Hesse Pencils and 3-Torsion Structures

Ane S.I. ANEMA, Jaap TOP and Anne TUIJP

Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence,
University of Groningen, P.O. Box 407, 9700 AK Groningen, The Netherlands
E-mail: *a.s.i.anema@22gd7.nl*, *j.top@rug.nl*, *annetuijp@gmail.com*

Received May 08, 2018, in final form September 18, 2018; Published online September 21, 2018
https://doi.org/10.3842/SIGMA.2018.102

Abstract. This paper intends to focus on the universal property of this Hesse pencil and of its twists. The main goal is to do this as explicit and elementary as possible, and moreover to do it in such a way that it works in every characteristic different from three.

Key words: Hesse pencil; Galois representation; torsion points; elliptic curves

2010 Mathematics Subject Classification: 14D10; 14G99

1 Introduction

In a paper with Noriko Yui [14], explicit equations for all elliptic modular surfaces corresponding to genus zero torsion-free subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ were presented. Arguably the most famous and classical one of these surfaces is the Hesse pencil, usually described as the family of plane cubics

$$x^3 + y^3 + z^3 + 6txyz = 0$$

(see, e.g., [14, Table 2] and references given there). The current paper intends to focus on the universal property of this Hesse pencil and of its twists (see Theorem 1.1). The main goal is to do this as explicit and elementary as possible, and moreover to do it in such a way that it works in every characteristic different from three. We are not aware of any earlier publication of these results in the special case of characteristic two, so although admittedly not very difficult, those appear to be new. The first author of this paper worked on the present results as a (small) part of his Ph.D. Thesis [1] and the third author did the same as part of her Bachelor's Thesis [15]. Both were supervised by the second author.

Let k be a perfect field of characteristic different from three. Denote the absolute Galois group of k by G_k. Given an elliptic curve E defined over k, one obtains a Galois representation on the 3-torsion group $E[3]$ of E. This paper describes the family of all elliptic curves that have equivalent Galois representations on $E[3]$. Recall that elliptic curves E and E' over k yield equivalent Galois representations on their 3-torsion if and only if $E[3]$ and $E'[3]$ are isomorphic as G_k-modules. To be more specific, we demand that the equivalence is symplectic: a symplectic homomorphism $\phi\colon E[3] \to E'[3]$ is defined as in [10], as follows. If

$$e_3(S,T) = e'_3(\phi(S), \phi(T))$$

for all $S, T \in E[3]$ where e_3 and e'_3 are the Weil-pairings on the 3-torsion of E and E' respectively, then ϕ is called a *symplectic* homomorphism, otherwise ϕ is called an *anti-symplectic* homomorphism.

This paper is a contribution to the Special Issue on Modular Forms and String Theory in honor of Noriko Yui. The full collection is available at http://www.emis.de/journals/SIGMA/modular-forms.html

Next, recall the definition of the Hessian of a polynomial. Let $F \in k[X, Y, Z]$ be a homogeneous polynomial of degree n. The *Hessian* $\mathrm{Hess}\,(F)$ of F is the determinant of the Hessian matrix of F, that is

$$\mathrm{Hess}\,(F) = \det \begin{pmatrix} \dfrac{\partial^2 F}{\partial X^2} & \dfrac{\partial^2 F}{\partial X \partial Y} & \dfrac{\partial^2 F}{\partial X \partial Z} \\ \dfrac{\partial^2 F}{\partial X \partial Y} & \dfrac{\partial^2 F}{\partial Y^2} & \dfrac{\partial^2 F}{\partial Y \partial Z} \\ \dfrac{\partial^2 F}{\partial X \partial Z} & \dfrac{\partial^2 F}{\partial Y \partial Z} & \dfrac{\partial^2 F}{\partial Z^2} \end{pmatrix},$$

which is either a homogeneous polynomial of degree $3n - 6$ or zero.

