since Ω has weights $(2,1)$ and the translation maps are characterised by the fact they preserve the invariant differential, this leads to an alternative proof of Lemma 12.2. In particular we avoid the need to split into cases.

It is known that the quotient of an elliptic normal quintic by the 5-torsion of its Jacobian is isomorphic to its Jacobian. So taking our universal family of elliptic normal quintics parametrised by $\wedge^2 V \otimes W \setminus \{\Delta = 0\}$ and quotienting out by the action of $\mathrm{SL}(V) \times \mathrm{SL}(W)$ we expect to obtain the universal family of Jacobians. We are therefore confident that everything in [2] generalises to the case $n = 5$, even if (as acknowledged in §11) we are yet to find the covariants that describe the covering map from $C(\phi)$ to its Jacobian.

We take a slightly different approach, still relying on Lemma 12.2. Let $\overline{k}$ be a separable closure for k. We put $\overline{V} = V \otimes_k \overline{k}$ and $\overline{W} = W \otimes_k \overline{k}$. Since $\mathrm{char}\, k \neq 2,3,5$ it turns out that all our work in the case of an algebraically closed field carries over to a separably closed field.

Lemma 12.4 *Let ϕ, $\phi' \in \wedge^2 V \otimes W$ with $C(\phi), C(\phi') \subset \mathbf{P}^4$ elliptic normal quintics. Suppose that $(g_V, g_W)\phi = \phi'$ for some $(g_V, g_W) \in \mathrm{SL}(\overline{V}) \times \mathrm{GL}(\overline{W})$. If $\det g_W \in k$ then the Jacobians of $C(\phi)$ and $C(\phi')$ are isomorphic over k.*

Proof. Since $\det g_W \in k$ the cocycle $\sigma \mapsto (\sigma(g_V)g_V^{-1}, \sigma(g_W)g_W^{-1})$ takes values in $\mathrm{SL}(\overline{V}) \times \mathrm{SL}(\overline{W})$. By Lemma 12.2 the cocycle $\sigma \mapsto \sigma(g_W)g_W^{-1}$ acts on $C(\phi')$ via translations. So g_W induces an isomorphism of Jacobians. $\square$

Proof of Proposition 12.1. Let $\phi \in \wedge^2 V \otimes W$ with $C(\phi) \subset \mathbf{P}^4$ an elliptic normal quintic. Let $A = -27c_4(\phi)$ and $B = -54c_6(\phi)$. Let $\phi' = \phi_{A,B}$ be given by (47). Proposition 6.1 tells us that $C(\phi)$ and $C(\phi')$ are isomorphic over $\overline{k}$. So by Lemma 2.5(i) there exists $(g_V, g_W) \in \mathrm{SL}(\overline{V}) \times \mathrm{GL}(\overline{W})$ with $(g_V, g_W)\phi = \phi'$. We apply c_4 and c_6 to both sides. For the left-hand side we note that c_4 and c_6 have weights $(8, 4)$ and $(12, 6)$. For the right-hand side we use (48). We obtain

$$\begin{aligned} (\det g_W)^4 c_4(\phi) &= 6^4 c_4(\phi) \\ (\det g_W)^6 c_6(\phi) &= 6^6 c_6(\phi). \end{aligned}$$

If $c_4(\phi) \neq 0$ and $c_6(\phi) \neq 0$ then $\det g_W = \pm 6$ and we may apply Lemma 12.4. In the remaining cases we compose (g_V, g_W) with one of the automorphisms of $C(\phi')$ described in the proof of Lemma 12.2. So in all cases we may suppose that $\det g_W = 6$. Lemma 12.4 tells us that the Jacobians of $C(\phi)$ and $C(\phi')$ are isomorphic. Since the latter is an elliptic curve with Weierstrass equation (46), this completes the proof of Proposition 12.1. $\square$

Finally Propositions 6.1 and 12.1 combine to prove Theorem 1.

Remark 12.5 As noted above, the invariants c_4 and c_6 have weights $(8, 4)$ and $(12, 6)$. So if we change our co-ordinates on $\mathbf{P}^4$, or change our basis for the space of quadrics defining our curve, then c_4 and c_6 change in a way that does not alter the Jacobian.

13 A practical algorithm

Let k be a field with $\mathrm{char}\, k \neq 2, 3, 5$. Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic defined by quadrics $p_1, \ldots, p_5 \in k[x_1, \ldots, x_5]$. We describe in detail our algorithm for computing the Jacobian of C and then give some examples in the case $k = \mathbf{Q}$.

