THE HESSIAN OF A GENUS ONE CURVE

TOM FISHER

Abstract. We continue our development of the invariant theory of genus one curves with the aim of computing certain twists of the universal family of elliptic curves parametrised by the modular curve $X(n)$ for $n = 2, 3, 4, 5$. Our construction makes use of a covariant we call the Hessian, generalising the classical Hessian that exists in degrees 2 and 3. In particular we give explicit formulae and algorithms for computing the Hessian in degrees 4 and 5. This leads to a practical algorithm for computing equations for visible elements of order n in the Tate-Shafarevich group of an elliptic curve. Taking Jacobians we also recover the formulae of Rubin and Silverberg for families of n-congruent elliptic curves.

1. Introduction

In our earlier paper [17] we developed the invariant theory of genus one curves of degrees $n = 2, 3, 4, 5$, our main original contribution being in the case $n = 5$. In this paper we study the covariants of a genus one curve, and find that the classical Hessian in degrees 2 and 3 has a natural generalisation to degrees 4 and 5. The arithmetic significance of the Hessian is that it allows us to compute certain twists of the universal family of elliptic curves parametrised by the modular curve $X(n)$. The existence of the Hessian is most easily shown by a double application of the evectant construction, described by Salmon [27, Art. 233] in the case $n = 3$. For this reason we study the contravariants in parallel with the covariants. In the case $n = 5$ taking evectants is not practical since the invariants are too large to write down as explicit polynomials. Nonetheless we have found a practical algorithm for evaluating the Hessian in this case.

In Sections 3 and 4 we relate the invariants of a genus one curve to the invariants described by Klein in his *Lectures on the icosahedron* [22]. We extend these methods in Sections 5 and 6 to show that the covariants and contravariants each form a free module of rank 2 over the ring of invariants. The invariants, covariants and contravariants are related by identities recorded in Sections 8 and 9. We call the polynomials arising in this context the *Hesse polynomials*. In Section 10 we give formulae for the Hessian and the contravariants in the cases $n = 2, 3, 4$. Our algorithm for evaluating the Hessian in the case $n = 5$ is described in Section 11.

We then turn to arithmetic applications. In Section 12 we discuss the relationship between a genus one normal curve $C \to \mathbb{P}^{n-1}$ and the n by n matrices that

Date: 25th November 2010.

describe the action of the n-torsion of its Jacobian. This is useful both for the later sections of this paper, and for the Hesse pencil method of n-descent, as described in [9, Section 5.1].

In Section 13 we show that the Hesse polynomials define the family of elliptic curves directly n-congruent to a given elliptic curve for $n = 2, 3, 4, 5$. These formulae were previously obtained by Rubin and Silverberg [25], [26], [28] by a different method. Let us note however that our formulae in the case $n = 3$ were already known to Salmon [27, Art. 230]. One advantage of our method is that it generalises immediately to the family of elliptic curves reverse n-congruent to a given elliptic curve.

In Sections 14 and 15 we use the Hessian to compute equations for elements in the Tate-Shafarevich group of an elliptic curve that are visible in the sense of Mazur [12], [24]. In the terminology of [24] we have developed the invariant theory necessary to compute both first and second twists.

We have contributed all formulae and algorithms in this paper to the computer algebra system MAGMA [23, Version 2.13].

2. Background and overview

We work over a perfect field K of characteristic not dividing $6n$. We write $\overline{K}$ for the algebraic closure and identify all K-schemes with their sets of $\overline{K}$-points. We recall some of our notation and results from [17].

Definition 2.1. A *genus one model* of degree $n = 2, 3, 4, 5$ is
(i) if $n = 2$ a binary quartic
(ii) if $n = 3$ a ternary cubic
(iii) if $n = 4$ a pair of quadrics in 4 variables
(iv) if $n = 5$ a 5×5 alternating matrix of linear forms in 5 variables.

We write X_n for the space of genus one models of degree n. It is an affine space of dimension $N = 10n/(6 - n)$. We give the co-ordinate ring $K[X_n]$ its usual grading by degree. A model $\phi \in X_n$ defines a subvariety C_ϕ of $\mathbb{P}(1, 1, 2)$ or $\mathbb{P}^{n-1}$ according as $n = 2$ or $n = 3, 4, 5$. In the case $n = 5$ the equations are the 4×4 Pfaffians of ϕ. A model ϕ is non-singular if C_ϕ is a smooth curve of genus one.

In [17] we defined a linear algebraic group $\mathcal{G}_n$ acting on X_n and said that models $\phi, \phi' \in X_n$ are equivalent if they belong to the same $\mathcal{G}_n$-orbit. We also defined a rational character on $\mathcal{G}_n$ by

$$\begin{array}{llll}
n = 2 & \det : \mathbb{G}_m \times \mathrm{GL}_2 \to \mathbb{G}_m; & [\mu, B] & \mapsto \mu \det B \\
n = 3 & \det : \mathbb{G}_m \times \mathrm{GL}_3 \to \mathbb{G}_m; & [\mu, B] & \mapsto \mu \det B \\
n = 4 & \det : \mathrm{GL}_2 \times \mathrm{GL}_4 \to \mathbb{G}_m; & [A, B] & \mapsto \det A \det B \\
n = 5 & \det : \mathrm{GL}_5 \times \mathrm{GL}_5 \to \mathbb{G}_m; & [A, B] & \mapsto (\det A)^2 \det B.
\end{array}$$

Notice that the definitions of $\mathcal{G}_2$ and X_2 are slightly different from those in [17, Section 3.2], since we will not be working over fields of characteristic 2. We write G_n for the commutator subgroup of $\mathcal{G}_n$. Thus $G_2 = \mathrm{SL}_2$, $G_3 = \mathrm{SL}_3$, $G_4 = \mathrm{SL}_2 \times \mathrm{SL}_4$ and $G_5 = \mathrm{SL}_5 \times \mathrm{SL}_5$.

Definition 2.2. The *ring of invariants* is

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

An invariant F has *weight* k if $F \circ g = (\det g)^k F$ for all $g \in \mathcal{G}_n$.

Lemma 2.3. *Every homogeneous invariant of degree d has weight k where $d = kn/(6-n)$.*

Proof: This is [17, Lemma 4.3]. Some care is needed in the case $n = 2$ since we have changed the definitions of $\mathcal{G}_2$ and X_2. □

Theorem 2.4. *Let $n = 2, 3, 4, 5$. There are invariants c_4, c_6 and Δ of weights 4, 6 and 12, related by $c_4^3 - c_6^2 = 1728\Delta$, such that*

(i) *The ring of invariants $K[X_n]^{G_n}$ is generated by c_4 and c_6.*
(ii) *A model $\phi \in X_n$ is non-singular if and only if $\Delta(\phi) \neq 0$.*
(iii) *If $\phi \in X_n(K)$ is non-singular then C_ϕ is a smooth curve of genus one defined over K with Jacobian $y^2 = x^3 - 27c_4(\phi)x - 54c_6(\phi)$.*

Proof: This is [17, Theorem 4.4]. The cases $n = 2, 3, 4$ are classical: see for example [1], [29]. □

For $g \in \mathcal{G}_n$ we write g^T for the element obtained by transposing the constituent matrices. We also write g^{-T} for $(g^T)^{-1}$.

Definition 2.5. A polynomial map $F : X_n \to X_n$ defined over K is

(i) a *covariant* if $F \circ g = g \circ F$ for all $g \in G_n$,
(ii) a *contravariant* if $F \circ g = g^{-T} \circ F$ for all $g \in G_n$.

A covariant or contravariant F is homogeneous of degree d if $F(\lambda\phi) = \lambda^d F(\phi)$ for all $\lambda \in \overline{K}$ and $\phi \in X_n$. It has *weight* k if $F \circ g = (\det g)^k g \circ F$, respectively $F \circ g = (\det g)^k g^{-T} \circ F$ for all $g \in \mathcal{G}_n$.

It is clear that the covariants and contravariants each form a module over the ring of invariants $K[X_n]^{G_n} = K[c_4, c_6]$.

Lemma 2.6. *Every homogeneous covariant, respectively contravariant, of degree d has weight k where $d = 1 + kn/(6-n)$, respectively $d = -1 + kn/(6-n)$.*

Proof: The proof is similar to that of Lemma 2.3. □

We are ready to state our main theorem.

Theorem 2.7. (i) *The covariants form a free* $K[c_4, c_6]$*-module of rank* 2 *generated by covariants* U *and* H *of weights* 0 *and* 2*.*

(ii) *The contravariants form a free* $K[c_4, c_6]$*-module of rank* 2 *generated by contravariants* P *and* Q *of weights* 4 *and* 6*.*

Our labelling of the covariants as U and H, and contravariants as P and Q, follows the notation used by Salmon [27, Arts 217-221] in the case $n = 3$. The covariant U is the identity map. We call H the Hessian since in degrees 2 and 3 it is computed as the determinant of the matrix of second partial derivatives. We know of no such simple construction in degrees 4 and 5. Since the Hessian of a genus one model is again a genus one model there is no natural generalisation of the statement (specific to the case $n = 3$) that a plane cubic and its Hessian meet at the points of inflection of the cubic.

3. The discrete invariants

We recall some classical theory from Klein's *Lectures on the icosahedron* [22].

Definition 3.1. Let Δ_n be the subgroup of PGL_2 generated by

$$\begin{array}{lccc} n = 2 & \begin{pmatrix} 1 & 1/8 \\ 24 & -1 \end{pmatrix} & \text{and} & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ n = 3 & \begin{pmatrix} 1 & 1/3 \\ 6 & -1 \end{pmatrix} & \text{and} & \begin{pmatrix} 1 & 0 \\ 0 & \zeta_3 \end{pmatrix} \\ n = 4 & \begin{pmatrix} 1 & 1/2 \\ 2 & -1 \end{pmatrix} & \text{and} & \begin{pmatrix} 1 & 0 \\ 0 & \zeta_4 \end{pmatrix} \\ n = 5 & \begin{pmatrix} \varphi & 1 \\ 1 & -\varphi \end{pmatrix} & \text{and} & \begin{pmatrix} 1 & 0 \\ 0 & \zeta_5 \end{pmatrix} \end{array}$$

where ζ_n is a primitive nth root of unity and $\varphi = 1 + \zeta_5 + \zeta_5^4$.

For $n = 3, 4, 5$ the group Δ_n acts on $\mathbb{P}^1$ as the group of rotations of a tetrahedron, octahedron, icosahedron. Under stereographic projection the vertices of these Platonic solids are at the roots of

$$\begin{array}{ll} n = 2 & D = a(64a^2 - b^2) \\ n = 3 & D = -a(27a^3 + b^3) \\ n = 4 & D = ab(16a^4 - b^4) \\ n = 5 & D = ab(a^{10} - 11a^5b^5 - b^{10}). \end{array}$$

The midpoints of the faces and edges are at the roots of

$$c_4 = \tfrac{-1}{((\deg D)-1)^2} \begin{vmatrix} \frac{\partial^2 D}{\partial a^2} & \frac{\partial^2 D}{\partial a \partial b} \\ \frac{\partial^2 D}{\partial a \partial b} & \frac{\partial^2 D}{\partial b^2} \end{vmatrix} \tag{3.1}$$

and

$$c_6 = \tfrac{1}{\deg c_4} \begin{vmatrix} \frac{\partial D}{\partial a} & \frac{\partial D}{\partial b} \\ \frac{\partial c_4}{\partial a} & \frac{\partial c_4}{\partial b} \end{vmatrix}. \tag{3.2}$$

Definition 3.2. Let $\widetilde{\Gamma}_n$ be the inverse image of Δ_n in SL_2, and let Γ_n be the commutator subgroup of $\widetilde{\Gamma}_n$. The ring of *discrete invariants* is

$$K[a,b]^{\Gamma_n} = \{ f \in K[a,b] : f \circ \gamma = f \text{ for all } \gamma \in \Gamma_n \}.$$

Theorem 3.3 (Klein). *The ring of discrete invariants is generated by c_4, c_6 and D, subject only to the relation $c_4^3 - c_6^2 = 1728 D^n$.*

Proof: Since the characteristic of K does not divide the order of Γ_n this is a standard calculation. We checked the answer using MAGMA [23]. □

We describe the action of $\widetilde{\Gamma}_n$ on the discrete invariants.

Lemma 3.4. *There is a unique character $\chi : \widetilde{\Gamma}_n \to \mathbb{G}_m$ of order $6-n$ such that*

$$\begin{aligned} D \circ \gamma &= \chi(\gamma) D \\ c_4 \circ \gamma &= \chi(\gamma)^2 c_4 \\ c_6 \circ \gamma &= \chi(\gamma)^3 c_6 \end{aligned} \tag{3.3}$$

for all $\gamma \in \widetilde{\Gamma}_n$. Moreover $\ker(\chi) = \Gamma_n$.

Proof: This follows by direct calculation. □

4. The Hesse family

In Section 2 we defined the ring of invariants $K[X_n]^{G_n}$ and in Section 3 we defined the ring of discrete invariants $K[a,b]^{\Gamma_n}$. We now identify $K[X_n]^{G_n}$ as a subring of $K[a,b]^{\Gamma_n}$. To do this we first define a linear map $u_n : K^2 \to X_n$,

$$\begin{aligned} u_2(a,b) &= a(x^4+z^4) + b(\tfrac{1}{4}x^2z^2) \\ u_3(a,b) &= a(x^3+y^3+z^3) + bxyz \\ u_4(a,b) &= \begin{pmatrix} a(x_1^2+x_3^2) - bx_2x_4 \\ a(x_2^2+x_4^2) - bx_1x_3 \end{pmatrix} \\ u_5(a,b) &= \begin{pmatrix} 0 & ax_1 & bx_2 & -bx_3 & -ax_4 \\ & 0 & ax_3 & bx_4 & -bx_5 \\ & & 0 & ax_5 & bx_1 \\ & - & & 0 & ax_2 \\ & & & & 0 \end{pmatrix}. \end{aligned}$$

The models $u_n(a,b)$ are called *Hesse models.* Collectively they form the *Hesse family.* The geometry of the Hesse family is discussed, for example, in [2], [3] in the cases $n = 3, 5$. The following two propositions will be proved in Section 7.

Proposition 4.1. *Every non-singular model $\phi \in X_n$ is equivalent to a Hesse model.*

Proposition 4.2. *Let $\mathcal{G}_n$ and $\widetilde{\Gamma}_n$ be the groups defined in Sections 2 and 3.*

(i) *There exists $g \in \mathcal{G}_n$ with $g \circ u_n = u_n$ and $\det(g) = -1$.*

(ii) *For each $\gamma \in \widetilde{\Gamma}_n$ there exists $g \in \mathcal{G}_n$ with $g \circ u_n = u_n \circ \gamma$.*

The map $u_n : K^2 \to X_n$ induces a homomorphism of polynomial rings $u_n^* : K[X_n] \to K[a,b]\,;\ F \mapsto F \circ u_n$. Proposition 4.2(ii) implies an analogous result where $\mathcal{G}_n$ and $\widetilde{\Gamma}_n$ are replaced by their commutator subgroups G_n and Γ_n. It follows that u_n^* restricts to a map

$$u_n^* : K[X_n]^{G_n} \to K[a,b]^{\Gamma_n}.$$

Lemma 4.3. *The map $u_n^* : K[X_n]^{G_n} \to K[a,b]^{\Gamma_n}$ is injective.*

Proof: Let $F \in K[X_n]^{G_n}$ be a homogeneous invariant vanishing on the Hesse family. By Proposition 4.1 it also vanishes at every non-singular $\phi \in X_n$. By Theorem 2.4(ii) the latter are Zariski dense in X_n. It follows that F is identically zero. □

Lemma 4.4. *The map u_n^* takes the invariants c_4, c_6 and Δ of Theorem 2.4 to the discrete invariants c_4, c_6 and D^n of Theorem 3.3.*

Proof: We compute the invariants of the generic Hesse model using the formulae and algorithms in [17, Sections 7 and 8]. This gives an alternative computational proof of Lemma 4.3. □

Lemma 4.5. *If $g \in \mathcal{G}_n$ and $\gamma \in \widetilde{\Gamma}_n$ satisfy $g \circ u_n = u_n \circ \gamma$ then $\chi(\gamma) = (\det g)^2$.*

PROOF: The map u_n^* identifies the invariants c_4 and c_6 with the corresponding discrete invariants. Since the former have weights 4 and 6, and the latter satisfy (3.3), we deduce

$$\begin{aligned} \chi(\gamma)^2 c_4(a,b) &= (\det g)^4 c_4(a,b) \\ \chi(\gamma)^3 c_6(a,b) &= (\det g)^6 c_6(a,b). \end{aligned}$$

It follows that $\chi(\gamma) = (\det g)^2$. □

We say that a discrete invariant is an invariant if it belongs to the image of u_n^*. The following theorem characterises the invariants among the discrete invariants, and thus serves as a prototype for our treatment of the covariants and contravariants in Section 6.