Given a curve $C = Z(F)$ with $F \in k[X, Y, Z]$ homogeneous of degree three, the *Hesse pencil* of C is defined as

$$\mathcal{C} = Z(tF + \mathrm{Hess}\,(F))$$

over $k(t)$. Recall that the discrete valuations on $k(t)$ correspond to the points in $\mathbb{P}^1(k)$, where we usually write $(t_0 : 1)$ as t_0 and $(1 : 0)$ as ∞. We denote the reduced curve of $\mathcal{C}$ at $t_0 \in \mathbb{P}^1(k)$ by C_{t_0}. Notice that $C_\infty = C$ and for $t_0 \neq \infty$

$$C_{t_0} = Z(t_0 F + \mathrm{Hess}\,(F)).$$

In the special case that $C = E$ is an elliptic curve given by a Weierstrass equation, we have (see Section 2) that the point O at infinity is a point on E_{t_0} for every $t_0 \in \mathbb{P}^1(k)$. If E_{t_0} is a smooth curve, then this makes it an elliptic curve with unit element O.

In the case of characteristic two, the standard definition of the Hessian does not lead to a satisfactory theory. In Sections 9.2 and 9.3 a modified Hessian is introduced for this case; in fact this modification was already used by Dickson [5] in 1915. The goal of this paper is to provide an elementary proof of the following theorem:

Theorem 1.1. *If E and E' are elliptic curves over k, with E given by some Weierstrass equation over k, then there exists a symplectic isomorphism $E[3] \to E'[3]$ if and only if E' appears in the Hesse pencil of E, i.e., $E_{t_0} \cong_k E'$ for some $t_0 \in \mathbb{P}^1(k)$.*

We note that both Fisher's paper [6] and Kuwata's paper [10] discuss, apart from the result above (although not in characteristic two) also the case of anti-symplectic isomorphisms between the 3-torsion groups of elliptic curves.

In Sections 2, 3 and 4 we show that the 3-torsion groups of an elliptic curve in Weierstrass form and its Hesse pencil are identical not only as sets, but also have the same group structure and Weil-pairings. Using the Weierstrass form of the Hesse pencil computed in Section 5 and the relation between a linear change of coordinates and its restriction to the 3-torsion group described in Section 6, we prove in Section 7 essentially by a counting argument that an isomorphism of the 3-torsion groups respecting the Weil-pairings is the restriction of a linear change of coordinates. The proof of the theorem is completed in Section 8. After this, we adapt the argument in order to conclude the same result in characteristic 2 (where a slightly adapted notion of Hesse pencil is required). We compare our results with existing literature in Section 10.

2 The flex points

Let $C = Z(F)$ be a plane curve with $F \in k[X, Y, Z]$ homogeneous of degree n and irreducible. A point P on C is called a *flex point* if there exists a line L such that the intersection number of C and L at P is at least three. Notice that in our definition P is allowed to be a singular point on C.

The *Hessian curve* of C is defined as $\mathrm{Hess}\,(C) = Z(\mathrm{Hess}\,(F))$.

Proposition 2.1. *If P is a point on C and $\operatorname{char}(k) \nmid (n-1)$, then P is a flex point if and only if $P \in C \cap \operatorname{Hess}(C)$.*

Proof. See [8, Exercise 5.23]. ■

From now on we will only work with curves of degree three, so the proposition above is only usable for fields k of characteristic different from two. This is the reason for why we exclude characteristic two for now; see Section 9 for the excluded case.

Corollary 2.2. *If P is a flex point on C, then it is also a point on the Hesse pencil $\mathcal{C}$ and it is again a flex point of each curve of the Hesse pencil.*

This is a well-known and old result in the case of $F = X^3 + Y^3 + Z^3$, see for example [11, Section VII.1].

Proof. A computation using Magma [4] shows that

$$\operatorname{Hess}(tF + \operatorname{Hess}(F)) = \alpha F + \beta \operatorname{Hess}(F)$$

with $\alpha, \beta \in k[t]$.