The first step is to write the quadrics p_i as the 4×4 Pfaffians of a 5×5 skew-symmetric matrix. This is done by computing the syzygies between the p_i and then appealing to the work of Buchsbaum and Eisenbud, [5], [11, §10].

Algorithm 13.1 (Writing the quadrics as Pfaffians)
`INPUT:` A vector $p = (p_i)_{i=1}^5$ of quadrics.
`OUTPUT:` A skew-symmetric matrix $\phi = (\phi_{ij})_{i=1}^5$ of linear forms.
1. begin
2. choose $(\Lambda_i)_{i=1}^5$ a basis for $\{\Lambda = (\lambda_{jk})_{j,k=1}^5 : \sum_{j,k} \lambda_{jk} x_j p_k = 0\}$;
3. A = `matrix(5,5,i,k,sum(j=1,5,`$\lambda_{i,jk} x_j$`))`;
4. solve for B = $(b_{ij})_{i,j=1}^5$ such that BA + $A^T B^T$ = 0;
5. ϕ = BA;
6. check `pfaffian(`$\phi^{\{i\}}$`)` $\propto p_i$;
7. end

Remarks. (i) The matrix A is a matrix of linear forms, whereas the matrix B is a matrix of constants.
(ii) We write $\phi^{\{i\}}$ for the 4×4 matrix obtained by deleting the ith row and ith column of ϕ. See [11, §1] for a definition of the Pfaffian.
(iii) If the p_i define an elliptic normal quintic then the vector space of step 2 has dimension 5, the matrix B of step 4 is uniquely determined up to scalars, and the condition of step 6 is satisfied. If any of these conditions fail then Algorithm 13.1 should output an error message to the effect that the p_i do not define an elliptic normal quintic.
(iv) The constants of proportionality in step 6 are uniquely determined up to squares. In general we should not expect to obtain equality.

Next we make explicit the algorithm described in §9.

Algorithm 13.2 (Computing the invariants)
`INPUT:` A skew-symmetric matrix $\phi = (\phi_{ij})_{i,j=1}^5$ of linear forms.
`OUTPUT:` Invariants c_4 and c_6.
1. begin
2. p = `vector(5,i,(-1)`^{i}`*pfaffian(`$\phi^{\{i\}}$`))`;
3. S = `det(matrix(5,5,i,j,`$\partial p_i / \partial x_j$`))`;
4. q = `vector(5,i,`
5. solve for ε_{jk} such that $\partial S / \partial x_i = \sum_{j \le k} \varepsilon_{jk} p_j p_k$;
6. `sum(j=1,5,sum(k=j,5,`$\varepsilon_{jk} x_j x_k$`)))`;
7. U = `matrix(5,5,i,j,sum(k=1,5,polcoeff(`ϕ_{jk}, x_i`)*`x_k`))`;
8. P = `matrix(5,5,i,j,sum(k=1,5,polcoeff(`$\partial p_k / \partial x_j, x_i$`)*`$x_k$`))`;
9. Q = `matrix(5,5,i,j,`$\partial q_i / \partial x_j$`)`;
10. F = `sum(I,I!*polcoeff(det(`P`),`x_I`)*polcoeff(det(`$U+tQ$`),`x_I`))`;

```
11.   c_4 = polcoeff(F,t)/40;
12.   c_6 = -polcoeff(F,t^3)/320;
13.   check c_4^2 = polcoeff(F,t^5)/128;
14. end
```

Remarks. (i) For ϕ an elliptic normal quintic, Lemma 9.1 shows that the quartics $\{p_i p_j \mid i \leq j\}$ are linearly independent. If there is a dependence relation Algorithm 13.2 should output an error message to the effect that the $C(\phi)$ is not elliptic normal quintic.
(ii) We employ the multi-index notation $I = (i_1, \dots i_5)$ with $x_I = x_1^{i_1} \dots x_5^{i_5}$ and $I! = i_1! \dots i_5!$. The sum of step 10 is taken over all 126 multi-indices of degree 5.

Finally Theorem 1 tells us that the Jacobian of C is

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

Remark 13.3 We test our algorithm by applying it in cases where we already know the Jacobian. These include $\phi = u_1(\lambda_0, \dots, \lambda_4)$ given by (13) and $\phi = \phi_{A,B}$ given by (47). We may also disguise our examples by changing co-ordinates on $\mathbf{P}^4$, or changing our basis for the space of quadrics. These examples illustrate the need for a reduction algorithm. It is hoped that this will be the subject of future work.