Theorem 4.6. *Let f be a homogeneous discrete invariant of degree d. Then f is an invariant if and only if $d = kn/(6-n)$ for some even integer k and*

$$f \circ \gamma = \chi(\gamma)^{k/2} f \tag{4.1}$$

for all $\gamma \in \widetilde{\Gamma}_n$.

PROOF: Suppose that $f = F \circ u_n$ for some invariant F. Lemma 2.3 shows that since F is homogeneous of degree d it has weight k where $d = kn/(6-n)$. We use Proposition 4.2(i) to show that k is even, and then Proposition 4.2(ii) combined with Lemma 4.5 to establish (4.1).

For the converse we use the description of the discrete invariants given in Theorem 3.3, namely that $K[a,b]^{\Gamma_n}$ is a free $K[c_4,c_6]$-module of rank n with basis $1, D, \ldots, D^{n-1}$. Using Lemma 3.4 we find that c_4 and c_6 satisfy the conditions required of an invariant, but D, D^2, …, D^{n-1} do not. It only remains to show that there are invariants of weights 4 and 6. This was established in Theorem 2.4. □

Remark 4.7. Our use of the Hesse family in the above proof is analogous to our use of the Weierstrass family in the proof of Theorem 2.4. The advantage of the Weierstrass family is that it allows us to work without restriction on the characteristic of K. The advantage of the Hesse family is that it allows us to study the covariants and contravariants.

5. The discrete covariants

In Section 3 we defined subgroups $\Gamma_n \subset \mathrm{SL}_2$ for $n = 2, 3, 4, 5$.

Definition 5.1. A *discrete covariant* is a Γ_n-equivariant polynomial map $p : K^2 \to K^2$. It is represented by a pair of polynomials (p_1, p_2) with $p_1, p_2 \in K[a,b]$.

The discrete covariants form a module M over the ring of discrete invariants $R = K[a,b]^{\Gamma_n} = K[D, c_4, c_6]$. There is a derivation

$$\partial : R \to M\,; \quad f \mapsto (-\tfrac{\partial f}{\partial b}, \tfrac{\partial f}{\partial a})$$

and an R-bilinear alternating form

$$[\ ,\ ] : M \times M \to R\,; \quad (p,q) \mapsto p_1 q_2 - p_2 q_1.$$

We write $U = (a,b)$ for the identity map.

Theorem 5.2. *The discrete covariants form a free $K[c_4, c_6]$-module of rank $2n$ with basis $D^i U$, $D^i \partial D$, ∂c_4, ∂c_6 for $i = 0, 1, \ldots, n-2$.*

For the proof we first show that M is a free $K[c_4, c_6]$-module. Then we show, by computing the Hilbert series, that the elements listed have the right degrees to be generators. Finally we check that our putative basis is independent.

Lemma 5.3. *M is a free $K[c_4, c_6]$-module.*

Proof: The proof follows the method described in [4, Section 4.3].

Since c_4 and c_6 are coprime they form a regular sequence in $K[a,b]$, and so $K[a,b]$ is a free $K[c_4, c_6]$-module. The projection map

$$K[a,b]^2 \to M\,; \quad p \mapsto \frac{1}{|\Gamma_n|} \sum_{\gamma \in \Gamma_n} \gamma \circ p \circ \gamma^{-1}$$

shows that M 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. □

Lemma 5.4. *The Hilbert series of M is*

$$h_M(z) = \frac{(z^{r-1} + z^{s-1}) + \sum_{i=0}^{n-2} (z^{it+1} + z^{it+t-1})}{(1-z^r)(1-z^s)}$$

where $r = \deg c_4$, $s = \deg c_6$ and $t = \deg D$.

Proof: By Molien's theorem [4, Theorem 2.5.3] the Hilbert series of R and M are

$$h_R(z) = \frac{1}{|\Gamma_n|} \sum_{\gamma \in \Gamma_n} \frac{1}{1 - \mathrm{Tr}(\gamma) z + z^2}$$

and

$$h_M(z) = \frac{1}{|\Gamma_n|} \sum_{\gamma \in \Gamma_n} \frac{\mathrm{Tr}(\gamma)}{1 - \mathrm{Tr}(\gamma) z + z^2}.$$

Thus

$$(1 + z^2) h_R(z) = 1 + z h_M(z).$$

But by Theorem 3.3 we already have

$$h_R(z) = \frac{\sum_{i=0}^{n-1} z^{it}}{(1-z^r)(1-z^s)}.$$

The lemma follows on noting that $(n-1)t+1 = r+s-1$. (In fact $r = 4n/(6-n)$, $s = 6n/(6-n)$ and $t = 12/(6-n)$.) □

By Lemma 5.4 the discrete covariants listed in the statement of Theorem 5.2 have the right degrees to generate M as a $K[c_4, c_6]$-module. It remains to show that they are independent.

Lemma 5.5. *Let f be a non-zero homogeneous discrete invariant. If* $\operatorname{char}(K) \nmid \deg(f)$ *then the discrete covariants U and ∂f generate a free R-module M_f with $fM \subset M_f \subset M$.*

Proof: The module M_f is free since by Euler's identity we have

$$[U, \partial f] = (\deg f) f \neq 0.$$

It contains fM since for $p \in M$ we have

$$(\deg f) f p = -[\partial f, p] U + [U, p] \partial f. \tag{5.1}$$

□

In the notation of this section we may re-write (3.2) as

$$[\partial D, \partial c_4] = (\deg c_4) c_6. \tag{5.2}$$

Applying ∂ and then $[\partial D, -]$ to the relation of Theorem 3.3 we obtain

$$[\partial D, \partial c_6] = (\deg c_6) c_4^2. \tag{5.3}$$

Then we take $f = D$ in (5.1) to get

$$\begin{aligned} 3D\partial c_4 &= n(-c_6 U + c_4 \partial D) \\ 2D\partial c_6 &= n(-c_4^2 U + c_6 \partial D). \end{aligned} \tag{5.4}$$

Taking linear combinations and using the identity $c_4^3 - c_6^2 = 1728 D^n$ we find

$$\begin{aligned} 1728 n D^{n-1} U &= 3c_6 \partial c_4 - 2c_4 \partial c_6 \\ 1728 n D^{n-1} \partial D &= 3c_4^2 \partial c_4 - 2c_6 \partial c_6. \end{aligned} \tag{5.5}$$

We already know by Theorem 3.3 that R is a free $K[c_4, c_6]$-module of rank n, with basis $1, D, \ldots, D^{n-1}$. Taking $f = D$ in Lemma 5.5 it follows that M is a $K[c_4, c_6]$-module of rank $2n$. Moreover the discrete covariants $D^i U, D^i \partial D$ for $i = 0, 1, \ldots, n-1$ generate a free submodule of maximal rank. The relations (5.4) and (5.5) show that we can replace $D^{n-1}U$ and $D^{n-1}\partial D$ by ∂c_4 and ∂c_6 without destroying this property. In other words the discrete covariants listed in the statement of Theorem 5.2 are independent. This completes the proof of Theorem 5.2.

We describe the action of $\widetilde{\Gamma}_n$ on the discrete covariants. The character $\chi : \widetilde{\Gamma}_n \to \mathbb{G}_m$ was defined in Lemma 3.4.

Lemma 5.6. *If a discrete invariant f satisfies*

$$f \circ \gamma = \chi(\gamma)^r f$$

for all $\gamma \in \Gamma_n$, then the discrete covariant $p = \partial f$ satisfies

$$p \circ \gamma = \chi(\gamma)^r \gamma \circ p$$

for all $\gamma \in \Gamma_n$.

Proof: This is proved by a short calculation using the chain rule. □

6. The covariants and contravariants

We use the discrete covariants to study the covariants and contravariants (see Definition 2.5), just as in Section 4 we used the discrete invariants to study the invariants. Recall that for $g \in \mathcal{G}_n$ we write g^T for the element obtained by transposing all constituent matrices. The following proposition will be proved in Section 7.

Proposition 6.1. *There is a finite subgroup $H_n \subset G_n$ with the following properties*

(i) $H_n = \{g \in G_n : g \circ u_n = u_n\}$
(ii) *The image of u_n is $X_n^{H_n} = \{\phi \in X_n : g\phi = \phi$ for all $g \in H_n\}$.*
(iii) *If $g \in H_n$ then $g^T \in H_n$.*

It is possible to view the contravariants as G_n-equivariant polynomial maps from X_n to its dual X_n^*. The connection is afforded by the following pairing on X_n.

Lemma 6.2. *There is a symmetric bilinear form $\langle\ ,\ \rangle$ on X_n such that*
(i) $\langle g\phi_1, \phi_2 \rangle = \langle \phi_1, g^T \phi_2 \rangle$ for all $g \in \mathcal{G}_n$ and $\phi_1, \phi_2 \in X_n$,
(ii) $\langle\ ,\ \rangle$ is non-degenerate on the image of u_n.

Proof: A suitable pairing is

$$\begin{array}{ll} n = 2 & \langle f, g \rangle = f(\frac{\partial}{\partial x}, \frac{\partial}{\partial z}) g(x, z) \\ n = 3 & \langle f, g \rangle = f(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}) g(x, y, z) \\ n = 4 & \langle f, g \rangle = \sum_{i=1}^2 f_i(\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_4}) g_i(x_1, \ldots, x_4) \\ n = 5 & \langle f, g \rangle = \sum_{i<j} f_{ij}(\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_5}) g_{ij}(x_1, \ldots, x_5). \end{array}$$

Properties (i) and (ii) are checked by routine calculation. □

The Hesse family was defined in Section 4 by specifying a map $u_n : K^2 \to X_n$. We now view K^2 as a space of column vectors. By Lemma 6.2(ii) there is a matrix $\varepsilon_n \in \mathrm{GL}_2(K)$ such that

$$\langle u_n(x), u_n(\varepsilon_n y) \rangle = x_1 y_2 - x_2 y_1 \tag{6.1}$$

for all $x, y \in K^2$. The following lemma is required for our treatment of the contravariants.

Lemma 6.3. *If $g \in \mathcal{G}_n$ and $\gamma \in \widetilde{\Gamma}_n$ satisfy $g \circ u_n = u_n \circ \gamma$ then*

$$g^{-T} \circ u_n \circ \varepsilon_n = u_n \circ \varepsilon_n \circ \gamma.$$

Proof: For $x, y \in K^2$ we have

$$\begin{aligned} \langle u_n(x), u_n(\varepsilon_n y)\rangle &= \langle u_n(\gamma x), u_n(\varepsilon_n \gamma y)\rangle && \text{by (6.1) and } \widetilde{\Gamma}_n \subset \mathrm{SL}_2 \\ &= \langle g(u_n(x)), u_n(\varepsilon_n \gamma y)\rangle && \text{since } g \circ u_n = u_n \circ \gamma \\ &= \langle u_n(x), g^T(u_n(\varepsilon_n \gamma y))\rangle && \text{by Lemma 6.2(i).} \end{aligned}$$

Since g acts on the image of u_n, Proposition 6.1(i) gives $gH_ng^{-1} = H_n$. We deduce by Proposition 6.1(iii) that $g^TH_ng^{-T} = H_n$ and hence by Proposition 6.1(ii) that g^T acts on the image of u_n. The lemma now follows by Lemma 6.2(ii) and the above calculation. □

Proposition 6.4. *Let $F : X_n \to X_n$ be a covariant, respectively contravariant. Then there is a discrete covariant f such that $F \circ u_n = u_n \circ f$, respectively $F \circ u_n = u_n \circ \varepsilon_n \circ f$. Moreover F is uniquely determined by f.*

Proof: Proposition 6.1 shows that F acts on the image of u_n. So there is a polynomial map $f : K^2 \to K^2$ satisfying $F \circ u_n = u_n \circ f$, respectively $F \circ u_n = u_n \circ \varepsilon_n \circ f$. It follows by Proposition 4.2(ii), combined with Lemma 6.3 in the case F is a contravariant, that f is a discrete covariant.

If F_1 and F_2 determine the same discrete covariant f then by Proposition 4.1 they agree on all non-singular models. By Theorem 2.4(ii) the non-singular models are Zariski dense in X_n, and from this we deduce that $F_1 = F_2$. □

We say that a discrete covariant f is a covariant, respectively contravariant, if it arises as described in Proposition 6.4. We obtain the following analogue of Theorem 4.6.

Theorem 6.5. *Let f be a homogeneous discrete covariant of degree d. Then f is a covariant, respectively contravariant, if and only if $d = 1 + kn/(6-n)$, respectively $d = -1 + kn/(6-n)$, for some even integer k and*

$$f \circ \gamma = \chi(\gamma)^{k/2}\gamma \circ f \tag{6.2}$$

for all $\gamma \in \widetilde{\Gamma}_n$.

Proof: Suppose that $F \circ u_n = u_n \circ f$, respectively $F \circ u_n = u_n \circ \varepsilon_n \circ f$, for some covariant, respectively contravariant, F. Lemma 2.6 shows that, since F is homogeneous of degree d, it has weight k where $d = 1 + kn/(6-n)$, respectively $d = -1 + kn/(6-n)$. In the case F is a covariant we use Proposition 4.2(i) to show that k is even, and Proposition 4.2(ii) combined with Lemma 4.5 to establish (6.2). In the case F is a contravariant we use Lemma 6.3 to make the necessary modifications.

For the converse we use the description of the discrete covariants given in Theorem 5.2, namely that M is a free $K[c_4, c_6]$-module generated by $D^i U$, $D^i \partial D$, ∂c_4, ∂c_6 for $i = 0, \ldots, n-2$. Using Lemmas 3.4 and 5.6 we find that only U and ∂D satisfy the conditions required of a covariant (with $k = 0, 2$) and only ∂c_4 and ∂c_6 satisfy the conditions required of a contravariant (with $k = 4, 6$). To complete the proofs of Theorems 2.7 and 6.5, it remains to show that there are covariants of weights 0 and 2 and contravariants of weights 4 and 6.

We construct the contravariants using a method described by Salmon in the case $n = 3$; see [27, Arts. 220, 221]. By Lemma 6.2 we may identify the contravariants with the space $\mathrm{Pol}_{G_n}(X_n, X_n^*)$ of G_n-equivariant polynomial maps from X_n to its dual X_n^*. If we pick a basis $x_1, \ldots, x_N$ for X_n^* then $K[X_n] = K[x_1, \ldots, x_N]$ and there is a derivation

$$\delta : K[X_n]^{G_n} \to \mathrm{Pol}_{G_n}(X_n, X_n^*)$$

given by $(\delta F)(\phi) = \sum_{i=1}^N \frac{\partial F}{\partial x_i}(\phi) x_i$. It may be checked that δ is independent of the choice of basis $x_1, \ldots, x_N$. The contravariants of weights 4 and 6 are the so-called evectants δc_4 and δc_6 of the invariants c_4 and c_6 in Theorem 2.4.

The covariant of weight 0 is of course the identity map. So it only remains to show that there is a covariant of weight 2. It is clear from Definition 2.5 that the composition of two contravariants is a covariant. If $n = 2$ then the contravariants have degrees 1 and 2, and their composition is the required covariant of weight 2. Otherwise, composing the contravariant of weight 4 with itself we find that

$$f_n(c_4, c_6) U + g_n(c_4, c_6) \partial D$$

is a covariant where

$$\begin{aligned} f_3(c_4, c_6) &= 3c_4^2 & \qquad f_4(c_4, c_6) &= 81c_4^6 + 40c_4^3c_6^2 - c_6^4 \\ g_3(c_4, c_6) &= c_6 & \qquad g_4(c_4, c_6) &= 6c_4c_6(5c_4^3 - c_6^2) \end{aligned}$$

and

$$\begin{aligned} f_5(c_4, c_6) =& 184528125c_4^{18} + 230364000c_4^{15}c_6^2 - 25697763c_4^{12}c_6^4 \\ & \qquad + 4909960c_4^9c_6^6 + 44583c_4^6c_6^8 + 984c_4^3c_6^{10} - c_6^{12} \\ g_5(c_4, c_6) =& 18c_4c_6(2399625c_4^{15} - 658917c_4^{12}c_6^2 \\ & \qquad + 245498c_4^9c_6^4 + 4246c_4^6c_6^6 + 205c_4^3c_6^8 - c_6^{10}). \end{aligned}$$

Since U is a covariant it follows that $g_n(c_4, c_6) \partial D$ is a covariant.

Let f be a homogeneous discrete invariant of positive degree with $D \nmid f$. We claim that if $f \partial D$ is a covariant then $f_1 \partial D$ is also a covariant for some proper factor f_1 of f. To see this let $(a : b)$ be a root of f. Then $\phi = u_n(a, b)$ is non-singular since $D(a, b) \neq 0$. By [17, Lemma 4.10] the Zariski closure of the orbit of

ϕ is the zero locus of an irreducible invariant F. The covariant corresponding to $f\partial D$ vanishes on the orbit of ϕ and is therefore divisible by F. This proves the claim.