Assume that P is a flex point, then $P \in C \cap \operatorname{Hess}(C)$ by Proposition 2.1, that is $F(P) = 0$ and $\operatorname{Hess}(F)(P) = 0$. So $(tF + \operatorname{Hess}(F))(P) = 0$, which implies that $P \in \mathcal{C}$. The computation above also implies that

$$\operatorname{Hess}(tF + \operatorname{Hess}(F))(P) = 0,$$

that is $P \in \operatorname{Hess}(\mathcal{C})$. Therefore $P \in \mathcal{C} \cap \operatorname{Hess}(\mathcal{C})$. Hence P is a flex point on $\mathcal{C}$ by Proposition 2.1. ■

Corollary 2.3. *Let $P \in C_{t_0} \cap C_{t_1}$. If $t_0 \neq t_1$, then P is a flex point on C.*

Proof. Suppose that $t_0 = (t_{00} : t_{01})$ and $t_1 = (t_{10} : t_{11})$, then

$$\begin{pmatrix} t_{00} & t_{01} \\ t_{10} & t_{11} \end{pmatrix} \begin{pmatrix} F(P) \\ \operatorname{Hess}(F)(P) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

with the matrix being invertible since $t_0 \neq t_1$. Thus $F(P) = 0$ and $\operatorname{Hess}(F)(P) = 0$, that is $P \in C \cap \operatorname{Hess}(C)$. Hence Proposition 2.1 implies that P is a flex point on C. ■

3 The 3-torsion group

Let $E = Z(F)$ be an elliptic curve with unit element O and $F \in k[X, Y, Z]$ homogeneous of degree 3. Recall the following well known fact.

Proposition 3.1. *Let S and T be points on E. If S is a flex point, then T is a flex point if and only if $S - T \in E[3]$.*

Proof. Let L_S and L_T be the tangent lines to E at S and T respectively. Assume that T is also a flex point. Consider the function $\frac{L_S}{L_T}$ on E which has divisor $3(S) - 3(T)$. From [13, Corollary III.3.5] it follows that $3S - 3T = O$. Hence $S - T \in E[3]$.

Assume that T is not a flex point. Now the divisor of the function $\frac{L_S}{L_T}$ is $3(S) - 2(T) - (T')$ with $T' \neq T$. From this it follows that $3S - 2T - T' = O$, thus $3S - 3T = T' - T \neq O$. Hence $S - T \notin E[3]$. ■

This result tells us that if O is a flex point on E, then the concepts of flex point and 3-torsion point coincide. In the previous section we learned that a flex point on E is also a flex point on $\mathcal{E} = \mathcal{Z}(tF + \mathrm{Hess}\,(F))$. Hence if we combine these statements, then we obtain $E[3] \subset \mathcal{E}[3]$. Since the characteristic of k is different from three, these sets are equal in size, thus the same. Moreover suppose that E_{t_0} for some $t_0 \in \mathbb{P}^1(k)$ is non-singular. Provide $\mathcal{E}$ and E_{t_0} with a group structure by taking O as the unit element. Since the flex points of $\mathcal{E}$ (considered as a plane cubic over $k(t)$) and of E_{t_0} (a cubic curve over k) are the same and a line that intersects an elliptic curve at two flex points will also intersect the curve at a third flex point, the group structures on $\mathcal{E}[3]$ and $E_{t_0}[3]$ are equal as well.

Recall that if the unit element O is a flex point on E, then we can find a projective linear transformation in $\mathrm{PGL}_3(k)$ such that E is given by a Weierstrass equation in the new coordinates. Moreover since the characteristic of k is different from two and three, we may even assume that $E\colon y^2 = x^3 + ax + b$ for some $a, b \in k$.

4 The Weil-pairing

In the previous section we saw that $\mathcal{E}[3] = E_{t_0}[3]$ for all $t_0 \in \mathbb{P}^1\left(\overline{k}\right)$ such that E_{t_0} is non-singular. Denote the Weil-pairing on the 3-torsion of $\mathcal{E}$ by e_3 and on the 3-torsion of E_{t_0} by $e_3^{t_0}$. An introduction to Weil-pairings can be found in [13, Section III.8] and [16, Sections 3.3 and 11.2].