We give some examples in the case $k = \mathbf{Q}$.

Example 13.4 In [8, Appendix B] we constructed an elliptic normal quintic violating the Hasse principle

$$\begin{aligned}
p_1 &= 11x_1^2 - x_2^2 + 5x_3^2 + x_4^2 - 5x_5^2 \\
p_2 &= x_2^2 + 10x_2x_3 + 5x_3^2 + 2x_1x_4 - x_2x_4 - 5x_3x_4 - 5x_2x_5 - 5x_3x_5 \\
p_3 &= x_2^2 + 2x_2x_3 + 5x_3^2 + x_2x_4 + x_3x_4 + 2x_1x_5 + x_2x_5 + 5x_3x_5 \\
p_4 &= 11x_1x_2 + 55x_1x_3 + 2x_2x_4 + 2x_4^2 - 10x_3x_5 + 10x_5^2 \\
p_5 &= 11x_1x_2 + 11x_1x_3 - 2x_3x_4 + 2x_2x_5 - 4x_4x_5.
\end{aligned}$$

Algorithm 13.1 writes these quadrics as the 4×4 Pfaffians of

$$\phi = \begin{pmatrix} 0 & -2x_5 & 2x_4 & -x_2 - x_3 & x_2 + 5x_3 \\ 2x_5 & 0 & -11x_1 & x_3 + x_5 & x_2 + x_4 \\ -2x_4 & 11x_1 & 0 & -x_2 + x_4 & -5x_3 + 5x_5 \\ x_2 + x_3 & -x_3 - x_5 & x_2 - x_4 & 0 & -x_1 \\ -x_2 - 5x_3 & -x_2 - x_4 & 5x_3 - 5x_5 & x_1 & 0 \end{pmatrix}.$$

Algorithm 13.2 computes the invariants

$$c_4(\phi) = 2^{12} \times 9384400 \qquad c_6(\phi) = 2^{18} \times 28748141000.$$

From these we compute a minimal Weierstrass equation for the Jacobian

$$275\text{B3} \qquad y^2 + y = x^3 + x^2 - 195508x - 33338481.$$

Conditional on the Birch Swinnerton-Dyer conjecture, Cremona's tables [6] show that this is the elliptic curve over $\mathbf{Q}$ of smallest conductor whose Tate-Shafarevich group contains an element of order 5.

Example 13.5 C. Wuthrich [27] has constructed an element of the Tate-Shafarevich group of order 5 using methods unrelated to [8], [9]. Written as an elliptic normal quintic his example is

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

Algorithms 13.1 and 13.2 compute the invariants

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

From these we compute a minimal Weierstrass equation for the Jacobian

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

It has square-free conductor $N = 1289106508910$. We are able to confirm that the Jacobian does not admit a rational 5-isogeny. So the methods of [8], [9] do not apply.

14 A special case

Let k be a field with $\operatorname{char} k \neq 5$. Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic defined over k whose Jacobian has a k-rational point of order 5. We recall an algorithm of C. O'Neil [19] for computing the Jacobian of C, and compare it with our general algorithm.

First, to give a supply of examples, we take x_0, y_0 linear forms on $\mathbf{P}^4$, defined over k, and $M \in \mathrm{GL}_5(k)$ with $M^5 = bI$ for some $b \in k^*$. We assume throughout that the image of M in PGL_5 has order 5. Let $x_i = M^i x_0$ and $y_i = M^i y_0$ for $i = 0, \dots, 4$. We define $C[M; x_0, y_0] \subset \mathbf{P}^4$ with equations the 4×4 Pfaffians of

$$\begin{pmatrix} 0 & x_3 & by_1 & y_4 & x_2 \\ & 0 & x_4 & y_2 & y_0 \\ & & 0 & bx_0 & y_3 \\ & - & & 0 & x_1 \\ & & & & 0 \end{pmatrix}. \tag{49}$$

Generically this will be an elliptic normal quintic. Explicitly writing out the Pfaffians it is clear that $C[M; x_0, y_0]$ is preserved by the action of M on $\mathbf{P}^4$. In other words M corresponds to a k-rational point of order 5 on the Jacobian. Conversely

Lemma 14.1 *Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic, defined over k, whose Jacobian has a k-rational point of order 5. Then $C = C[M; x_0, y_0]$ for some x_0, y_0 linear forms on $\mathbf{P}^4$, defined over k, and $M \in \mathrm{GL}_5(k)$.*