Finally we check for $n = 3, 4, 5$ that $g_n(c_4, c_6)$ is not divisible by $\Delta = (c_4^3 - c_6^2)/1728$, equivalently $g_n(1,1) \neq 0$. In fact $g_3(1,1) = 1$, $g_4(1,1) = 2^3 \cdot 3$ and $g_5(1,1) = 2^{14} \cdot 3^7$. It follows by the claim in the last paragraph that ∂D is a covariant. □

We write $U : X_n \to X_n$ for the identity map.

Definition 6.6. (i) The Hessian $H : X_n \to X_n$ is the unique covariant (of weight 2) satisfying

$$H \circ u_n = u_n \circ \partial D.$$

(ii) The contravariants $P, Q : X_n \to X_n$ are the unique contravariants (of weights 4 and 6) satisfying

$$\begin{aligned} \kappa^{-1}(\deg c_4) P \circ u_n &= u_n \circ \varepsilon_n \circ \partial c_4 \\ \kappa^{-1}(\deg c_6) Q \circ u_n &= u_n \circ \varepsilon_n \circ \partial c_6. \end{aligned}$$

where $\kappa = 1/4, 1, 2, 5$ for $n = 2, 3, 4, 5$. (The scaling factor κ has been chosen to simplify the formulae in Section 10.)

Theorem 6.7. *Let $\langle\ ,\ \rangle$ be the pairing defined in the proof of Lemma 6.2. Then*

$$\begin{aligned} \langle U, P \rangle &= \kappa c_4 & \qquad \langle H, P \rangle &= \kappa c_6 \\ \langle U, Q \rangle &= \kappa c_6 & \qquad \langle H, Q \rangle &= \kappa c_4^2. \end{aligned}$$

Proof: It suffices to prove this for $\phi \in X_n$ a Hesse model. By (6.1) the required identities are

$$\begin{aligned} [U, \partial c_4] &= (\deg c_4) c_4 & \qquad [\partial D, \partial c_4] &= (\deg c_4) c_6 \\ [U, \partial c_6] &= (\deg c_6) c_6 & \qquad [\partial D, \partial c_6] &= (\deg c_6) c_4^2. \end{aligned}$$

These were proved in Section 5. □

7. The Heisenberg group

In this section we prove some results postponed from Sections 4 and 6.

Definition 7.1. A genus one normal curve $C \to \mathbb{P}^{n-1}$ is
(i) if $n = 2$ a double cover of $\mathbb{P}^1$ ramified at 4 points,
(ii) if $n \geq 3$ a genus one curve embedded in $\mathbb{P}^{n-1}$ by a complete linear system of degree n.

It is well known that $E = \mathrm{Jac}(C)$ acts on C by translation, and translation by $P \in E$ extends to an automorphism of $\mathbb{P}^{n-1}$ if and only if $P \in E[n]$.

Definition 7.2. The Heisenberg group of $C \to \mathbb{P}^{n-1}$ is the group of all matrices in SL_n that act on C as translation by an n-torsion point of its Jacobian. As a group it is a central extension of $E[n]$ by μ_n with commutator given by the Weil pairing $e_n : E[n] \times E[n] \to \mu_n$.

Definition 7.3. The standard Heisenberg group of degree n is the subgroup $H_n \subset \mathrm{SL}_n$ generated by

$$\sigma_n = \xi_n \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix}, \text{ and } \tau_n = \xi_n \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

where $\xi_n = 1$ for n odd, and $\xi_n = \zeta_{2n}$ for n even.

Lemma 7.4. *Let $C \to \mathbb{P}^{n-1}$ be a genus one normal curve with Jacobian E. Let S, T be a basis for $E[n]$ with $e_n(S,T) = \zeta_n$. Then we can change co-ordinates on $\mathbb{P}^{n-1}$ so that translation by S and T is given by the images of σ_n and τ_n in PGL_n. In particular $C \to \mathbb{P}^{n-1}$ has Heisenberg group H_n.*

PROOF: This is standard. See for example [14, Proposition 2.3]. □

The following lemma is based on results in [21, Chapter III].

Lemma 7.5. *Let $C \to \mathbb{P}^{n-1}$ be a genus one normal curve with Heisenberg group H_n. If $n = 2, 3, 4, 5$ then $C = C_\phi$ for some Hesse model ϕ.*

PROOF: Case $n = 2$. We decompose X_2 as an H_2-module and find that (up to scalars) there are exactly three binary quartics whose roots are permuted by H_2, but do not belong to the Hesse family. These are the pairwise products of xz, $x^2 - z^2$ and $x^2 + z^2$. These quartics do not have Heisenberg group H_2, since H_2 fails to act transitively on their roots.

Case $n = 3$. We decompose X_3 as a H_3-module and find that (up to scalars) there are exactly eight ternary cubics that define curves fixed by H_3, but do not belong to the Hesse family. These are

$$\begin{array}{ll} x^3 + \zeta_3^i y^3 + \zeta_3^{2i} z^3 & \text{for } i = 1, 2 \\ x^2 y + \zeta_3^i y^2 z + \zeta_3^{2i} x z^2 & \text{for } i = 0, 1, 2 \\ x y^2 + \zeta_3^i y z^2 + \zeta_3^{2i} x^2 z & \text{for } i = 0, 1, 2. \end{array}$$

These curves do not have Heisenberg group H_3 since the action of H_3 modulo its centre is not fixed point free.

Case $n = 4$. We decompose the space of quadrics in 4 variables as an H_4-module. We find that there are exactly three 2-dimensional subspaces that define a curve fixed by H_4, but do not belong to the Hesse family. These are spanned by

$$\begin{array}{lll} x_1x_2 + x_3x_4 & \text{and} & x_2x_3 + x_1x_4, \\ x_1x_2 - x_3x_4 & \text{and} & x_2x_3 - x_1x_4, \\ x_1^2 - x_3^2 & \text{and} & x_2^2 - x_4^2. \end{array}$$

Each of these pairs of quadrics defines a singular curve.

Case $n = 5$. We take $C \subset \mathbb{P}^4$ with equations

$$ax_i^2 + bx_{i+1}x_{i+4} + cx_{i+2}x_{i+3} = 0 \qquad \text{for } i = 1, 2, 3, 4, 5$$

where all subscripts are read mod 5. Since C has Heisenberg group H_5 it meets the hyperplane $\{x_1 = 0\}$ in 5 distinct points. By Riemann-Roch these points span the hyperplane. So C contains a point of the form $(0 : z_2 : z_3 : z_4 : z_5)$ with each z_i non-zero. A short calculation then shows that $a^2 + bc = 0$ and so $C = C_\phi$ where $\phi = u_5(a, b)$. □

Lemma 7.6. *Let $\phi, \phi' \in X_n$ be non-singular models. If $C_\phi = C_{\phi'}$ then ϕ and ϕ' are equivalent. Moreover if $n = 4, 5$ and $\phi' = [A, I_n]\phi$ then $A \in \mathrm{GL}_2$ is uniquely determined if $n = 4$, and $A \in \mathrm{GL}_5$ is uniquely determined up to sign if $n = 5$.*

Proof: This is clear for $n = 2, 3, 4$. The case $n = 5$ follows from the Buchsbaum-Eisenbud acyclicity criterion and the properties of minimal free resolutions. See for example [17, Section 5.2]. □

Combining the last three lemmas shows that every non-singular model is equivalent to a Hesse model.

Proof of Proposition 4.1: Let $\phi \in X_n$ be a non-singular model. By definition this means that C_ϕ is a smooth curve of genus one. In the cases $n = 2, 3$ it is clear that $C_\phi \to \mathbb{P}^{n-1}$ is a genus one normal curve. The cases $n = 4, 5$ are treated in [17, Proposition 5.10(i)]. By Lemma 7.4 we may assume that $C_\phi \to \mathbb{P}^{n-1}$ has Heisenberg group H_n. Then Lemma 7.5 shows that $C_\phi = C_{\phi'}$ for some Hesse model ϕ' and finally Lemma 7.6 shows that ϕ and ϕ' are equivalent. □

If $n = 2, 3$ then H_n is already a subgroup of $G_n = \mathrm{SL}_n$. If $n = 4, 5$ we identify H_n as a subgroup of G_n via $\sigma_4 \mapsto [\sigma_2, \sigma_4]$, $\tau_4 \mapsto [\tau_2, \tau_4]$ and $\sigma_5 \mapsto [\zeta_5^3\sigma_5^4, \sigma_5]$, $\tau_5 \mapsto [\tau_5^3, \tau_5]$.

Lemma 7.7. *Let $u_n : K^2 \to X_n$ be the linear map defining the Hesse family. Then $g \circ u_n = u_n$ for all $g \in H_n$.*

Proof: This is checked by direct calculation. □

Lemma 7.8. *Let $\phi \in X_n$ be a non-singular Hesse model. Then C_ϕ has Heisenberg group H_n and $H_n = \{g \in G_n : g\phi = \phi\}$.*

PROOF: In view of the last two lemmas, it suffices to show that if $g \in G_n$ with $g\phi = \phi$ then the automorphism γ of C_ϕ induced by g is a translation map. By [17, Proposition 5.19] we have $\gamma^*\omega_\phi = \omega_\phi$. So this follows from [17, Lemma 2.4]. □

Next we show that $H_n \subset G_n$ has the properties stated in Section 6.

PROOF OF PROPOSITION 6.1: (i) We must show that $H_n = \{g \in G_n : g \circ u_n = u_n\}$. This follows from Lemmas 7.7 and 7.8.
(ii) By Lemma 7.7 we have $\operatorname{im}(u_n) \subset X_n^{H_n}$. We prove equality by showing that $\dim(X_n^{H_n}) = 2$. The character of X_n as a representation of H_n is constant on the centre of H_n and elsewhere takes value $\xi_n = 1, 1, 0$ for $n = 2, 3, 5$. Thus

$$\dim(X_n^{H_n}) = \frac{1}{n^3}(n \dim X_n + (n^3 - n)\xi_n) = 2.$$

The case $n = 4$ is similar.
(iii) It is clear from the definition of H_n that if $g \in H_n$ then $g^T \in H_n$. □

We prepare for the proof of Proposition 4.2 by describing the normaliser of H_n, where H_n is viewed first as a subgroup of GL_n and then as a subgroup of $\mathcal{G}_n$.

Lemma 7.9. *There is an exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & \Theta_n \arrow[r] & N_{\mathrm{GL}_n}(H_n) \arrow[r, "\pi"] & \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \arrow[r] & 0. \end{tikzcd}$$

where $\Theta_n \subset \mathrm{GL}_n$ is generated by H_n and the scalar matrices.

PROOF: Let $g \in \mathrm{GL}_n$ with $gH_ng^{-1} = H_n$. Writing $\propto$ for equality in PGL_n we have $g\,\sigma_n\,g^{-1} \propto \sigma_n^a\,\tau_n^c$ and $g\,\tau_n\,g^{-1} \propto \sigma_n^b\,\tau_n^d$ for some $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$. We define $\pi(g) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. It is easy to check that π is a group homomorphism with kernel Θ_n. Then Lemma 7.4 shows that $\operatorname{im}(\pi) = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. □

Lemma 7.10. *Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve with Heisenberg group H_n and $j(C) \neq 0, 1728$. If $g \in N_{\mathrm{GL}_n}(H_n)$ acts on C then $\pi(g) = \pm I_2$.*

PROOF: The translation maps identify $E = \operatorname{Jac}(C)$ as a normal subgroup of $\operatorname{Aut}(C)$. Conjugation by g acts on $\operatorname{Aut}(C)$ and hence on E. But the condition on the j-invariant ensures that the only automorphisms of E are $[\pm 1]$. □

Lemma 7.11. *There is an exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & \Theta_n' \arrow[r] & N_{\mathcal{G}_n}(H_n) \arrow[r, "\pi"] & \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \arrow[r] & 0 \end{tikzcd}$$

where $\Theta_n' \subset \mathcal{G}_n$ is generated by H_n and the centre of $\mathcal{G}_n$.

Proof: If $n = 2, 3$ then $\mathcal{G}_n = \mathbb{G}_m \times \mathrm{GL}_n$ and the lemma already follows by Lemma 7.9. If $n = 4, 5$ then $\mathcal{G}_n = \mathrm{GL}_m \times \mathrm{GL}_n$ where $m = 2, 5$. Projection onto the second factor gives a map $\iota : N_{\mathcal{G}_n}(H_n) \to N_{\mathrm{GL}_n}(H_n)$ whose kernel is contained in the centre of $\mathcal{G}_n$. The lemma will follow by Lemma 7.9 once we show that ι is surjective.

Let $B \in \mathrm{GL}_n$ with $BH_nB^{-1} = H_n$ and let $\phi \in X_n$ be a non-singular Hesse model. We know by Lemma 7.8 that C_ϕ has Heisenberg group H_n. If $\phi' = [I_m, B]\phi$ then $C_{\phi'}$ also has Heisenberg group H_n. So by Lemmas 7.5 and 7.6 there is a Hesse model ϕ'' with $\phi'' = [A, I_n]\phi'$ for some $A \in \mathrm{GL}_m$. Putting $g = [A, B]$ we have $\phi'' = g\phi$. Finally Lemma 7.8 shows that $gH_ng^{-1} = H_n$. □

Let $\alpha \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. By Lemma 7.11 there exists $g \in N_{\mathcal{G}_n}(H_n)$ with $\pi(g) = \alpha$. Proposition 6.1(ii) shows that g acts on the image of u_n. Since u_n is linear we have $g \circ u_n = u_n \circ \gamma$ for some $\gamma \in \mathrm{GL}_2$. Sending α to the class of γ defines a group homomorphism

$$\nu : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_2.$$

It is well defined by Lemmas 7.7 and 7.11. The subgroup $\Delta_n \subset \mathrm{PGL}_2$ was defined in Section 3.

Lemma 7.12. *The map ν has kernel $\{\pm I_2\}$ and image Δ_n.*

Proof: It is possible to prove the lemma by a direct calculation. An alternative method is as follows. First we use Lemma 7.10 to show that the kernel of ν is contained in $\{\pm I_2\}$. Then by Theorem 2.4(ii) and Lemma 4.4 the image of ν permutes the roots of D. Splitting into the cases $n = 2, 3, 4, 5$ it is easy to check that Δ_n is the full group of such automorphisms and $|\Delta_n| = |\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})|$. The lemma follows by counting. □

Proof of Proposition 4.2: (i) This can be proved by simply writing down a suitable element in the cases $n = 2, 3, 4, 5$. An alternative method is as follows. Let $(a : b)$ be a point on $\mathbb{P}^1$ that is fixed by no non-trivial element of Δ_n. Then $\phi = u_n(a, b)$ is a non-singular Hesse model. We claim that there exists $g \in \mathcal{G}_n$ with $g\phi = \phi$ and $\det g = -1$. To prove this we first use [17, Proposition 4.6] to reduce to the case of a Weierstrass model, and then take $g = \gamma_n([-1; 0, 0, 0])$ in [17, Proposition 4.7]. By Lemma 7.8 we have $gH_ng^{-1} = H_n$ and so $g \circ u_n = u_n \circ \gamma$ for some $\gamma \in \mathrm{GL}_2$. The image of γ in PGL_2 permutes the roots of D and hence belongs to Δ_n. Our choice of $(a : b)$ now forces γ to be a scalar matrix. Since $g\phi = \phi$ it follows that $g \circ u_n = u_n$.
(ii) We recall that $\widetilde{\Gamma}_n$ is the inverse image of Δ_n in SL_2. So this is immediate from Lemma 7.12. □

Remark 7.13. It is possible to interpret $\nu : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_2$ as describing the automorphisms of the modular curve $X(n) \cong \mathbb{P}^1$ obtained by relabelling the n-torsion of the elliptic curves parametrised by $Y(n)$.

Remark 7.14. By Definition 3.2 and Lemma 7.12 both $\widetilde{\Gamma}_n$ and $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ are central extensions of Δ_n by $\{\pm 1\}$. In the cases $n = 3, 5$ we have $\widetilde{\Gamma}_n \cong \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, but this is not true for $n = 2, 4$.

8. The Hesse polynomials

The Hessian $H : X_n \to X_n$ was defined in Section 6.

Lemma 8.1. *If $\phi \in X_n$ is non-singular then the subspace of X_n fixed by the stabiliser of ϕ in G_n is spanned by ϕ and $H(\phi)$.*

Proof: By Proposition 4.1 it suffices to prove the lemma for ϕ a Hesse model. Then by Lemma 7.8 the stabiliser is H_n and by Proposition 6.1(ii) the fixed subspace is the Hesse family. Writing $\phi = u_n(a, b)$ it only remains to check that (a, b) and $(-\frac{\partial D}{\partial b}, \frac{\partial D}{\partial a})$ are linearly independent. Since $D(a, b)^n = \Delta(\phi) \neq 0$ this is clear by Euler's identity. □

The pencil spanned by U and H has the following interpretation.