Proposition 4.1. *Let E be an elliptic curve given by a Weierstrass equation and let $\mathcal{E}$ be its Hesse pencil. The Weil-pairings e_3 and $e_3^{t_0}$ on $E[3]$ are equal.*

Proof. Let $S, T \in E[3]$ generate $E[3]$. The Weil-pairing is determined by its value on (S, T). Follow [13, Exercise 3.16] to construct the Weil-pairings. Recall that O is a flex point on E.

Let L_O, L_S, L_T and L_{-T} be the tangent lines to $\mathcal{E}$ at O, S, T and $-T$ respectively. Define $D_S = (S) - (O)$ and $D_T = 2(T) - 2(-T)$. Notice that D_S and D_T have disjoint support. Since $2T - 2(-T) = T$ in $\mathcal{E}$, it follows that $D_T \sim (T) - (O)$. Consider the functions $f_S = \frac{L_S}{L_O}$ and $f_T = \left(\frac{L_T}{L_{-T}}\right)^2$, then $\mathrm{div}\,(f_S) = 3D_S$ and $\mathrm{div}\,(f_T) = 3D_T$. The Weil-pairing on $\mathcal{E}$ is defined as

$$e_3(S,T) = \frac{f_S(D_T)}{f_T(D_S)} = \left(\frac{f_S(T)}{f_S(-T)}\right)^2 \frac{f_T(O)}{f_T(S)} = \left(\frac{L_S(T)L_O(-T)L_T(O)L_{-T}(S)}{L_O(T)L_S(-T)L_{-T}(O)L_T(S)}\right)^2.$$

Let $s \in k(S,T)(t)$ be a local coordinate at t_0. Choose the equations of the tangent lines such that they are also defined over $k(S,T)[[s]]$ and are non-zero modulo s. Notice that L_O, L_S, L_T and L_{-T} modulo s are tangent lines to E_{t_0} at O, S, T and $-T$ respectively. Follow the construction above to obtain the Weil-pairing $e_3^{t_0}(S,T)$ on E_{t_0}.

Now $L_O(T)$ is a unit in $k(S,T)[[s]]$, because T is not contained in the tangent line L_O modulo s to E_{t_0} at O. Similarly the other terms in the expression of $e_3(S,T)$ are units as well. Thus by construction $e_3(S,T) \bmod s = e_3^{t_0}(S,T)$. Recall that $e_3(S,T)$ is a root of unity. Hence $e_3 = e_3^{t_0}$. ■

5 The Weierstrass form

Proposition 5.1. *Let E be an elliptic curve given by the Weierstrass equation $y^2z = x^3 + axz^2 + bz^3$ with $a, b \in k$. Then the Hesse pencil $\mathcal{E}$ can be given by*

$$ty^2z + 3xy^2 = tx^3 - 3ax^2z + (at - 9b)xz^2 + \left(bt + a^2\right)z^3$$

over $k(t)$. The linear change of coordinates

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix} \qquad \text{with} \qquad A = \begin{pmatrix} t & 0 & 3at^2 - 27bt - 9a^2 \\ 0 & 1 & 0 \\ -3 & 0 & t^3 + 9at - 27b \end{pmatrix}$$

transforms this into the Weierstrass form $\mathcal{E}^W : \eta^2\zeta = \xi^3 + a_t\xi\zeta^2 + b_t\zeta^3$, with

$$a_t = at^4 - 18bt^3 - 18a^2t^2 + 54abt - \bigl(27a^3 + 243b^2\bigr),$$
$$b_t = bt^6 + 4a^2t^5 - 45abt^4 + 270b^2t^3 + 135a^2bt^2 + \bigl(108a^4 + 486ab^2\bigr)t - \bigl(243a^3b + 1458b^3\bigr).$$

Moreover $\Delta\bigl(\mathcal{E}^W\bigr) = \Delta(E)(\det A)^3$ and $\det A = t^4 + 18at^2 - 108bt - 27a^2$.