Proof. Proposition 1.1(i) gives $C = C(\phi)$ for some $\phi \in \wedge^2 V \otimes W$. The action of a k-rational point of order 5 corresponds to $(g_V, g_W) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$ with $(g_V, g_W)\phi = \phi$. We choose a basis for V such that

$$g_V = \begin{pmatrix} 0 & a^{-1} & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & a^{-1} & 0 \\ 0 & 0 & 0 & 0 & a^{-1} \\ -a & 0 & 0 & 0 & 0 \end{pmatrix}$$

for some $a \in k^*$. Then we take $M = g_W$ and $b = a^2$. Writing out the identity $(g_V, g_W)\phi = \phi$ it follows that ϕ takes the form (49). $\square$

The Jacobian of $C[M; x_0, y_0]$ must belong to the universal family of elliptic curves with a specified k-rational point of order 5. Choosing a co-ordinate λ on $X_1(5)$ this family has equations

$$D_\lambda : \qquad y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2.$$

The cusps are at $\lambda = 0, \infty, \phi^5, \overline{\phi^5}$ where $\phi = 1 + \zeta_5 + \zeta_5^4$ is the golden ratio. In [8], [9] we wrote C_λ for the family of curves 5-isogenous to D_λ, and saw that $C_\lambda \simeq D_{\eta(\lambda)}$ over $k(\mu_5)$ where η is the involution $\lambda \mapsto (\phi^5\lambda + 1)/(\lambda - \phi^5)$. We give two methods for computing $\lambda = \lambda(M; x_0, y_0)$.

Proposition 14.2 *Let $C \subset \mathbf{P}^4$ be an elliptic normal quintic preserved by $M \in \mathrm{GL}_5(k)$. Let Q be a quadratic form whose translates under M define C. Let $B(u,v) = Q(u+v) - Q(u) - Q(v)$ be the corresponding bilinear form. Let $v_0, \ldots, v_4$ be the eigenvectors of M, ordered such that the corresponding eigenvalues are in geometric progression. Then C has Jacobian D_λ where*

$$\lambda = \eta(\lambda') \quad \text{and} \quad \lambda' = \prod_{i=0}^{4} \frac{Q(v_i)}{B(v_{i+1}, v_{i+4})}.$$

Proof. This is [19, Theorem 4.2]. The only modification we have made is to put the answer in Weierstrass form. □

Remark 14.3 The proof of Proposition 14.2 exhibits an isomorphism between the Jacobian of C and D_λ. This isomorphism is defined over a Galois extension of k. It maps the subgroup generated by M to the subgroup generated by $(x,y) = (0,0)$. But an elliptic curve equipped with a rational point of order 5 has no automorphisms. So comparing the above isomorphism with its Galois conjugates shows that it must after all be defined over k.

Our second method takes greater account of the form of the equations for $C[M; x_0, y_0]$. We define polynomials $F(x) = x^5 + 3x^4 + 4x^3 + 2x^2 + x$ and $G(x) = x^4 - 2x^3 + 4x^2 - 3x + 1$ satisfying

$$\phi^5 F(x) + G(x) = (\phi x + 1)^5 \quad \text{and} \quad F(x) - \phi^5 G(x) = (x - \phi)^5. \tag{50}$$

Proposition 14.4 *Let $C = C[M; x_0, y_0]$ be an elliptic normal quintic, with $y_0 = \sum_{i=0}^4 a_i x_i$. Let ω be a symbol[7] such that*

$$\prod_{\beta^5 = b} (a_0 + \beta a_1 + \ldots + \beta^4 a_4) = (a_0 + \omega)^5. \tag{51}$$

Then $C[M; x_0, y_0]$ has Jacobian D_λ where $\lambda = F(a_0 + \omega)/G(a_0 + \omega)$.

[7] For an introduction to symbolic notation see [12].