Theorem 8.2. *Let $C \to \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n = 2, 3, 4, 5$. Then $C = C_\phi$ for some $\phi \in X_n$ and*

(i) *If $\phi' = \lambda\phi + \mu H(\phi)$ is non-singular then $C_{\phi'} \to \mathbb{P}^{n-1}$ has the same Heisenberg group as $C \to \mathbb{P}^{n-1}$.*

(ii) *If $C' \to \mathbb{P}^{n-1}$ is a genus one normal curve with the same Heisenberg group as $C \to \mathbb{P}^{n-1}$ then $C' = C_{\phi'}$ for some $\phi' = \lambda\phi + \mu H(\phi)$.*

Proof: The existence of ϕ is clear for $n = 2, 3, 4$. In the case $n = 5$ the genus one model ϕ is computed from the equations defining C using the algorithm in [18], based on the Buchsbaum-Eisenbud structure theorem [6], [7] for Gorenstein ideals of codimension 3.
(i) By Proposition 4.1 we may assume that ϕ is a Hesse model. Since the Hessian H acts on the Hesse family it follows by Lemma 7.8 that both $C \to \mathbb{P}^{n-1}$ and $C' \to \mathbb{P}^{n-1}$ have Heisenberg group H_n
(ii) Again we may assume that ϕ is a Hesse model. Then Lemma 7.5 gives $C' = C_{\phi'}$ for some Hesse model ϕ'. Since $\phi, \phi' \in X_n$ both have stabiliser $H_n \subset G_n$ it follows by Lemma 8.1 that $\phi' = \lambda\phi + \mu H(\phi)$ for some $\lambda, \mu \in \overline{K}$. □

In the later sections of this paper we will be concerned with the arithmetic application of Theorem 8.2. First however we record some formulae.

Lemma 8.3. *There are polynomials $f(\lambda, \mu)$, $g(\lambda, \mu)$ with coefficients in $K[c_4, c_6]$ such that*

$$H(\lambda U + \mu H) = f(\lambda, \mu)U + g(\lambda, \mu)H.$$

Proof: Writing $H(\lambda U + \mu H) = \sum F_{ij} \lambda^i \mu^j$ it is clear that the F_{ij} are covariants. By Theorem 2.7(i) they are $K[c_4, c_6]$-linear combinations of U and H. □

We compute the polynomials $f(\lambda, \mu)$ and $g(\lambda, \mu)$ just by working with the Hesse family. The case $n = 3$ is classical: see [20, Section II.7] or [27, Art. 225]. We will see in Theorem 8.5 below that $f(\lambda, \mu)$ and $g(\lambda, \mu)$ are scalar multiples of the partial derivatives of

$$\mathbf{D}(\lambda, \mu) = \begin{vmatrix} \lambda & \mu \\ f(\lambda, \mu) & g(\lambda, \mu) \end{vmatrix}.$$

Lemma 8.4. *There are polynomials $\mathbf{D}(\lambda, \mu)$, $\mathbf{c}_4(\lambda, \mu)$ and $\mathbf{c}_6(\lambda, \mu)$ with coefficients in $K[c_4, c_6]$ such that*

$$\begin{aligned} \mathbf{D}(\lambda, \mu) &= D(\lambda a - \mu \tfrac{\partial D}{\partial b}, \lambda b + \mu \tfrac{\partial D}{\partial a})/D(a, b) \\ \mathbf{c}_4(\lambda, \mu) &= c_4(\lambda a - \mu \tfrac{\partial D}{\partial b}, \lambda b + \mu \tfrac{\partial D}{\partial a}) \\ \mathbf{c}_6(\lambda, \mu) &= c_6(\lambda a - \mu \tfrac{\partial D}{\partial b}, \lambda b + \mu \tfrac{\partial D}{\partial a}). \end{aligned}$$

Proof: The coefficients of $\mathbf{D}(\lambda, \mu)$ belong to $K[a, b]$ since if $D(a, b) = 0$ then $(a : b) = (-\frac{\partial D}{\partial b} : \frac{\partial D}{\partial a})$. The same is already clear for $\mathbf{c}_4(\lambda, \mu)$ and $\mathbf{c}_6(\lambda, \mu)$. We must show that the coefficients belong to $K[c_4, c_6]$.

Let $r = \deg c_4 = 4n/(6 - n)$. Putting $\mathbf{c}_4(\lambda, \mu) = \sum_{j=0}^{r} f_j \lambda^{r-j} \mu^j$ we find that $f_j \in K[a, b]$ has degree $2n(2 + j)/(6 - n)$ and satisfies $f_j \circ \gamma = \chi^{2+j}(\gamma) f_j$ for all $\gamma \in \widetilde{\Gamma}_n$. So f_j is a discrete invariant satisfying the conditions of Theorem 4.6. It therefore belongs to $K[c_4, c_6]$. The other cases are similar. □

We call $\mathbf{D}(\lambda, \mu)$, $\mathbf{c}_4(\lambda, \mu)$ and $\mathbf{c}_6(\lambda, \mu)$ the *Hesse polynomials*. They are easily computed from the description in Lemma 8.4. In the cases $n = 2, 3, 4, 5$ we find

$$\begin{aligned} \mathbf{D}(\lambda, \mu) &= \lambda^3 - 3c_4 \lambda \mu^2 - 2c_6 \mu^3 \\ \mathbf{D}(\lambda, \mu) &= \lambda^4 - 6c_4 \lambda^2 \mu^2 - 8c_6 \lambda \mu^3 - 3c_4^2 \mu^4 \\ \mathbf{D}(\lambda, \mu) &= \lambda^6 - 15c_4 \lambda^4 \mu^2 - 40c_6 \lambda^3 \mu^3 - 45c_4^2 \lambda^2 \mu^4 - 24c_4 c_6 \lambda \mu^5 + (27c_4^3 - 32c_6^2) \mu^6 \\ \mathbf{D}(\lambda, \mu) &= \lambda^{12} - 66c_4 \lambda^{10} \mu^2 - 440c_6 \lambda^9 \mu^3 - 1485c_4^2 \lambda^8 \mu^4 \\ &\quad - 3168c_4 c_6 \lambda^7 \mu^5 + (5940c_4^3 - 10560c_6^2) \lambda^6 \mu^6 - 4752c_4^2 c_6 \lambda^5 \mu^7 \\ &\quad - (66825c_4^4 - 63360c_4 c_6^2) \lambda^4 \mu^8 - (142560c_4^3 c_6 - 140800c_6^3) \lambda^3 \mu^9 \\ &\quad - (133650c_4^5 - 133056c_4^2 c_6^2) \lambda^2 \mu^{10} - (61560c_4^4 c_6 - 61440c_4 c_6^3) \lambda \mu^{11} \\ &\quad + (91125c_4^6 - 193536c_4^3 c_6^2 + 102400c_6^4) \mu^{12}. \end{aligned}$$

The polynomials $\mathbf{D}(\lambda,\mu)$ share with the $D(a,b)$ the property that their roots are arranged as the vertices of one of the Platonic solids. By (3.1) and (3.2) we have

$$\mathbf{c}_4(\lambda,\mu) = \tfrac{-1}{(\deg D)^2((\deg D)-1)^2} \begin{vmatrix} \frac{\partial^2 \mathbf{D}}{\partial \lambda^2}(\lambda,\mu) & \frac{\partial^2 \mathbf{D}}{\partial \lambda \partial \mu}(\lambda,\mu) \\ \frac{\partial^2 \mathbf{D}}{\partial \lambda \partial \mu}(\lambda,\mu) & \frac{\partial^2 \mathbf{D}}{\partial \mu^2}(\lambda,\mu) \end{vmatrix}$$

and

$$\mathbf{c}_6(\lambda,\mu) = \tfrac{1}{\deg D \deg c_4} \begin{vmatrix} \frac{\partial \mathbf{D}}{\partial \lambda}(\lambda,\mu) & \frac{\partial \mathbf{D}}{\partial \mu}(\lambda,\mu) \\ \frac{\partial \mathbf{c}_4}{\partial \lambda}(\lambda,\mu) & \frac{\partial \mathbf{c}_4}{\partial \mu}(\lambda,\mu) \end{vmatrix}.$$

The Hesse polynomials are related by

$$\mathbf{c}_4(\lambda,\mu)^3 - \mathbf{c}_6(\lambda,\mu)^2 = (c_4^3 - c_6^2)\,\mathbf{D}(\lambda,\mu)^n. \tag{8.1}$$

Theorem 8.5. *There are identities*

$$\begin{aligned} c_4(\lambda U + \mu H) &= \mathbf{c}_4(\lambda,\mu) \\ c_6(\lambda U + \mu H) &= \mathbf{c}_6(\lambda,\mu) \\ (\deg D) H(\lambda U + \mu H) &= -\tfrac{\partial \mathbf{D}}{\partial \mu}(\lambda,\mu) U + \tfrac{\partial \mathbf{D}}{\partial \lambda}(\lambda,\mu) H. \end{aligned}$$

Proof: As usual it suffices to check these relations on the Hesse family. Each is a straightforward consequence of Lemma 8.4. □

Remark 8.6. We have $\Delta(\lambda U + \mu H) = \Delta \mathbf{D}(\lambda,\mu)^n$. So the pencil spanned by a non-singular model and its Hessian has singular fibres at the roots of $\mathbf{D}(\lambda,\mu) = 0$. These may also be characterised as the fibres whose Hessian is a scalar multiple of the original model. (See also Theorem 12.2.)

9. The dual Hesse polynomials

In Section 8 we worked only with the invariants c_4 and c_6 and covariants U and H. If we bring the contravariants P and Q into play then there are many more identities to consider. Again these are already in [27] in the case $n = 3$.

Theorem 9.1. *There are identities*

$$\begin{aligned} (\deg c_4) P(\lambda U + \mu H) &= f_4(\lambda,\mu) P + g_4(\lambda,\mu) Q \\ (\deg c_6) Q(\lambda U + \mu H) &= f_6(\lambda,\mu) P + g_6(\lambda,\mu) Q \end{aligned}$$

where

$$\begin{pmatrix} f_4(\lambda,\mu) & f_6(\lambda,\mu) \\ g_4(\lambda,\mu) & g_6(\lambda,\mu) \end{pmatrix} = \begin{pmatrix} c_4 & c_6 \\ c_6 & c_4^2 \end{pmatrix}^{-1} \begin{pmatrix} \frac{\partial \mathbf{c}_4}{\partial \lambda}(\lambda,\mu) & \frac{\partial \mathbf{c}_6}{\partial \lambda}(\lambda,\mu) \\ \frac{\partial \mathbf{c}_4}{\partial \mu}(\lambda,\mu) & \frac{\partial \mathbf{c}_6}{\partial \mu}(\lambda,\mu) \end{pmatrix}.$$

Proof: Reducing to the Hesse family we must show that

$$(\deg \Delta) \begin{pmatrix} \partial c_4(\lambda U + \mu \partial D) \\ \partial c_6(\lambda U + \mu \partial D) \end{pmatrix} = \begin{pmatrix} f_4(\lambda,\mu) & g_4(\lambda,\mu) \\ f_6(\lambda,\mu) & g_6(\lambda,\mu) \end{pmatrix} \begin{pmatrix} 3\partial c_4 \\ 2\partial c_6 \end{pmatrix}.$$

This follows from

$$(\deg D) D \begin{pmatrix} \partial c_4(\lambda U + \mu \partial D) \\ \partial c_6(\lambda U + \mu \partial D) \end{pmatrix} = \begin{pmatrix} \frac{\partial \mathbf{c}_4}{\partial \lambda}(\lambda,\mu) & \frac{\partial \mathbf{c}_4}{\partial \mu}(\lambda,\mu) \\ \frac{\partial \mathbf{c}_6}{\partial \lambda}(\lambda,\mu) & \frac{\partial \mathbf{c}_6}{\partial \mu}(\lambda,\mu) \end{pmatrix} \begin{pmatrix} \partial D \\ -U \end{pmatrix}$$

which is obtained by differentiating the definition in Lemma 8.4, and

$$1728 n D^{n-1} \begin{pmatrix} \partial D \\ -U \end{pmatrix} = \begin{pmatrix} c_4^2 & -c_6 \\ -c_6 & c_4 \end{pmatrix} \begin{pmatrix} 3\partial c_4 \\ 2\partial c_6 \end{pmatrix}$$

which is a restatement of (5.5). □

The *dual Hesse polynomials* $\mathfrak{D}(\xi,\eta)$, $\mathfrak{c}_4(\xi,\eta)$, $\mathfrak{c}_6(\xi,\eta)$ are defined in terms of the Hesse polynomials $\mathbf{D}(\lambda,\mu)$, $\mathbf{c}_4(\lambda,\mu)$, $\mathbf{c}_6(\lambda,\mu)$ by

$$n=2 \qquad \begin{aligned} \mathbf{D}(\lambda,\mu) &= -(c_4^3 - c_6^2)\,\mathfrak{c}_6(\xi,\eta) \\ \mathbf{c}_4(\lambda,\mu) &= (c_4^3 - c_6^2)\,\mathfrak{c}_4(\xi,\eta) \\ \mathbf{c}_6(\lambda,\mu) &= (c_4^3 - c_6^2)^2\,\mathfrak{D}(\xi,\eta) \end{aligned}$$

$$n=3 \qquad \begin{aligned} \mathbf{D}(\lambda,\mu) &= -(c_4^3 - c_6^2)\,\mathfrak{c}_4(\xi,\eta) \\ \mathbf{c}_4(\lambda,\mu) &= -(c_4^3 - c_6^2)^2\,\mathfrak{D}(\xi,\eta) \\ \mathbf{c}_6(\lambda,\mu) &= -(c_4^3 - c_6^2)^2\,\mathfrak{c}_6(\xi,\eta) \end{aligned}$$

$$n=4 \qquad \begin{aligned} \mathbf{D}(\lambda,\mu) &= (c_4^3 - c_6^2)^2\,\mathfrak{D}(\xi,\eta) \\ \mathbf{c}_4(\lambda,\mu) &= (c_4^3 - c_6^2)^2\,\mathfrak{c}_4(\xi,\eta) \\ \mathbf{c}_6(\lambda,\mu) &= (c_4^3 - c_6^2)^3\,\mathfrak{c}_6(\xi,\eta) \end{aligned}$$

$$n=5 \qquad \begin{aligned} \mathbf{D}(\lambda,\mu) &= (c_4^3 - c_6^2)^3\,\mathfrak{D}(\xi,\eta) \\ \mathbf{c}_4(\lambda,\mu) &= (c_4^3 - c_6^2)^4\,\mathfrak{c}_4(\xi,\eta) \\ \mathbf{c}_6(\lambda,\mu) &= (c_4^3 - c_6^2)^6\,\mathfrak{c}_6(\xi,\eta) \end{aligned}$$

where $\lambda = c_6\xi + c_4^2\eta$ and $\mu = -c_4\xi - c_6\eta$. It follows by (8.1) that

$$\mathfrak{c}_4(\xi,\eta)^3 - \mathfrak{c}_6(\xi,\eta)^2 = (c_4^3 - c_6^2)^{n-1}\mathfrak{D}(\xi,\eta)^n.$$

Theorem 9.2. *There are identities*

$$\begin{aligned}\tau^2 c_4(\xi P + \eta Q) &= \mathfrak{c}_4(\xi,\eta)\\ \tau^3 c_6(\xi P + \eta Q) &= \mathfrak{c}_6(\xi,\eta)\\ \tau(\deg D) H(\xi P + \eta Q) &= -\tfrac{\partial \mathfrak{D}}{\partial \eta}(\xi,\eta) P + \tfrac{\partial \mathfrak{D}}{\partial \xi}(\xi,\eta) Q\\ \tau^2(\deg c_4) P(\xi P + \eta Q) &= f_4(\xi,\eta) U + g_4(\xi,\eta) H\\ \tau^3(\deg c_6) Q(\xi P + \eta Q) &= f_6(\xi,\eta) U + g_6(\xi,\eta) H\end{aligned}$$

where $\tau = 1, 2, 12, 12^4$ *for* $n = 2, 3, 4, 5$ *and*

$$\begin{pmatrix} f_4(\xi,\eta) & f_6(\xi,\eta) \\ g_4(\xi,\eta) & g_6(\xi,\eta)\end{pmatrix} = \begin{pmatrix} c_4 & c_6 \\ c_6 & c_4^2 \end{pmatrix}^{-1} \begin{pmatrix} \frac{\partial \mathfrak{c}_4}{\partial \xi}(\xi,\eta) & \frac{\partial \mathfrak{c}_6}{\partial \xi}(\xi,\eta) \\ \frac{\partial \mathfrak{c}_4}{\partial \eta}(\xi,\eta) & \frac{\partial \mathfrak{c}_6}{\partial \eta}(\xi,\eta)\end{pmatrix}.$$

Proof: Again it suffices to check these identities on the Hesse family. We did this by direct computation using MAGMA [23]. □

In the case $n = 2$, the Hesse polynomials and dual Hesse polynomials are the same. In MAGMA our function `HessePolynomials(n,r,[c4,c6])` returns the Hesse polynomials $\mathbf{D}, \mathbf{c}_4, \mathbf{c}_6$ if $r = 1$ and the dual Hesse polynomials $\mathfrak{D}, \mathfrak{c}_4, \mathfrak{c}_6$ if $r = -1$.