Observe that the t in the proposition is equal to $8t$ in the previous sections.

Proof. The proof boils down to computing the map A, which can be found in three steps. First map the tangent line to $\mathcal{E}$ at O to the line at infinity. Next scale the z-coordinate so that the coefficient in front of x^3 and y^2z are equal up to minus sign. Finally shift the y – resp. the x-coordinate so that the xyz, yz^2 resp. the x^2z terms vanish. ■

This proposition shows that

$$j(\mathcal{E}) = 1728 \frac{4}{4a^3 + 27b^2} \left(\frac{at^4 - 18bt^3 - 18a^2t^2 + 54abt - \bigl(27a^3 + 243b^2\bigr)}{t^4 + 18at^2 - 108bt - 27a^2} \right)^3.$$

6 Linear change of coordinates I

Proposition 6.1. *Let $P_i \in \mathbb{P}^2(k)$ for $i = 1, \ldots, 4$ be points such that no three of them are collinear. If $Q_i \in \mathbb{P}^2(k)$ for $i = 1, \ldots, 4$ is another such set of points, then there exists a unique $A \in \mathrm{PGL}_3(k)$ such that $A(P_i) = Q_i$ for all $i = 1, \ldots, 4$.*

This is a well-known result which is easily proved using some elementary linear algebra. Observe that an analogous result holds for two sets of $n + 2$ points in $\mathbb{P}^n(k)$ such that no $n + 1$ of them lie on a hyperplane.

Proposition 6.2. *Let E be an elliptic curve given by a Weierstrass equation defined over k. If $E[3] = \langle S, T\rangle$, then any line in $\mathbb{P}^2\bigl(\overline{k}\bigr)$ contains at most two of the following points: O, S, T, $S + T$.*

Proof. Suppose that L is a line in $\mathbb{P}^2\bigl(\overline{k}\bigr)$ containing three of the points O, S, T and $S + T$. Denote these by P_1, P_2 and P_3. Since E is given by a Weierstrass equation, O is a flex point, thus $P_1 + P_2 + P_3 = O$. However this is impossible for the points mentioned above. Hence such a line L does not exist. ■

Suppose that we are given two elliptic curves E and E' as in the proposition above with $E[3] = \langle S, T\rangle$ and $E'[3] = \langle S', T'\rangle$, then Propositions 6.1 and 6.2 imply that there exists an $A \in \mathrm{PGL}_3\bigl(\overline{k}\bigr)$ such that $O \mapsto O'$, $S \mapsto S'$, $T \mapsto T'$ and $S + T \mapsto S' + T'$ and that this A is unique.

7 Linear change of coordinates II

Proposition 7.1. *Let E and E' be elliptic curves given by a Weierstrass equation defined over k. If $\phi\colon E[3] \to E'[3]$ is an isomorphism which respects the Weil-pairings, then there exists some $t_0 \in \mathbb{P}^1\big(\overline{k}\big)$ such that the fiber E_{t_0} of the Hesse pencil of E admits a linear change of coordinates $\Phi\colon E_{t_0} \to E'$ with $\Phi|_{E[3]} = \phi$.*

The essence of the proof of this proposition is the following: We determine the $t_i \in \mathbb{P}^1\big(\overline{k}\big)$ for which the j-invariant of E_{t_i} is equal to the j-invariant of E'. For each of these t_i's we obtain a number of linear changes of coordinates $E_{t_i} \to E$. A counting argument shows that ϕ is the restriction of one of those maps. The following observation is used in the counting argument:

Lemma 7.2. *Let E and E' be elliptic curves. Then 24 out of the 48 isomorphisms $E[3] \to E'[3]$ respect the Weil-pairings.*