Proof. Let $e_0, \ldots, e_4$ be linear forms on $\mathbf{P}^4$ defined over $K = k(\mu_5, \sqrt[5]{b})$ with $Me_i = \zeta_5^i \sqrt[5]{b} e_i$ for $i = 0, \ldots, 4$. We further arrange that

$$x_0 = e_0 + \ldots + e_4 \quad \text{and} \quad y_0 = l_0 e_0 + \ldots + l_4 e_4$$

where the l_i are the linear forms on the left hand side of (51). According to [9, Proposition 2.8], C must have equations of the form

$$\tau_i e_i^2 + e_{i+1}e_{i+4} - \tau_{i+2}\tau_{i+3}e_{i+2}e_{i+3} = 0.$$

Comparing a few coefficients we find

$$\tau_i = \frac{(\phi l_i + 1)(l_i - \phi)}{(l_{i+1} - \phi)(l_{i+4} - \phi)}.$$

Continuing to work over K, the Jacobian of C is isomorphic to $C_{\lambda'}$ where

$$\begin{aligned} \lambda' &= \prod_{i=0}^{4} \left(\frac{\phi l_i + 1}{l_i - \phi} \right) && \text{by [9, Proposition 2.12]} \\ &= \left(\frac{\phi(a_0 + \omega) + 1}{a_0 + \omega - \phi} \right)^5 && \text{by (51)} \\ &= \frac{\phi^5 F(a_0 + \omega) + G(a_0 + \omega)}{F(a_0 + \omega) - \phi^5 G(a_0 + \omega)} && \text{by (50)} \end{aligned}$$

Putting $\lambda = \eta(\lambda') = F(a_0 + \omega)/G(a_0 + \omega)$ the Jacobian of C is isomorphic to D_λ. Remark 14.3 shows that this isomorphism is defined over k. $\square$

We give an example in the case $k = \mathbf{Q}$.

Example 14.5 Let $y_0 = x_0 + x_2 - x_3$ and $b = 3$. Then $C = C[M; x_0, y_0]$ is defined by the quadric

$$Q = 12x_0^2 - 9x_0x_1 - 3x_0x_4 + 3x_1x_2 + 4x_1x_4 - x_2^2 - x_3x_4$$

and its translates under M. Using either Proposition 14.2 or Proposition 14.4 the Jacobian is D_λ with $\lambda = 8$. For the latter we make the substitutions

$$(\omega, \omega^2, \omega^3, \omega^4, \omega^5) \mapsto (0, 3/2, 0, 9, -18).$$

On the other hand Algorithm 13.2 gives

$$c_4 = -48^4 \times 1055, \qquad c_6 = 48^6 \times 15535.$$

Each of these methods shows that the Jacobian is

$$50\text{B}2 \qquad y^2 + xy + y = x^3 + x^2 + 22x - 9.$$

Remark 14.6 Suppose we are given 5 quadrics defining an elliptic normal quintic and are told that its Jacobian has a k-rational point of order 5. To compute the Jacobian using Proposition 14.2 or Proposition 14.4 we must first find the matrix M. We do not know a good way of doing this. So even in this special case where the Jacobian has a k-rational point of order 5, our general algorithm is to be preferred.

A Character table for $\Gamma = \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$.

We write $\phi = 1 + \zeta_5 + \zeta_5^4$ and $\overline{\phi} = 1 - \phi = 1/\phi$ for its conjugate.

	1	1	20	20	30	12	12	12	12
	I	$-I$	ST	$-ST$	S	T	$-T$	T^2	$-T^2$
ψ_1	1	1	1	1	1	1	1	1	1
ψ_2	4	4	1	1	0	-1	-1	-1	-1
ψ_3	5	5	-1	-1	1	0	0	0	0
ψ_4	3	3	0	0	-1	ϕ	ϕ	$\overline{\phi}$	$\overline{\phi}$
ψ_5	3	3	0	0	-1	$\overline{\phi}$	$\overline{\phi}$	ϕ	ϕ
χ_1	2	-2	-1	1	0	$-\phi$	ϕ	$-\overline{\phi}$	$\overline{\phi}$
χ_2	2	-2	-1	1	0	$-\overline{\phi}$	$\overline{\phi}$	$-\phi$	ϕ
χ_3	4	-4	1	-1	0	-1	1	-1	1
χ_4	6	-6	0	0	0	1	-1	1	-1

B How big are the invariants?

Let c_4 and c_6 be the invariants for the elliptic normal quintic, as described in Theorem 1. The smaller invariant c_4 is a homogeneous polynomial of degree 20 in 50 variables. We aim to improve on the trivial upper bound

$$|c_4| \leq \binom{69}{20} \approx 1.156 \times 10^{17}.$$

We first consider the case $n = 3$. The invariant subring for the action of $\mathrm{SL}(W)$ on $k[S^3W]$ is generated by homogeneous polynomials of degrees 4 and 6 respectively. As explained in [23, §4.4-5] there are upper bounds

$$\begin{aligned} |c_4| &\leq \dim(S^4(S^3W))^{\mathbf{T}} &= 25 \\ |c_6| &\leq \dim(S^6(S^3W))^{\mathbf{T}} &= 103 \end{aligned} \tag{52}$$

where $\mathbf{T} \subset \mathrm{SL}(W)$ is the subgroup of diagonal matrices. But knowing explicit expressions for c_4 and c_6 we find $|c_4| = 25$ and $|c_6| = 103$. In other words, equality holds in (52).