10. Formulae

In the cases $n = 2, 3, 4$ we give formulae for the Hessian H and for the contravariants P and Q. Theorem 6.7 then gives a practical method for computing the invariants. Alternatively we can compute the invariants using the formulae in [1] or [17, Section 7].

10.1. **Formulae in the case $n = 2$.** The binary quartic

$$f(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

has Hessian

$$\begin{aligned} H = (1/3) \times &\begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial z} \\ \frac{\partial^2 f}{\partial x \partial z} & \frac{\partial^2 f}{\partial z^2}\end{vmatrix} \\ = (8ac - 3b^2)&x^4 + (24ad - 4bc)x^3z + (48ae + 6bd - 4c^2)x^2z^2 \\ &+ (24be - 4cd)xz^3 + (8ce - 3d^2)z^4. \end{aligned}$$

and contravariants

$$\begin{aligned} P &= ex^4 - dx^3z + cx^2z^2 - bxz^3 + az^4 \\ Q &= (8ce - 3d^2)x^4 - (24be - 4cd)x^3z + (48ae + 6bd - 4c^2)x^2z^2 \\ &\quad - (24ad - 4bc)xz^3 + (8ac - 3b^2)z^4. \end{aligned}$$

The covariants and contravariants are closely related, the reason being that X_2 is isomorphic to its dual X_2^* as a $G_2 = \mathrm{SL}_2$-module.

10.2. **Formulae in the case $n = 3$.** The ternary cubic $U = U(x, y, z)$ has Hessian

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

The contravariant P, called in [27] the Caylean, is given by

$$P \;=\; (-1/xyz) \times \begin{vmatrix} \frac{\partial U}{\partial x}(0, z, -y) & \frac{\partial U}{\partial y}(0, z, -y) & \frac{\partial U}{\partial z}(0, z, -y) \\ \frac{\partial U}{\partial x}(-z, 0, x) & \frac{\partial U}{\partial y}(-z, 0, x) & \frac{\partial U}{\partial z}(-z, 0, x) \\ \frac{\partial U}{\partial x}(y, -x, 0) & \frac{\partial U}{\partial y}(y, -x, 0) & \frac{\partial U}{\partial z}(y, -x, 0) \end{vmatrix}.$$

The contravariant Q may be computed from the coefficient of $\lambda^2\mu$ in the first identity of Theorem 9.1, which in this case reads

$$P(\lambda U + \mu H) = (\lambda^3 + 3c_4\lambda\mu^2 + 4c_6\mu^3)P + 3(\lambda^2\mu - c_4\mu^3)Q.$$

10.3. **Formulae in the case $n = 4$.** We identify a genus one model of degree 4 with a pair of 4×4 symmetric matrices. Explicitly

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

where $q_1(x_1, \ldots, x_4) = \frac{1}{2}\mathbf{x}^T A\mathbf{x}$ and $q_2(x_1, \ldots, x_4) = \frac{1}{2}\mathbf{x}^T B\mathbf{x}$. In the classical literature, as surveyed in [1], the covariants and contravariants are SL_4-equivariant maps from X_4 to a space of quadrics. In this setting the invariants a, b, c, d, e, contravariants S_0, S_1, S_2, S_3 and covariants A, T_1, T_2, B are given by

$$\begin{aligned} \det(sA + tB) &= as^4 + bs^3t + cs^2t^2 + dst^3 + et^4 \\ \operatorname{adj}(sA + tB) &= S_0s^3 + S_1s^2t + S_2st^2 + S_3t^3 \\ \operatorname{adj}(s(\operatorname{adj} A) + t(\operatorname{adj} B)) &= a^2As^3 + aT_1s^2t + eT_2st^2 + e^2Bt^3. \end{aligned}$$

In terms of these, the Hessian is

$$H = \begin{pmatrix} 6T_2 - cA - 6bB \\ 6T_1 - cB - 6dA \end{pmatrix}$$

and the contravariants are

$$P = \begin{pmatrix} 6eS_0 - 3dS_1 + cS_2 - 3bS_3 \\ -3dS_0 + cS_1 - 3bS_2 + 6aS_3 \end{pmatrix}$$

and

$$Q = \begin{pmatrix} (12ce-18d^2)S_0 + (-18be+3cd)S_1 + (12ae+6bd-c^2)S_2 + (-18ad+3bc)S_3 \\ (-18be+3cd)S_0 + (12ae+6bd-c^2)S_1 + (-18ad+3bc)S_2 + (12ac-18b^2)S_3 \end{pmatrix}.$$

11. An evaluation algorithm

In the case $n = 5$ the invariants c_4 and c_6 are homogeneous polynomials of degrees 20 and 30 in 50 variables. They are therefore too large to compute as explicit polynomials. Nonetheless we have found a practical algorithm for evaluating them (see [17, Section 8]). The Hessian $H : X_5 \to X_5$ is a 50-tuple of homogeneous polynomials of degree 11 in 50 variables. Rather than attempt to compute these polynomials, we shall again give an evaluation algorithm.

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

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

where $v_1,\ldots,v_5$ and $x_1,\ldots,x_5$ are bases for V and W. The action of $\mathcal{G}_5 = \mathrm{GL}(V) \times \mathrm{GL}(W)$ is the natural one. The covariants and contravariants considered so far are the special cases $Y = X_5$ and $Y = X_5^*$ of the following more general definition.

Definition 11.1. Let (ρ, Y) be a rational representation of $\mathcal{G}_5$. A covariant is a polynomial map $F : \wedge^2 V \otimes W \to Y$ such that $F \circ g = \rho(g) \circ F$ for all $g \in G_5$.

The 4×4 Pfaffians of $\phi \in X_5$ are quadrics $p_1, \ldots, p_5$ satisfying

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

Let $v_1^*,\ldots,v_5^*$ be the basis for V^* dual to $v_1,\ldots,v_5$. We define covariants

$$\begin{array}{ll} P_2 : \wedge^2 V \otimes W \to V^* \otimes S^2 W\,; & \phi \mapsto \sum_{i=1}^5 v_i^* \otimes p_i(x_1,\ldots,x_5) \\ Q_6 : \wedge^2 V \otimes W \to S^2 V \otimes W; & \phi \mapsto \sum_{i=1}^5 q_i(v_1,\ldots,v_5) \otimes x_i. \\ R_{10} : \wedge^2 V \otimes W \to S^5 V^*; & \phi \mapsto \det(\sum_{k=1}^5 \frac{\partial^2 p_k}{\partial x_i \partial x_j} v_k^*) \\ S_{10} : \wedge^2 V \otimes W \to S^5 W\,; & \phi \mapsto \det(\frac{\partial p_i}{\partial x_j}) \end{array}$$

where the auxiliary quadrics q_i satisfy

$$\frac{\partial}{\partial x_i} S_{10}(\phi) = q_i(p_1,\ldots,p_5). \tag{11.1}$$

The proof that Q_6 exists, and is uniquely determined by (11.1), is given in [17, Section 8]. We write $\langle\ ,\ \rangle$ for the contraction

$$S^a V \times S^{a+b} V^* \to S^b V^*$$
$$(f(v_1,\ldots,v_5), g(v_1^*,\ldots,v_5^*)) \mapsto f(\tfrac{\partial}{\partial v_1^*},\ldots,\tfrac{\partial}{\partial v_5^*}) g(v_1^*,\ldots,v_5^*)$$

and identify $X_5 = \wedge^2 V \otimes W$ with the space of 10×5 matrices via

$$\sum_{i<j} v_i \wedge v_j \sum_k a_{ijk} x_k \equiv \begin{pmatrix} a_{121} & a_{122} & \cdots & a_{125} \\ a_{131} & a_{132} & \cdots & a_{135} \\ \vdots & \vdots & & \vdots \\ a_{451} & a_{452} & \cdots & a_{455} \end{pmatrix}.$$

Theorem 11.2. *The Hessian $H : X_5 \to X_5$ satisfies*

$$\begin{aligned} P_2 \circ H &= 4c_4 P_2 - \tfrac{3}{16} \langle Q_6, \langle Q_6, R_{10} \rangle \rangle \\ \det(U; H) &= 12^5 \Delta. \end{aligned}$$

These conditions uniquely determine $H(\phi)$ for $\phi \in X_5$ non-singular.

Proof: The covariance of these identities is clear, so it suffices to check them for ϕ a Hesse model. We did this by direct calculation. If $\phi \in X_5$ is non-singular then $H(\phi)$ is equivalent to a Hesse model, and therefore defines a curve. So for the final statement all we need to know is that if $\phi_1, \phi_2 \in X_5$ each define a curve and $P_2(\phi_1) = P_2(\phi_2)$ then $\phi_1 = \pm \phi_2$. This follows from the Buchsbaum-Eisenbud acyclicity criterion and the properties of minimal free resolutions. See for example [17, Section 5.2]. □

To compute the Hessian of a non-singular model $\phi \in X_5$ we begin by computing its invariants using the algorithm in [17, Section 8]. The auxiliary quadrics $q_1, \ldots, q_5$ are computed as a by-product of this algorithm. Then we use the first identity of Theorem 11.2 to compute the 4×4 Pfaffians of $H(\phi)$. The genus one model $H(\phi)$ is recovered from its 4×4 Pfaffians using the algorithm in [18]. This only determines $H(\phi)$ up to sign. In applications where the sign matters we use the second identity in Theorem 11.2 to make a consistent choice.

Remark 11.3. We have found similar algorithms for computing the contravariants (i.e. covariants for $Y = \wedge^2 V^* \otimes W^*$) and also the covariants for $Y = \wedge^2 W \otimes V^*$ and $Y = \wedge^2 W^* \otimes V$. We will report on these constructions and their arithmetic applications in [19]. (See also Remark 14.4.)

12. Theta groups

Let $C \to \mathbb{P}^{n-1}$ be a genus one normal curve defined over K. We recall that $E = \mathrm{Jac}(C)$ acts on C by translation, and translation by $P \in E$ extends to an automorphism of $\mathbb{P}^{n-1}$ if and only if $P \in E[n]$. Analogous to Definition 7.2 we have

Definition 12.1. The *theta group* of $C \to \mathbb{P}^{n-1}$ is the group of all matrices in GL_n that act on C as translation by some $T \in E[n]$. As a group it is a central extension of $E[n]$ by $\mathbb{G}_m$ with commutator given by the Weil pairing.

Let $T \mapsto M_T$ be a Galois equivariant section for $\Theta \to E[n]$. We consider the following pair of inverse problems.

(i) Given equations for $C \to \mathbb{P}^{n-1}$ how can we compute the matrices M_T for $T \in E[n]$?
(ii) Given the matrices M_T for $T \in E[n]$ how can we compute equations for $C \to \mathbb{P}^{n-1}$?

We restrict to $n = 2, 3, 4, 5$ and write $C = C_\phi$ where ϕ is a genus one model of degree n defined over K. The pencil of curves spanned by ϕ and its Hessian is a twist of the Hesse family. In particular there are $12/(6-n)$ singular fibres, and each of these is an n-gon. Generalising the terminology in [20, Section II.7] we call these the syzygetic n-gons. If we change co-ordinates so that one of the syzygetic n-gons has vertices $(1 : 0 : 0 : \ldots), (0 : 1 : 0 : \ldots), \ldots$ then the action of some $T \in E[n]$ is given by $M_T = \mathrm{Diag}(1, \zeta_n, \zeta_n^2, \ldots)$ where ζ_n is a primitive nth root of unity. Conversely the following theorem gives formulae for a syzygetic n-gon in terms of ζ_n and T.

Theorem 12.2. *Let ϕ be a non-singular genus one model of degree $n = 2, 3, 4, 5$ with invariants c_4 and c_6. Let $T = (x_T, y_T)$ be a torsion point of order n on the Jacobian $E : \ y^2 = x^3 - 27c_4x - 54c_6$. Then there is a syzygetic n-gon defined by $\psi = \xi_T\phi + 3H(\phi)$ and if $n \geq 3$ this model satisfies $H(\psi) = -(\frac{1}{3}\eta_T)^2\psi$ where*

$$\xi_T = \begin{cases} x_T & \text{if } n = 2, 3, 4 \\ (1 + \zeta_5 + \zeta_5^4)x_T + (1 + \zeta_5^2 + \zeta_5^3)x_{2T} & \text{if } n = 5 \end{cases}$$

and

$$\eta_T = \begin{cases} (\zeta_3 - \zeta_3^{-1})y_T & \text{if } n = 3 \\ (\zeta_4 - \zeta_4^{-1})(x_T - x_{2T})y_T & \text{if } n = 4 \\ (x_T - x_{2T})^4\big((\zeta_5 - \zeta_5^4)^5 y_T + (\zeta_5^2 - \zeta_5^3)^5 y_{2T}\big) & \text{if } n = 5. \end{cases}$$

Proof: The syzygetic n-gons are the fibres of the pencil $\lambda\phi + \mu H(\phi)$ where $(\lambda : \mu)$ is a root of Hesse polynomial $\mathbf{D}(\lambda, \mu) = 0$. A calculation using division polynomials shows that $\mathbf{D}(\xi_T, 3) = 0$. Then by Theorem 8.5 and a further calculation using division polynomials $H(\psi) = \frac{1}{3(\deg \mathbf{D})}\frac{\partial \mathbf{D}}{\partial \lambda}(\xi_T, 3)\psi = -(\frac{1}{3}\eta_T)^2\psi$. □

Remark 12.3. The syzygetic n-gon in Theorem 12.2 has field of definition $K(\xi_T)$, whereas an orientation of the n-gon is defined over $K(\xi_T, \eta_T)$. If $\zeta_n \in K$ then these fields are just $K(x_T)$ and $K(T) = K(x_T, y_T)$.

Theorem 12.2 is the basis for our method for computing the M_T, i.e. for solving problem (i). We have worked out explicit formulae in the cases $n = 2, 3, 4$. These are given in [11, Section 6.2], [15] and [16]. Applications include testing equivalence of genus one models, adding Selmer group elements (represented as explicit covering curves), and computing the inner product used for the reduction of genus one models. In the case $n = 5$ we have not yet found formulae for the M_T as explicit as the ones we gave for $n = 2, 3, 4$.

We now turn to problem (ii), i.e. we try to recover C from the M_T. This is required for the Hesse pencil method of n-descent as described in [9, Section 5.1]. See also the example of 5-descent in [10, Section 9.3].

We return to considering arbitrary $n \geq 2$. Generalising Definition 12.1 we have

Definition 12.4. A theta group for $E[n]$ is a central extension of $E[n]$ by $\mathbb{G}_m$ with commutator given by the Weil pairing.

The maps $\mathbb{G}_m \to \Theta$ and $\Theta \to E[n]$ are considered part of the data defining the theta group. Thus an isomorphism of theta groups is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, equal] & \Theta_1 \arrow[r] \arrow[d, "\cong"] & E[n] \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{G}_m \arrow[r] & \Theta_2 \arrow[r] & E[n] \arrow[r] & 0
\end{tikzcd}$$

If we ignore the Galois action (i.e. by passing to the algebraic closure $\overline{K}$), then there is only one such group. Its automorphism group is naturally a copy of $\text{Hom}(E[n], \mathbb{G}_m)$ which we identify with $E[n]$ via the Weil pairing. Let Θ_E be the base choice of theta group arising from the construction of Definition 12.1 for E embedded in $\mathbb{P}^{n-1}$ via the complete linear system $|n.0_E|$. Then as noted in [9, Section 1.6] the group $H^1(K, E[n])$ parametrises the theta groups for $E[n]$ (up to K-isomorphism) as twists of Θ_E.

Theorem 12.5. *Let $E[n] \to \text{GL}_n$; $T \mapsto M_T$ be a Galois equivariant map arising as a section of a theta group Θ for $E[n]$. Then*

- (i) *There is a genus one normal curve $C \to \mathbb{P}^{n-1}$ defined over K with Jacobian E and theta group Θ.*
- (ii) *If $n \geq 3$ then the genus one normal curves $C \subset \mathbb{P}^{n-1}$ for which each matrix M_T acts as translation by some n-torsion point of* Jac(C) *are parametrised by a twist of the modular curve $Y(n)$.*

Proof: See [9, Theorem 5.2 and Proposition 5.5]. □

Theorem 12.5(ii) is false in the case $n = 2$ since replacing a 2-covering $y^2 = g(x)$ by a quadratic twist $dy^2 = g(x)$ does not change the matrices M_T.

Again restricting to $n = 2, 3, 4, 5$ we explain how to compute the family of curves in Theorem 12.5(ii). In the cases $n = 2, 3$ we solve for the 2-dimensional Heisenberg invariant subspace of X_n. The case $n = 3$ is also described in [9, Lemma 5.6]. The cases $n = 4$, 5 are more complicated since we do not yet know the action of $E[n]$ on the space of equations defining $C \subset \mathbb{P}^{n-1}$.

Lemma 12.6. *If $n = 4$ then the space of quadrics $Q \in K[x_1, \ldots, x_4]$ satisfying $Q \circ M_T^2 = -(\det M_T)Q$ for all $T \in E[4] \setminus E[2]$ has dimension* 4.