Proof. Let $S, T \in E[3]$ be such that $E[3] = \langle S, T\rangle$ and $e_3(S,T) = \zeta_3$ with ζ_3 a fixed primitive third root of unity. Choose $S', T' \in E'[3]$ likewise. Since $E[3]$ and $E'[3]$ are two-dimensional vector spaces over $\mathbb{F}_3$, there exists a bijection

$$\begin{aligned} \mathrm{GL}_2(\mathbb{F}_3) &\longrightarrow \mathrm{Iso}\big(E[3], E'[3]\big), \\ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \phi_A(\alpha S + \beta T) = (\alpha a + \beta b)S' + (\alpha c + \beta d)T'. \end{aligned}$$

Notice that

$$e_3'(\phi_A(S), \phi_A(T)) = e_3'\big(aS' + bT', cS' + dT'\big) = e_3'\big(S', T'\big)^{ad-bc} = \zeta_3^{\det A}.$$

So ϕ_A respects the Weil-pairings if and only if $\det A = 1$, that is $A \in \mathrm{SL}_2(\mathbb{F}_3)$. Now $|\mathrm{GL}_2(\mathbb{F}_3)| = 48$ and $[\mathrm{GL}_2(\mathbb{F}_3)\colon \mathrm{SL}_2(\mathbb{F}_3)] = 2$. Hence there are 48 isomorphisms $E[3] \to E'[3]$ of which 24 respect the Weil-pairings. ■

Next we prove the proposition.

Proof of Proposition 7.1. Let j_0 and j_0' be the j-invariants of E and E' respectively. Denote the specialization of $\mathcal{E}^W$ at $t_0 \in \mathbb{P}^1\big(\overline{k}\big)$ by $E_{t_0}^W$. If $E_{t_0}^W$ is non-singular, then let $A_{t_0}\colon E_{t_0} \to E_{t_0}^W$ be the isomorphism induced by the linear change of coordinates A from Proposition 5.1 at t_0.

Assume that $j_0' \neq j_0, 0, 1728$ and take a_t as defined in Proposition 5.1. Consider the polynomial

$$G = -1728(4a_t)^3 - j_0'\Delta\big(\mathcal{E}^W\big) = \big(j_0 - j_0'\big)\Delta(E)\, t^{12} + 2^{13}3^6a^2bt^{11} + \cdots .$$

in $k[t]$, whose roots give $E_{t_0}^W$'s with j-invariant equal to j_0'. The polynomial G has degree 12 and its discriminant is

$$-3^{147}{j_0'}^8\big(j_0' - 1728\big)^6\Delta(E)^{44},$$

which is non-zero, so G has distinct roots $t_1, \ldots, t_{12}$ in $\overline{k}$. Since the j-invariant of $E_{t_i}^W$ is equal to j_0', there exists an isomorphism $\Psi_i\colon E_{t_i}^W \to E'$. An isomorphism respects the Weil-pairings, see [13, Proposition III.8.2] or [16, Theorem 3.9]. From Sections 3 and 4 it follows that $E_{t_i}[3] = E[3]$ as groups with identical Weil-pairings. Therefore for every $i = 1, \ldots, 12$ and $\sigma \in \mathrm{Aut}\,(E') \cong \mathbb{Z}/2\mathbb{Z}$

$$\phi_{i,\sigma} = (\sigma \circ \Psi_i \circ A_{t_i})|_{E_{t_i}[3]}\colon\ E[3] \to E'[3]$$

is an isomorphism respecting the Weil-pairings. Notice that $\sigma \circ \Psi_i \circ A_{t_i}$ is an element of $\mathrm{PGL}_3(\overline{k})$, because $E_{t_i}^W$ and E' are in Weierstrass form and A is a linear change of coordinates. All 24 isomorphisms $\phi_{i,\sigma}$ are distinct as the following argument shows. Suppose that $\phi_{i,\sigma} = \phi_{j,\tau}$, then $\sigma \circ \Psi_i \circ A_{t_i} = \tau \circ \Psi_j \circ A_{t_j}$ according to Section 6. Let $P \in E' \setminus E'[3]$, then $Q = (\sigma \circ \Psi_i \circ A_{t_i})^{-1}(P)$ is a point in $E_{t_i} \cap E_{t_j}$, so Corollary 2.3 implies that $t_i = t_j$, that is $i = j$. Since Ψ_i and A_{t_i} are isomorphisms, $\sigma = \tau$. Thus $\phi_{i,\sigma} = \phi_{j,\tau}$ if and only if $i = j$ and $\sigma = \tau$. Since the $\phi_{i,\sigma}$'s respect the Weil-pairings, Lemma 7.2 implies that these are all the possible isomorphisms $E[3] \to E'[3]$ that respect the Weil-pairings. Hence $\phi = \phi_{i,\sigma}$ for some $i = 1, \ldots, 12$ and $\sigma \in \mathrm{Aut}(E')$, which proves the proposition in this case.