Returning to the case $n = 5$, there are upper bounds

$$\begin{aligned} |c_4| &\leq \dim(S^{20}(\wedge^2 V \otimes W))^{\mathbf{T}} \\ |c_6| &\leq \dim(S^{30}(\wedge^2 V \otimes W))^{\mathbf{T}} \end{aligned}$$

where the maximal torus $\mathbf{T}$ is now the subgroup of $\mathrm{SL}(V) \times \mathrm{SL}(W)$ consisting of pairs of diagonal matrices. Even to compute the first of these estimates is a non-trivial combinatorial problem.

Definition B.1 *Let $f_r(x_1, \ldots, x_5)$ be the number of ways of placing $8r$ balls, equally distributed among r colours, in a 5×5 array of boxes such that*
(i) No balls are placed on the leading diagonal.
(ii) The arrangement is symmetric about the leading diagonal.
(iii) The row totals are $x_1, \ldots, x_5$.

It is clear that $f_r(x_1, \ldots, x_5) = 0$ unless $\sum x_i = 8r$ and $0 \leq x_i \leq 4r$. Some examples are

$$\begin{aligned} f_2(8,8,0,0,0) &= 1 \\ f_2(4,3,3,3,3) &= 2454. \end{aligned}$$

Let $X = \{x \in \mathbf{Z}^5 \mid f_2(x) \neq 0\}$. We find that $|X| = 3195$ and list the pairs $(x, f_2(x))$ for $x \in X$. It is feasible to store the function f_1 in a look-up table. Finally we compute

$$\begin{aligned} \dim S^{20}(\wedge^2 V \otimes W)^{\mathbf{T}} &= f_5(8,8,8,8,8) \\ &= \textstyle\sum_{x,y \in X} f_1(8 - x - y) f_2(x) f_2(y) \\ &= 172\,786\,883\,860 \\ &\approx 1.728 \times 10^{11}. \end{aligned}$$

Although this is only an upper bound for $|c_4|$, comparison with the case $n = 3$ suggests that it is not far from the truth. These observations support our belief that the invariants in the case $n = 5$ are too large to write down as explicit polynomials.

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 `pari` [3].

References

[1] A. Adler, S. Ramanan, *Moduli of abelian varieties*, Lecture Notes in Mathematics **1644**, Springer-Verlag, Berlin, 1996.

[2] 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.

[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, `pari/gp`, a computer algebra package, `http://www.parigp-home.de`

[4] D.J. Benson, *Polynomial invariants of finite groups,* London Mathematical Society, Lecture Note Series **190**, Cambridge University Press, Cambridge, 1993.

[5] 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.

[6] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[7] J.E. Cremona, Classical invariants and 2-descent on elliptic curves, *J. Symbolic Comput.* **31** (2001), no. 1-2, 71–87.

[8] T.A. Fisher, *On 5 and 7 descents for elliptic curves*, PhD thesis, University of Cambridge, 2000.

[9] T.A. Fisher, Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$, *J. Eur. Math. Soc.* **3** (2001), 169–201.

[10] T.A. Fisher, *The Cassels-Tate pairing and the Platonic solids*, to appear in *J. Number Theory.*

[11] T.A. Fisher, *On curves of genus one defined by Pfaffians*, preprint.

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

[13] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, New York-Heidelberg, 1977.

[14] G. Horrocks, D. Mumford, A rank 2 vector bundle on $\mathbf{P}^4$ with $15,000$ symmetries, *Topology* **12** (1973), 63–81.

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

[16] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[17] F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Translated by G. G. Morrice, Dover Publications, New York, 1956.

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

[19] C. O'Neil, Jacobians of genus one curves, *Math. Res. Lett.* **8** (2001), no. 1-2, 125–140.

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

[21] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[22] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

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

[24] J. Vélu, *Courbes elliptiques munies d'un sous-groupe* $\mathbf{Z}/n\mathbf{Z} \times \mu_n$, Bull. Soc. Math. France Mém. **57**, 1978.

[25] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris* Sér. A-B 273 (1971), A238–A241.

[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.*