Proof: We first note that the condition on the quadrics is independent of the scaling of the matrices M_T. Working over $\overline{K}$ we may assume that $E[4]$ is generated by T_1 and T_2 acting via

$$M_{T_1} = \begin{pmatrix} 1 & & & \\ & i & & \\ & & -1 & \\ & & & -i \end{pmatrix} \quad \text{and} \quad M_{T_2} = \begin{pmatrix} & & & 1 \\ 1 & & & \\ & 1 & & \\ & & 1 & \end{pmatrix}.$$

Then the space of quadrics in question has basis $x_1^2 + x_3^2$, x_1x_3, $x_2^2 + x_4^2$, x_2x_4. □

Let $H \cong H_4$ be the intersection of Θ with SL_4. Lemma 12.6 constructs a 4-dimensional representation of H, say V. Intersecting the H-invariant subspace of $\wedge^2 V$ with the image of $V \times V \to \wedge^2 V$; $(v_1, v_2) \mapsto v_1 \wedge v_2$ gives a conic $\Gamma \subset \mathbb{P}(\wedge^2 V)$. Each point on Γ corresponds to a 2-dimensional H-invariant space of quadrics. We have thus constructed the family of curves specified in Theorem 12.5(ii). Theorem 12.5(i) shows that $\Gamma(K) \neq \emptyset$ and hence $\Gamma \cong \mathbb{P}^1$.

In the case $n = 5$ we again let $H \cong H_5$ be the intersection of Θ with SL_5. The space of linear forms on $\mathbb{P}^4$ is a 5-dimensional representation of H, say W. If we ignore the Galois action then this is the unique irreducible representation of H with central character $\zeta \mapsto \zeta$. Again by inspection of the character table for H_5 there is a unique irreducible representation V of H with central character $\zeta \mapsto \zeta^2$. Since V is 5-dimensional the representations $\wedge^2 W$ and $S^2 W$ are isomorphic (over $\overline{K}$) to either 2 or 3 copies of V. We solve by linear algebra for a non-zero H-equivariant K-linear map $\pi : S^2 W \to \wedge^2 W$. Then either the kernel or image of π is a copy of V. The proof of Proposition 6.1 shows that the space $(\wedge^2 V \otimes W)^H$ is 2-dimensional. Since our construction of V from W is Galois equivariant, we can find a basis for this space defined over K. Identifying $\wedge^2 V \otimes W$ with the space of genus one models of degree 5 we have thus constructed the family of curves specified in Theorem 12.5(ii).

We return to considering the cases $n = 2, 3, 4, 5$. Let ϕ be a non-singular genus one model defining a curve in the family specified in Theorem 12.5(ii). By Theorem 8.2 we can recover the whole family by taking linear combinations of ϕ and its Hessian. Problem (ii), stated at the start of this section, is now reduced to

(iii) Given a non-singular genus one model $\phi \in X_n(K)$, find all models $\phi' = \lambda\phi + \mu H(\phi)$ with $(\lambda : \mu) \in \mathbb{P}^1(K)$ and $\mathrm{Jac}(C_{\phi'}) \cong E$.

Let c_4, c_6, Δ be the invariants of ϕ and $\mathbf{D}, \mathbf{c}_4, \mathbf{c}_6$ the Hesse polynomials, with coefficients evaluated at $c_4, c_6 \in K$. Then the fibres with the same j-invariant as E correspond to the roots $(\lambda : \mu) \in \mathbb{P}^1$ of the binary form

$$\mathbf{c}_4(\lambda, \mu)^3 - j(E)\, \Delta\, \mathbf{D}(\lambda, \mu)^n.$$

Solving for the K-rational roots of a polynomial of degree $12n/(6-n)$ we are left with only finitely many possibilities for ϕ' (up to quadratic twists in the case $n = 2$). We then use Theorem 2.4(iii) to decide which of these define a curve with Jacobian E.

As noted in [9, Section 5.1] it can happen that the family of curves in Theorem 12.5(ii) contains more than one curve defined over K with Jacobian E. However this does not happen in the generic case, i.e. when

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is surjective. In the event that more than one curve remains, we use our solution to problem (i) to determine which of these is correct.

13. The modular curves $X_E(n)$ and $X_E^-(n)$

Definition 13.1. Elliptic curves E and E' defined over K are *directly n-congruent* if there is an isomorphism of Galois modules $E[n] \cong E'[n]$ that respects the Weil pairing. They are *reverse n-congruent* if there is an isomorphism of Galois modules $\psi : E[n] \cong E'[n]$ satisfying $e_n(\psi S, \psi T) = e_n(S,T)^{-1}$ for all $S, T \in E[n]$.

The elliptic curves directly n-congruent to E are parametrised by $Y_E(n)$ and those reverse n-congruent to E by $Y_E^-(n)$. The smooth projective models $X_E(n)$ and $X_E^-(n)$ are twists of $X(n)$.

In the cases $n = 2, 3, 4, 5$ we have $X(n) \cong \mathbb{P}^1$. We show that the Hesse polynomials define the families of curves parametrised by $X_E(n) \cong \mathbb{P}^1$. Recall that in the case $n = 3$ the Hesse polynomials were already known to Salmon [27].

Theorem 13.2. *Let $n = 2, 3, 4, 5$. Let E be an elliptic curve over K,*

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

and let $E_{\lambda,\mu}$ be the family of curves

$$y^2 = x^3 - 27\mathbf{c}_4(\lambda,\mu)x - 54\mathbf{c}_6(\lambda,\mu)$$

where the coefficients of the Hesse polynomials $\mathbf{c}_4(\lambda,\mu)$ and $\mathbf{c}_6(\lambda,\mu)$ are evaluated at $c_4, c_6 \in K$. Then an elliptic curve E' over K is directly n-congruent to E if and only if it is isomorphic over K to $E_{\lambda,\mu}$ for some $\lambda, \mu \in K$.

Proof: Let $E \to \mathbb{P}^{n-1}$ be the genus one normal curve given by the complete linear system $|n.0_E|$. It is defined by some $\phi \in X_n(K)$ with invariants c_4 and c_6.
(i) Suppose that $\phi' = \lambda\phi + \mu H(\phi)$ is non-singular. By Theorem 8.2(i) the genus one normal curves $C_\phi \to \mathbb{P}^{n-1}$ and $C_{\phi'} \to \mathbb{P}^{n-1}$ have the same Heisenberg group. By Theorems 2.4(iii) and 8.5 their Jacobians are E and $E_{\lambda,\mu}$. It follows by Definition 7.2 that E and $E_{\lambda,\mu}$ are n-congruent.
(ii) By Theorem 12.5(i) there is a genus one normal curve $C' \to \mathbb{P}^{n-1}$ with Jacobian E' and the same Heisenberg group as $E \to \mathbb{P}^{n-1}$. Then Theorem 8.2(ii)

shows that $C' = C_{\phi'}$ for some $\phi' = \lambda\phi + \mu H(\phi)$. Since C' is defined over K we may arrange that $\lambda, \mu \in K$. Taking Jacobians gives $E' \cong E_{\lambda,\mu}$. □

If we split into the cases $c_4c_6 \neq 0$, $c_4 = 0$, $c_6 = 0$, then Theorem 13.2 reduces to formulae obtained by Rubin and Silverberg [25], [26], [28]. To explain the relationship in the case $c_4c_6 \neq 0$ we write

$$H_1 = \frac{-c_6^2 U + c_4c_6 H}{c_4^3 - c_6^2}.$$

Lemma 13.3. *There are polynomials $\alpha(J,t)$ and $\beta(J,t)$ such that*

$$\begin{aligned} c_4(U + tH_1) &= \mathbf{c}_4(1 - \tfrac{c_6^2}{c_4^3-c_6^2}t, \tfrac{c_4c_6}{c_4^3-c_6^2}t) = \alpha(J,t)c_4 \\ c_6(U + tH_1) &= \mathbf{c}_6(1 - \tfrac{c_6^2}{c_4^3-c_6^2}t, \tfrac{c_4c_6}{c_4^3-c_6^2}t) = \beta(J,t)c_6 \end{aligned}$$

where $J = c_4^3/(c_4^3 - c_6^2)$.

Proof: Theorem 8.5 gives the first two equalities. Then expanding $c_4(U+tH_1)/c_4$ and $c_6(U + tH_1)/c_6$ in powers of t we see that the coefficients are weight zero elements of $K[c_4, c_6, \Delta^{-1}]$ and therefore polynomials in J. □

Corollary 13.4. *Let $n = 3, 4, 5$. Let E be an elliptic curve over K,*

$$y^2 = x^3 + ax + b,$$

and let E_t be the family of curves

$$y^2 = x^3 + \alpha(J,t)ax + \beta(J,t)b$$

where $J = j(E)/1728 = 4a^3/(4a^3 + 27b^2)$.
(i) Every elliptic curve E_t over K with $t \in \mathbb{P}^1(K)$ is directly n-congruent to E.
(ii) If $j(E) \neq 0, 1728$ then every elliptic curve E' over K, that is directly n-congruent to E, is isomorphic over K to E_t for some $t \in \mathbb{P}^1(K)$.

Proof: This follows from Theorem 13.2 and Lemma 13.3. We assume $n = 3, 4, 5$ so that $E_{\lambda,\mu}$ is determined up to isomorphism by the ratio $(\lambda : \mu) \in \mathbb{P}^1(K)$. (This is false for $n = 2$.) The condition $j(E) \neq 0, 1728$ is required so that the matrix

$$\begin{pmatrix} 1 & \frac{-c_6^2}{c_4^3-c_6^2} \\ 0 & \frac{c_4c_6}{c_4^3-c_6^2} \end{pmatrix}$$

is non-singular. □

The polynomials $\alpha(J,t)$ and $\beta(J,t)$ for $n = 3, 5, 4, 2$ are written out in [25, Theorem 4.1 and Appendix], [28], [26]. They are also returned by our MAGMA function `RubinSilverbergPolynomials`.

Our proof of Theorem 13.2 only requires the existence of the Hessian, not the explicit formulae and algorithms in Sections 10 and 11. Alternatively the theorem can be proved (without using the Hessian) by adapting the method of Rubin and Silverberg. For this we replace the 2 by 2 matrix A used in [25] (which is singular for $j(E) = 0, 1728$ – hence the restriction in Corollary 13.4(ii)) by the matrix

$$\begin{pmatrix} a & -\frac{\partial D}{\partial b} \\ b & \frac{\partial D}{\partial a} \end{pmatrix}$$

used in Lemma 8.4.

The analogue of Theorem 13.2 for $X_E^-(n)$ is obtained by replacing the Hesse polynomials $\mathbf{c}_4(\lambda, \mu)$ and $\mathbf{c}_6(\lambda, \mu)$ by the dual Hesse polynomials $\tau^{-2}\mathfrak{c}_4(\xi, \eta)$ and $\tau^{-3}\mathfrak{c}_6(\xi, \eta)$. The proof uses the contravariants P and Q instead of the covariants U and H. To see why this works, recall that if M_T is a matrix describing the action of $T \in E[n]$ on $C \to \mathbb{P}^{n-1}$ then the Weil pairing is given by $e_n(S,T)I_n = M_S M_T M_S^{-1} M_T^{-1}$. Replacing each matrix M_T by its inverse transpose therefore has the effect of switching the sign of the Weil pairing.

If $n = 2$ or 5 then n-congruence and reverse n-congruence are the same (since -1 is a square mod n). The families parametrised by $X_E(n)$ and $X_E^-(n)$ are therefore isomorphic. If $n = 4$ then (by the formulae in Section 9) the only change is that we take the quadratic twist by the discriminant Δ. The analogue of Corollary 13.4 for reverse 3-congruence holds for the family of curves

$$y^2 = x^3 - 4\gamma(J,t)Jax - 8\beta(J,t)J^2 b$$

where $\gamma(J,t) = \mathbf{D}(1 - \frac{c_6^2}{c_4^3 - c_6^2}t, \frac{c_4 c_6}{c_4^3 - c_6^2}t)$. By (8.1) and Lemma 13.3 we may characterise $\gamma(J,t)$ as the unique polynomial in $\mathbb{Z}[J,t]$ satisfying $\gamma(J,t)^3 = \alpha(J,t)^3 J + \beta(J,t)^2(1-J)$.

14. Visibility of Tate-Shafarevich groups

In this section we recall the theory of visibility, introduced by Mazur [12], [24], and explain how we can use it to compute explicit elements of the Tate-Shafarevich group of an elliptic curve. We give some examples in Section 15.

We start with a short exact sequence of abelian varieties

$$0 \longrightarrow E \xrightarrow{\iota} A \xrightarrow{\psi} F' \longrightarrow 0$$

defined over a number field K. If $P \in F'(K)$ then restricting the group law on A gives the fibre $\psi^{-1}(P)$ the structure of torsor under E. It therefore represents an element of the Weil-Châtelet group $H^1(K,E)$. In fact this element is $\delta(P)$ where δ is the connecting map in the long exact sequence

$$\ldots \longrightarrow F'(K) \xrightarrow{\delta} H^1(K,E) \xrightarrow{\iota_*} H^1(K,A) \longrightarrow \ldots$$

Following Mazur we define $\xi \in H^1(K,E)$ to be *visible* in A if $\xi = \delta(P)$ for some $P \in F'(K)$, equivalently $\iota_*(\xi) = 0$.

Now let E and F be elliptic curves with a common finite Galois submodule Φ. We put $E' = E/\Phi$ and $F' = F/\Phi$. Then $A = (E \times F)/\Phi$ is an abelian surface and taking Galois cohomology of

$$\begin{tikzcd}
0 \arrow[r] & \Phi \arrow[r] \arrow[d] & F \arrow[r] \arrow[d] & F' \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & E \arrow[r] & A \arrow[r] & F' \arrow[r] & 0
\end{tikzcd}$$

gives the following commutative diagram whose rows are the Kummer exact sequences for $\phi_E : E \to E'$ and $\phi_F : F \to F'$.

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(K)}{\phi_E E(K)} \arrow[r] & H^1(K,\Phi) \arrow[r] \arrow[d, equal] & H^1(K,E)[\phi_E] \arrow[r] & 0 \\
0 \arrow[r] & \frac{F'(K)}{\phi_F F(K)} \arrow[r] \arrow[urr, "\delta"'] & H^1(K,\Phi) \arrow[r] & H^1(K,F)[\phi_F] \arrow[r] & 0
\end{tikzcd}$$

We are interested in the case $\Phi = E[n] = F[n]$ for some integer $n \geq 2$. In particular ϕ_E and ϕ_F are multiplication-by-n on $E = E'$ and $F = F'$.

In [9] we gave a list of geometric interpretations of the group $H^1(K, E[n])$. Two of these are relevant here. The first is that $H^1(K, E[n])$ parametrises the torsor divisor class pairs $(C, [D])$ as twists of $(E, [n.0_E])$. The second, already recalled in Section 12, is that $H^1(K, E[n])$ parametrises the theta groups for $E[n]$ as twists of Θ_E. If D is a K-rational divisor then $(C, [D])$ determines a morphism $C \to \mathbb{P}^{n-1}$ via the complete linear system $|D|$ and then a theta group by the construction of Definition 12.1. We checked in [9, Section 1.6] that this construction is compatible with the above two interpretations of $H^1(K, E[n])$.

Lemma 14.1. *If n is odd then Θ_E depends only on $E[n]$ (regarded as a Galois module equipped with the Weil pairing) and not on E.*

Proof: See [9, Lemma 3.11]. □

Our method for computing equations for visible elements of $Ш(E/K)[n]$ is as follows. First we find a second elliptic curve F/K that is directly n-congruent to E (see Definition 13.1). Then we convert $P \in F(K)$ to a torsor C under E by realising the map δ in the above diagram as the composite

$$\frac{F(K)}{nF(K)} \xrightarrow{\delta_F} H^1(K, F[n]) \cong H^1(K, E[n]) \xrightarrow{\iota_{E,*}} H^1(K, E)[n]. \tag{14.1}$$

We recall from [9, Remark 1.10] that, in terms of torsor divisor class pairs, the maps δ_F and $\iota_{E,*}$ are given by $P \mapsto (F, [(n-1).0_F + P])$ and $(C, [D]) \mapsto C$. In contrast we realise the middle isomorphism in (14.1) by using that $E[n]$ and $F[n]$ have the same theta groups (see Definition 12.4).

We make this construction explicit in the cases $n = 2, 3, 4, 5$. First we map $F \longrightarrow \mathbb{P}^{n-1}$ via the complete linear system $|(n-1).0_F + P|$, and let $\phi \in X_n(K)$ be a genus one model defining the image. Then we compute the Hessian $H(\phi)$ using the formulae and algorithms in Sections 10 and 11. Theorem 8.2 shows that the family of genus one normal curves with the same theta group as C_ϕ is defined by taking linear combinations of ϕ and $H(\phi)$. We therefore solve for all genus one models $\phi' = \lambda\phi + \mu H(\phi)$ with $(\lambda : \mu) \in \mathbb{P}^1(K)$ and $\mathrm{Jac}(C_{\phi'}) \cong E$. We know by Theorem 12.5(i) that there is always at least one such model. As explained at the end of Section 12 we can use the Hesse polynomials to solve for $(\lambda : \mu)$. Notice that if ϕ is chosen to have the same invariants as a fixed Weierstrass equation for F then we can use the same $(\lambda : \mu)$ for all $P \in F(K)$. Finally we check to see whether $C = C_{\phi'}$ is everywhere locally soluble. If so then it represents an element of $\text{Ш}(E/K)[n]$. We refer to [13] for some theoretical explanation as to why the torsors computed using visibility often turn out to be everywhere locally soluble.

The definition of visibility requires that the middle isomorphism in (14.1) is the natural one induced by the isomorphism $E[n] \cong F[n]$. However in the above construction we have identified $H^1(K, E[n])$ and $H^1(K, F[n])$ as parametrising the theta groups for $E[n] \cong F[n]$, first as twists of Θ_E and then as twists of Θ_F. So we are only using the natural isomorphism if $\Theta_E \cong \Theta_F$. Lemma 14.1 shows that this is always true for n odd, but it can fail if n is even. Nonetheless our construction defines an explicit map $F(K)/nF(K) \rightarrow H^1(K, E)[n]$, and even though it may differ by a shift from the one specified by Mazur, it seems in numerical examples to be just as good for constructing elements of $\text{Ш}(E/K)[n]$.

The method extends to pairs of elliptic curves E and F that are reverse n-congruent. Instead of taking linear combinations of ϕ and its Hessian, we take linear combinations of $P(\phi)$ and $Q(\phi)$ where P and Q are the contravariants. The role of the Hesse polynomials is then taken by the dual Hesse polynomials. If Θ is a theta group then we write $\Theta^\vee$ for the dual theta group obtained by replacing the map $\alpha : \mathbb{G}_m \rightarrow \Theta$ by $\lambda \mapsto \alpha(\lambda)^{-1}$. The analogue of Lemma 14.1 is

Lemma 14.2. *If n is odd and E and F are reverse n-congruent then $\Theta_E \cong \Theta_F^\vee$.*

Proof: The proof of Lemma 14.1 carries over immediately. □

Remark 14.3. Bruin and Dahmen [5] have used our construction for reverse 3-congruent elliptic curves to show that every element of $\text{Ш}(E/K)[3]$ is visible in the Jacobian of a genus 2 curve.

Remark 14.4. Since -1 is a square mod 5 there is no difference between direct and reverse 5-congruence. The case where $E[5]$ and $F[5]$ are isomorphic as Galois modules, but the isomorphism cannot be chosen to respect the Weil pairing, will be discussed further in [19]. Our solution in this case relies on algorithms for evaluating the covariants mentioned in Remark 11.3.

15. Examples

We illustrate the theory in Section 14 by computing equations for some visible elements of $\text{Ш}(E/\mathbb{Q})$. In each case we start with a pair of n-congruent elliptic curves $E/\mathbb{Q}$ and $F/\mathbb{Q}$ taken from the paper of Cremona and Mazur [12]. The Mordell Weil group $F(\mathbb{Q})$ is then used to "explain" certain elements in the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})$. As the method does not rely on the existence of rational isogenies we have deliberately chosen examples where $E/\mathbb{Q}$ is the only elliptic curve in its isogeny class.

Assuming a suitable elliptic curve $F/\mathbb{Q}$ is known, computing equations for elements of $\text{Ш}(E/\mathbb{Q})[n]$ using visibility is very much faster than doing an n-descent. This is especially true in the case $n = 5$ where the problem of computing class groups and units often makes 5-descent impractical.

In presenting these examples we use the algorithms for minimising and reducing genus one models of degrees $n = 2, 3, 4$ described in [11]. In other words we make changes of co-ordinates so that the models considered have small integer coefficients. We do not record the changes of co-ordinates used, as these may be recovered using the algorithms in [8], [15], [16], as implemented in our MAGMA function `IsEquivalent`. In the examples with $n > 2$ the models ϕ_i are the ones returned by our MAGMA function `GenusOneModel(n,P)`.

15.1. **An example of $\text{Ш}(E/\mathbb{Q})[2]$.** There is no distinction between direct and reverse 2-congruence. The formulae in Section 13 show that the elliptic curves

$$\begin{aligned} E = 571\text{a}1: &\quad y^2 + y = x^3 - x^2 - 929x - 10595 \\ F = 571\text{b}1: &\quad y^2 + y = x^3 + x^2 - 4x + 2 \end{aligned}$$

are 2-congruent. We have $E(\mathbb{Q}) = 0$ and $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (0, 1)$ and $P_2 = (1, 0)$. Mapping $F \to \mathbb{P}^1$ via the complete linear system $|0_F + P|$ for $P = 0_F, P_1, P_2, P_1 + P_2$ we obtain binary quartics

$$\begin{aligned} \phi_1 &= 4x^3z + 16x^2z^2 + 4xz^3 + z^4 \\ \phi_2 &= x^4 + 4x^3z + 4x^2z^2 - 12xz^3 + 4z^4 \\ \phi_3 &= x^4 + 4x^3z - 2x^2z^2 - 8xz^3 + 9z^4 \\ \phi_4 &= x^4 - 8x^3z + 10x^2z^2 + 4xz^3 + z^4 \end{aligned}$$

with invariants $c_4 = 3328$, $c_6 = -202240$ and $\Delta = -2^{12} \cdot 571$. Let $\mathbf{D}, \mathbf{c}_4, \mathbf{c}_6$ be the Hesse polynomials with coefficients evaluated at c_4, c_6. The binary form

$$\mathbf{c}_4(\lambda, \mu)^3 - j(E)\Delta\mathbf{D}(\lambda, \mu)^2 = 0$$

has a unique $\mathbb{Q}$-rational root at $(\lambda : \mu) = (-116 : 1)$. Solving for $d \in \mathbb{Q}^\times$ with $\mathbf{c}_4(-166, 1) = d^2c_4(E)$ and $\mathbf{c}_6(-166, 1) = d^3c_6(E)$ we find $d \in 3(\mathbb{Q}^\times)^2$. We therefore compute $3(-116\phi_i + H(\phi_i))$ for $i = 1, 2, 3, 4$ and then minimise and reduce to obtain

$$\begin{aligned}
\psi_1 &= -4x^4 - 60x^3z - 232x^2z^2 - 52xz^3 - 3z^4\\
\psi_2 &= -11x^4 - 68x^3z - 52x^2z^2 + 164xz^3 - 64z^4\\
\psi_3 &= -15x^4 - 52x^3z + 38x^2z^2 + 144xz^3 - 115z^4\\
\psi_4 &= -19x^4 + 112x^3z - 142x^2z^2 - 68xz^3 - 7z^4.
\end{aligned}$$

Each of these binary quartics ψ_i has discriminant $-2^{12} \cdot 571$, and defines a curve that is local solubility at $p = 2, 571$. Real solubility is automatic since the discriminant is negative. The binary quartic ψ_3 has a rational root at $(x : z) = (1 : 1)$. It follows that the ψ_i define a subgroup of $\text{Ш}(E/\mathbb{Q})[2]$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ with ψ_3 corresponding to the identity. The fact ϕ_1 represents the identity in $H^1(\mathbb{Q}, F[2])$ whereas ψ_3 represents the identity in $H^1(\mathbb{Q}, E[2])$ shows that in this example Θ_E and Θ_F are not isomorphic.

15.2. **Examples of $\text{Ш}(E/\mathbb{Q})[3]$.** We give two examples, one where the elliptic curves E and F are directly 3-congruent, and another where they are reverse 3-congruent. The formulae in Section 13 show that the elliptic curves

$$\begin{aligned}
E = 2006\text{e}1 :& \quad y^2 + xy = x^3 + x^2 - 58293654x - 171333232940\\
F = 2006\text{d}1 :& \quad y^2 + xy = x^3 + x^2 - 88x + 284
\end{aligned}$$

are directly 3-congruent. We have $E(\mathbb{Q}) = 0$ and $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (-10, 22)$ and $P_2 = (2, 10)$. Embedding $F \subset \mathbb{P}^2$ via the complete linear system $|2.0_F + P|$ for $P = P_1, P_2, P_1 + P_2, P_1 - P_2$ we obtain ternary cubics

$$\begin{aligned}
\phi_1 &= x^2y - 2x^2z + xy^2 - xyz - xz^2 - 2y^3 + y^2z + 5yz^2 + 2z^3\\
\phi_2 &= -x^2y - xy^2 - 5xyz + xz^2 + 2y^2z + 9yz^2 - z^3\\
\phi_3 &= -x^2y + 2xy^2 - 7xyz + xz^2 - y^2z + 6yz^2 - z^3\\
\phi_4 &= x^3 + 3x^2y + 2x^2z + xy^2 + xyz - 2xz^2 - y^3 + 2y^2z + yz^2 - 2z^3
\end{aligned}$$

with the same invariants $c_4 = 4249$, $c_6 = -277181$ and $\Delta = -2^2 \cdot 17^2 \cdot 59$ as F. Let $\mathbf{D}, \mathbf{c}_4, \mathbf{c}_6$ be the Hesse polynomials with coefficients evaluated at c_4, c_6. The binary form

$$\mathbf{c}_4(\lambda, \mu)^3 - j(E)\Delta\mathbf{D}(\lambda, \mu)^3 = 0$$

has a unique $\mathbb{Q}$-rational root at $(\lambda : \mu) = (521 : 9)$. We therefore compute $521\phi_i + 9H(\phi_i)$ for $i = 1, 2, 3, 4$ and then minimise and reduce to obtain

$$\begin{aligned}
\psi_1 &= 9x^3 - 16x^2y + 5x^2z + 38xy^2 + 129xyz + 6xz^2 + 59y^3 - 81y^2z - 58yz^2 - 124z^3\\
\psi_2 &= 9x^3 + 43x^2y - 27x^2z + 75xy^2 + 53xyz + 92xz^2 - 4y^3 + 75y^2z + 2yz^2 + 124z^3
\end{aligned}$$

$$\psi_3 = 9x^3 + 43x^2y - 27x^2z + 27xy^2 + 85xyz - 43xz^2 + 74y^3 + 74y^2z - 58yz^2 - 92z^3$$
$$\psi_4 = 43x^3 + 38x^2y + 22x^2z - 48xy^2 - 43xyz + 65xz^2 + 11y^3 - 5y^2z + 113yz^2 + 50z^3.$$

Each of these ternary cubics has the same invariants as E, and defines a curve that is locally soluble at $p = 2, 17, 59$ (the bad primes of E). It follows that the ψ_i define the inverse pairs of non-zero elements in a subgroup of $\text{Ш}(E/\mathbb{Q})[3]$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

Our second example is similar. The formulae in Section 13 show that the elliptic curves

$$\begin{aligned} E = 2541\text{d}1: &\quad y^2 + y = x^3 - x^2 - 180572x - 26845765 \\ F = 2541\text{c}1: &\quad y^2 + xy + y = x^3 + x^2 + 3x + 12 \end{aligned}$$

are reverse 3-congruent. We have $E(\mathbb{Q}) = 0$ and $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (-2, 2)$ and $P_2 = (0, 3)$. Embedding $F \subset \mathbb{P}^2$ via the complete linear system $|2.0_F + P|$ for $P = P_1, P_2, P_1 + P_2, P_1 - P_2$ we obtain ternary cubics

$$\begin{aligned} \phi_1 &= -x^2z + xy^2 - xyz + xz^2 + 2y^2z + yz^2 - 6z^3 \\ \phi_2 &= -x^2z + xy^2 + xyz + xz^2 - y^2z + 6yz^2 \\ \phi_3 &= -x^2y + xy^2 + xyz + 2xz^2 + 2y^2z - 3yz^2 + z^3 \\ \phi_4 &= -x^2y + xyz + xz^2 + y^3 + 2y^2z - 2yz^2 + 2z^3 \end{aligned}$$

with the same invariants $c_4 = -143$, $c_6 = -9449$ and $\Delta = -3^2 \cdot 7^2 \cdot 11^2$ as F. Let $\mathfrak{D}, \mathfrak{c}_4, \mathfrak{c}_6$ be the dual Hesse polynomials with coefficients evaluated at c_4, c_6. The binary form

$$\mathfrak{c}_4(\xi, \eta)^3 - 1728j(E)\Delta^2\mathfrak{D}(\xi, \eta)^3 = 0$$

has a unique $\mathbb{Q}$-rational root at $(\xi : \eta) = (-55 : 1)$. We therefore compute $-55P(\phi_i) + Q(\phi_i)$ for $i = 1, 2, 3, 4$ and then minimise and reduce to obtain

$$\begin{aligned} \psi_1 &= -x^3 - 3x^2y - 7x^2z - 14xy^2 + 8xyz + 13xz^2 - y^3 + 26y^2z + 2yz^2 + 70z^3 \\ \psi_2 &= -3x^3 - 14x^2y - 5x^2z - xy^2 + 4xyz - 15xz^2 - 5y^3 + 30y^2z - 16yz^2 - 26z^3 \\ \psi_3 &= 3x^3 + 7x^2y - 4x^2z + 3xy^2 + 28xyz + 25xz^2 - 9y^3 - 5y^2z + 6yz^2 + 35z^3 \\ \psi_4 &= x^3 + 7x^2y - 12x^2z + 9xy^2 + 10xyz + 37xz^2 - 4y^3 + 8y^2z + 2yz^2 + 35z^3. \end{aligned}$$

Each of these ternary cubics has the same invariants as E, and defines a curve that is locally soluble at $p = 3, 7, 11$ (the bad primes of E). It follows that the ψ_i define the inverse pairs of non-zero elements in a subgroup of $\text{Ш}(E/\mathbb{Q})[3]$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

15.3. **Examples of $\text{Ш}(E/\mathbb{Q})[4]$.** We give two examples, one where the elliptic curves E and F are directly 4-congruent, and another where they are reverse 4-congruent. The formulae in Section 13 show that the elliptic curves

$$\begin{aligned} E = 2045\text{b}1 : \quad & y^2 + xy = x^3 - x^2 - 5470x - 862675 \\ F = 4090\text{b}1 : \quad & y^2 + xy = x^3 + x^2 + 7x + 37 \end{aligned}$$

are directly 4-congruent. We have $E(\mathbb{Q}) = 0$ and $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (2, 7)$ and $P_2 = (18, 71)$. Embedding $F \subset \mathbb{P}^3$ via the complete linear system $|3.0_F + P|$ for $P = P_1, P_2, P_1 + P_2, P_1 + 2P_2, P_1 - P_2, 2P_1 + P_2$ we obtain quadric intersections

$$\phi_1 = \begin{pmatrix} x_1x_4 - x_2x_3 - x_2x_4 + x_3^2 - x_3x_4 + 2x_4^2 \\ x_1x_3 + x_1x_4 + x_2^2 - x_2x_3 + x_3^2 - 7x_3x_4 - 4x_4^2 \end{pmatrix}$$

$$\phi_2 = \begin{pmatrix} x_1x_3 + x_2^2 + x_2x_4 - x_3^2 - 2x_3x_4 - 2x_4^2 \\ x_1x_3 + x_1x_4 + x_2^2 - x_2x_3 + 3x_3^2 - x_3x_4 - 2x_4^2 \end{pmatrix}$$

$$\phi_3 = \begin{pmatrix} x_1x_4 - x_2x_3 + x_2x_4 + 3x_4^2 \\ x_1x_2 + x_1x_4 - 8x_2x_4 + x_3^2 + 4x_4^2 \end{pmatrix}$$

$$\phi_4 = \begin{pmatrix} x_1x_3 - x_2x_4 + x_3^2 - x_3x_4 + x_4^2 \\ x_1x_2 - x_1x_3 - 2x_2x_3 + x_2x_4 + 3x_4^2 \end{pmatrix}$$

$$\phi_5 = \begin{pmatrix} x_1x_2 + x_1x_4 - 2x_2x_3 + 2x_2x_4 + x_3^2 - 2x_4^2 \\ -x_1x_4 + 2x_2^2 + x_2x_3 + 3x_2x_4 + x_4^2 \end{pmatrix}$$

$$\phi_6 = \begin{pmatrix} x_1x_3 + x_2x_3 + 3x_2x_4 + x_3^2 + x_4^2 \\ x_1x_4 + x_2^2 - x_2x_3 - 3x_3x_4 - x_4^2 \end{pmatrix}$$

with the same invariants $c_4 = -311$, $c_6 = -29573$ and $\Delta = -2^8 \cdot 5 \cdot 409$ as F. Let $\mathbf{D}, \mathbf{c}_4, \mathbf{c}_6$ be the Hesse polynomials with coefficients evaluated at c_4, c_6. The binary form

$$\mathbf{c}_4(\lambda, \mu)^3 - j(E)\Delta\mathbf{D}(\lambda, \mu)^4 = 0$$

has a unique $\mathbb{Q}$-rational root at $(\lambda : \mu) = (5 : 1)$. We therefore compute $\phi_i' = 5\phi_i + H(\phi_i)$ for $i = 1, \ldots, 6$ and then minimise and reduce to obtain

$$\psi_1 = \begin{pmatrix} x_1x_2 + 2x_1x_4 - x_2x_3 - 4x_2x_4 + x_3^2 + x_3x_4 + x_4^2 \\ x_1^2 + 2x_1x_2 + x_1x_3 + 3x_1x_4 + 7x_2^2 - x_2x_3 + 2x_3^2 - 4x_3x_4 - 2x_4^2 \end{pmatrix}$$

$$\psi_2 = \begin{pmatrix} 2x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 - 2x_2x_4 + 3x_3^2 + 2x_3x_4 + 4x_4^2 \\ x_1^2 - x_1x_2 - x_2^2 - 5x_2x_3 + 4x_2x_4 - 2x_3^2 + x_3x_4 \end{pmatrix}$$

$$\psi_3 = \begin{pmatrix} x_1x_3 + 3x_1x_4 + x_2^2 - x_2x_3 + x_3^2 - 3x_3x_4 + x_4^2 \\ x_1^2 + 4x_1x_2 + 2x_1x_3 - 6x_1x_4 - x_2x_3 - 2x_2x_4 - 2x_3^2 - 2x_3x_4 + 2x_4^2 \end{pmatrix}$$

$$\psi_4 = \begin{pmatrix} 2x_1x_2 + 2x_1x_3 + x_1x_4 + x_2^2 + x_2x_3 + x_3^2 + x_3x_4 + 2x_4^2 \\ x_1^2 + x_1x_2 - 3x_1x_3 - 4x_1x_4 + 2x_2^2 + 3x_2x_4 + 3x_3^2 - 2x_3x_4 - x_4^2 \end{pmatrix}$$

$$\psi_5 = \begin{pmatrix} x_1^2 + x_1x_2 + x_1x_3 + x_1x_4 - x_2^2 - 2x_2x_3 + x_3^2 + x_3x_4 + 2x_4^2 \\ x_1^2 - 4x_1x_2 - 2x_2^2 - 4x_2x_3 + 5x_2x_4 - 3x_3^2 + 2x_3x_4 - x_4^2 \end{pmatrix}$$

$$\psi_6 = \begin{pmatrix} x_1x_2 + 3x_1x_3 + x_2^2 + x_2x_4 + x_3^2 - 2x_3x_4 + 5x_4^2 \\ x_1^2 - x_1x_2 - x_1x_3 + 7x_1x_4 + x_2x_3 + 3x_2x_4 + x_3^2 + 3x_3x_4 - x_4^2 \end{pmatrix}.$$

Each of these quadric intersections has the same invariants as E, and defines a curve that is locally soluble at $p = 5, 409$ (the bad primes of E). Solubility over the reals is automatic since the discriminant is negative. Repeating for $P = 0_F$ we obtain a quadric intersection equivalent to the one defining $E \subset \mathbb{P}^3$ embedded by $|4.0_E|$. So in this example Θ_E and Θ_F are isomorphic. It follows that the ψ_i define the inverse pairs of elements of order 4 in a subgroup of $Ш(E/\mathbb{Q})[4]$ isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$.

Our second example is similar. The formulae in Section 13 show that the elliptic curves

$$\begin{aligned} E = 1309\text{a1}: &\quad y^2 + y = x^3 - 406957x - 99924251 \\ F = 1309\text{b1}: &\quad y^2 + y = x^3 - x^2 - 22x + 52 \end{aligned}$$

are reverse 4-congruent. We have $E(\mathbb{Q}) = 0$ and $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (16, 59)$ and $P_2 = (-1, 8)$. Embedding $F \subset \mathbb{P}^3$ via the complete linear system $|3.0_F + P|$ for $P = P_1, P_2, P_1 + P_2, P_1 + 2P_2, P_1 - P_2, 2P_1 + P_2$ we obtain quadric intersections

$$\phi_1 = \begin{pmatrix} x_1x_3 + x_1x_4 + x_2x_4 - 2x_3x_4 + x_4^2 \\ x_1x_4 + x_2^2 + x_2x_3 - x_2x_4 - 2x_3^2 \end{pmatrix}$$

$$\phi_2 = \begin{pmatrix} x_1x_3 + x_2x_3 + x_2x_4 + 2x_3x_4 \\ x_1x_4 + x_2^2 - 3x_2x_4 + x_3^2 + x_3x_4 - 2x_4^2 \end{pmatrix}$$

$$\phi_3 = \begin{pmatrix} x_1x_3 + x_1x_4 - x_2x_4 + x_3^2 - x_3x_4 - 2x_4^2 \\ x_1x_3 + x_2^2 - x_2x_4 + 3x_3x_4 - 2x_4^2 \end{pmatrix}$$

$$\phi_4 = \begin{pmatrix} x_1x_2 + x_1x_3 + x_2^2 + x_2x_4 - x_3^2 - x_4^2 \\ x_1x_2 + x_2x_3 + x_2x_4 + 3x_3x_4 + x_4^2 \end{pmatrix}$$

$$\phi_5 = \begin{pmatrix} x_1x_4 + x_2x_3 + x_2x_4 - x_3x_4 + x_4^2 \\ x_1x_2 + 3x_2x_3 - 2x_2x_4 + x_3^2 + 3x_3x_4 + 2x_4^2 \end{pmatrix}$$

$$\phi_6 = \begin{pmatrix} x_1x_3 + x_2^2 - x_3^2 - x_3x_4 - x_4^2 \\ x_1x_2 + x_1x_3 + 2x_2x_3 - x_2x_4 + 2x_3x_4 + x_4^2 \end{pmatrix}$$

with the same invariants $c_4 = 1072$, $c_6 = -38744$ and $\Delta = -7^2 \cdot 11 \cdot 17^2$ as F. Let $\mathfrak{D}, \mathfrak{c}_4, \mathfrak{c}_6$ be the dual Hesse polynomials with coefficients evaluated at c_4, c_6. The binary form

$$\mathfrak{c}_4(\xi, \eta)^3 - 1728^2 j(E) \Delta^3 \mathfrak{D}(\xi, \eta)^4 = 0$$

has a unique $\mathbb{Q}$-rational root at $(\xi : \eta) = (35 : 1)$. We therefore compute $35P(\phi_i) + Q(\phi_i)$ for $i = 1, \ldots, 6$ and then minimise and reduce to obtain

$$\psi_1 = \begin{pmatrix} x_1^2 + 2x_1x_2 + 4x_1x_3 + x_1x_4 + 2x_2^2 + 7x_2x_3 + x_2x_4 + 2x_3^2 - 8x_3x_4 + 7x_4^2 \\ 2x_1x_2 + x_1x_3 + x_1x_4 + x_2^2 + 2x_2x_3 + 13x_3^2 - 2x_3x_4 + 4x_4^2 \end{pmatrix}$$

$$\psi_2 = \begin{pmatrix} x_1x_3 + x_1x_4 + x_2^2 - 4x_2x_3 - 4x_3^2 - 17x_3x_4 - 8x_4^2 \\ x_1^2 + x_1x_4 + x_2x_3 - 3x_2x_4 + x_3^2 - 4x_3x_4 + 20x_4^2 \end{pmatrix}$$

$$\psi_3 = \begin{pmatrix} x_1^2 + x_1x_3 + x_2^2 + x_2x_3 - x_2x_4 - x_3^2 - 4x_3x_4 + 3x_4^2 \\ 5x_1x_2 + 3x_1x_3 + 3x_1x_4 + 2x_2^2 + 2x_2x_3 + 4x_2x_4 - 7x_3^2 - 4x_3x_4 - 8x_4^2 \end{pmatrix}$$

$$\psi_4 = \begin{pmatrix} x_1^2 + x_1x_2 + 2x_1x_3 + 5x_1x_4 + x_2^2 + 3x_2x_3 + 6x_2x_4 + 2x_3^2 - 2x_3x_4 - 7x_4^2 \\ 2x_1^2 - 2x_1x_3 + 6x_1x_4 + 2x_2^2 + x_2x_3 + 7x_2x_4 + 2x_3^2 - 5x_3x_4 + 4x_4^2 \end{pmatrix}$$

$$\psi_5 = \begin{pmatrix} 4x_1x_2 + 4x_1x_3 + x_1x_4 - 6x_2x_3 - 4x_2x_4 + x_3^2 - 3x_3x_4 + x_4^2 \\ x_1^2 + x_1x_2 - x_1x_3 + 2x_1x_4 + 7x_2^2 - 5x_2x_3 - 4x_2x_4 + x_3^2 + x_3x_4 + 2x_4^2 \end{pmatrix}$$

$$\psi_6 = \begin{pmatrix} 3x_1x_3 + 6x_1x_4 + x_2^2 + x_3^2 - x_3x_4 + 9x_4^2 \\ x_1^2 + 3x_1x_2 - 6x_1x_3 - 10x_1x_4 + 2x_2x_3 + 3x_2x_4 - x_3^2 - 5x_3x_4 + 2x_4^2 \end{pmatrix}.$$

Each of these quadric intersections has the same invariants as E, and defines a curve that is locally soluble at $p = 7, 11, 17$ (the bad primes of E). Solubility over the reals is automatic since the discriminant is negative. Repeating for $P = 2P_2$

we obtain a quadric intersection equivalent to the one defining $E \subset \mathbb{P}^3$ embedded by $|4.0_E|$. So in this example the theta groups Θ_E and $\Theta_F^\vee$ differ by a 2-torsion element in $H^1(\mathbb{Q}, E[4]) \cong H^1(\mathbb{Q}, F[4])$. It follows that the ψ_i define the inverse pairs of elements of order 4 in a subgroup of $Ш(E/\mathbb{Q})[4]$ isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$.

15.4. **An example of $Ш(E/\mathbb{Q})[5]$.** The formulae in Section 13 show that the elliptic curves

$$\begin{aligned} E = 1058\text{d}1 : &\quad y^2 + xy = x^3 - x^2 - 332311x - 73733731 \\ F = 1058\text{c}1 : &\quad y^2 + xy + y = x^3 + 2 \end{aligned}$$

are directly 5-congruent. We have $E(\mathbb{Q}) = 0$ and $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (-1, 1)$ and $P_2 = (0, 1)$. Embedding $F \subset \mathbb{P}^4$ via the complete linear system $|4.0_F + P|$ for $P = P_1$, i.e.

$$(x, y) \mapsto (x^2 + 1 : -y - 1 : x : (y + 1)/(x + 1) : 1),$$

we obtain (using the algorithm in [18]) a genus one model

$$\phi_1 = \begin{pmatrix} 0 & -x_1 + x_3 - x_5 & x_4 & x_2 + x_4 & -x_4 \\ & 0 & x_2 + x_5 & -x_1 + x_5 & -x_3 \\ & & 0 & x_3 & x_5 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix}$$

with the same invariants $c_4 = -23$, $c_6 = -1909$ and $\Delta = -2^2 \cdot 23^2$ as F. Let $\mathbf{D}, \mathbf{c}_4, \mathbf{c}_6$ be the Hesse polynomials with coefficients evaluated at c_4, c_6. The binary form

$$\mathbf{c}_4(\lambda, \mu)^3 - j(E)\Delta\mathbf{D}(\lambda, \mu)^5 = 0$$

has a unique $\mathbb{Q}$-rational root at $(\lambda : \mu) = (-23 : 1)$. We compute the Hessian $H(\phi_1)$ using the algorithm in Section 11 and find it has entries

$$\begin{aligned} H_{12} &= x_1 - 61x_3 - 35x_5 & H_{24} &= x_1 - 12x_2 + 12x_3 + 47x_5 \\ H_{13} &= 12x_1 - 12x_2 + 36x_3 - 13x_4 - 60x_5 & H_{25} &= -12x_1 - 12x_2 + 25x_3 - 24x_4 - 36x_5 \\ H_{14} &= -x_2 - 12x_3 - 37x_4 - 12x_5 & H_{34} &= -24x_2 + 35x_3 - 24x_4 - 48x_5 \\ H_{15} &= 12x_2 - 12x_3 - 11x_4 + 12x_5 & H_{35} &= -12x_3 - x_5 \\ H_{23} &= 12x_1 + 23x_2 - 12x_3 + 72x_4 + 47x_5 & H_{45} &= -24x_2 + 12x_3 - 12x_5 \end{aligned}$$

Then we compute $\phi_1' = -23\phi_1 + H(\phi_1)$ and make a transformation of the form $[A, \lambda I_5] : \phi_1' \mapsto \lambda A \phi_1' A^T$ for some $\lambda \in \mathbb{Q}^\times$ and $A \in \mathrm{GL}_5(\mathbb{Q})$ to obtain

$$\psi_1 = \begin{pmatrix} 0 & -x_2 & x_5 & -x_2+x_3+x_5 & -x_4-2x_5 \\ & 0 & 2x_4 & -x_1-2x_5 & -x_3+2x_4-x_5 \\ & & 0 & -2x_3 & x_1+x_3+x_4 \\ & - & & 0 & -x_2+4x_3+4x_4-2x_5 \\ & & & & 0 \end{pmatrix}.$$

This genus one model has the same invariants as E, and its 4 by 4 Pfaffians define a curve $C \subset \mathbb{P}^4$ that is locally soluble at $p = 2, 23$ (the bad primes of E). It follows that C represents a non-trivial element of $\text{Ш}(E/\mathbb{Q})[5]$. We note that, unlike the examples in [14], the elliptic curve E does not admit any $\mathbb{Q}$-rational isogenies of degree 5. Repeating for $P = r_1P_1 + r_2P_2$ for $0 \le r_1, r_2 \le 4$ we find equations for all elements in a subgroup of $\text{Ш}(E/\mathbb{Q})[5]$ isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$. The full list of equations, together with similar examples for other elliptic curves $E/\mathbb{Q}$ of small conductor, may be found on the author's website.

References

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

[2] M. Artebani and I. Dolgachev, The Hesse pencil of plane cubic curves, *Enseign. Math.* (2) 55 (2009), no. 3-4, 235–273.

[3] W. Barth, K. Hulek and R. Moore, Shioda's modular surface $S(5)$ and the Horrocks-Mumford bundle, *Vector bundles on algebraic varieties* (Bombay, 1984), 35–106, Tata Inst. Fund. Res. Stud. Math., 11, Tata Inst. Fund. Res., Bombay, 1987.

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

[5] N. Bruin and S.R. Dahmen, Visualizing elements of Sha[3] in genus 2 Jacobians, in *Algorithmic number theory (ANTS-IX)*, G. Hanrot, F. Morain, E. Thomé (eds.), Lecture Notes in Comput. Sci. 6197, Springer, 2010, 110–125.

[6] D.A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3. *Amer. J. Math.* 99 (1977), no. 3, 447–485.

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

[8] J.E. Cremona and T.A. Fisher, On the equivalence of binary quartics, *J. Symbolic Comput.* 44 (2009), no. 6, 673–682.

[9] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, Explicit n-descent on elliptic curves, I. Algebra, *J. reine angew. Math.* 615 (2008), 121–155.

[10] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves, III Algorithms*, in preparation.

[11] J.E. Cremona, T.A. Fisher and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, *Algebra & Number Theory*, Vol. 4 (2010), No. 6, 763–820.

[12] J.E. Cremona and B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Experiment. Math.* 9 (2000), no. 1, 13–28.

[13] J.E. Cremona and B. Mazur, Appendix to: A. Agashe and W. Stein, Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero, *Math. Comp.* 74 (2005), no. 249, 455–484.

[14] T.A. Fisher, Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$, *J. Eur. Math. Soc.* 3 (2001) Issue 2, 169-201.

[15] T.A. Fisher, Testing equivalence of ternary cubics, in *Algorithmic number theory (ANTS-VII)*, F. Hess, S. Pauli, M. Pohst (eds.), Lecture Notes in Comput. Sci. 4076, Springer, 2006, 333-345.

[16] T.A. Fisher, Some improvements to 4-descent on an elliptic curve, in *Algorithmic number theory (ANTS-VIII)*, A.J. van der Poorten, A. Stein (eds.), Lecture Notes in Comput. Sci. 5011, Springer, 2008, 125–138.

[17] T.A. Fisher, The invariants of a genus one curve, *Proc. Lond. Math. Soc.* (3) 97 (2008) 753-782.

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

[19] T.A. Fisher, *Invariant theory for the elliptic normal quintic, I. Twists of* $X(5)$, in preparation.

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

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

[22] F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Dover Publications, Inc., New York, N.Y., 1956.

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

[24] B. Mazur, Visualizing elements of order three in the Shafarevich-Tate group, *Asian J. Math.* 3 (1999), no. 1, 221–232.

[25] K. Rubin and A. Silverberg, Families of elliptic curves with constant mod p representations, *Elliptic curves, modular forms, and Fermat's last theorem*, 148–161, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[26] K. Rubin and A. Silverberg, Mod 2 representations of elliptic curves, *Proc. Amer. Math. Soc.* 129 (2001), no. 1, 53–57.

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

[28] A. Silverberg, Explicit families of elliptic curves with prescribed mod N representations, *Modular forms and Fermat's last theorem*, 447–461, Springer, New York, 1997.

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

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

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