Suppose that $j_0' = j_0$ and $j_0' \neq 0, 1728$, then the G above has degree 11 and the discriminant of G is

$$-2^{130}3^{195}a^{20}b^{10}\Delta(E)^{30},$$

which is again non-zero, so G has distinct roots $t_1, \ldots, t_{11}$ in $\overline{k}$. In this case the j-invariant of E_∞ is also equal to j_0', so let $t_{12} = \infty$. The argument presented before now finishes the proof in this case.

Assume that $j_0' = 0$. This case is the same as before with the exception of the polynomial G, which in this case should be replaced by a_t. The four distinct t_i's and the six elements in $\mathrm{Aut}(E')$ again give 24 isomorphisms $\phi_{i,\sigma}$.

Finally, if $j_0' = 1728$, then replace G by b_t (defined in Proposition 5.1) and proceed as before. ■

8 Proof of the theorem

In the proof of Theorem 1.1 we need a result from Galois cohomology, namely:

Lemma 8.1. *If k is a perfect field, then $\mathrm{PGL}_3(\overline{k})^{G_k} = \mathrm{PGL}_3(k)$.*

Proof. Consider the short exact sequence of G_k-groups

$$1 \longrightarrow \overline{k}^* \longrightarrow \mathrm{GL}_3(\overline{k}) \longrightarrow \mathrm{PGL}_3(\overline{k}) \longrightarrow 1,$$

which induces the exact sequence in the first row of the diagram

$$\begin{tikzcd}
1 \arrow[r] & \overline{k}^{*G_k} \arrow[r] & \mathrm{GL}_3(\overline{k})^{G_k} \arrow[r] & \mathrm{PGL}_3(\overline{k})^{G_k} \arrow[r] & \mathrm{H}^1(G_k, \overline{k}^*) \\
1 \arrow[r] & k^* \arrow[r] \arrow[u] & \mathrm{GL}_3(k) \arrow[r] \arrow[u] & \mathrm{PGL}_3(k) \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

The second row is the definition of $\mathrm{PGL}_3(k)$ and the vertical maps are the inclusion maps. Hilbert's Theorem 90 gives that $\mathrm{H}^1(G_k, \overline{k}^*) = \{1\}$. Since $\overline{k}^{*G_k} = k^*$ and $\mathrm{GL}_3(\overline{k})^{G_k} = \mathrm{GL}_3(k)$, also $\mathrm{PGL}_3(\overline{k})^{G_k} = \mathrm{PGL}_3(k)$. ■

Proof of Theorem 1.1. Assume that $\Phi \colon E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(k)$ is an isomorphism defined over k. This map respects the Weil-pairings according to [13, Proposition III.8.2]. So $\Phi|_{E_{t_0}[3]} \colon E_{t_0}[3] \to E'[3]$ is a symplectic isomorphism. In Sections 3 and 4 it was shown that $E[3] = E_{t_0}[3]$ as groups and have identical Weil-pairings. Thus $\Phi|_{E_{t_0}[3]}$ can be considered as a symplectic isomorphism $E[3] \to E'[3]$. Hence $\Phi|_{E_{t_0}[3]}$ is the desired map.

Suppose that there exists a symplectic isomorphism $\phi\colon E[3] \to E'[3]$, then Proposition 7.1 implies that there exists a $\Phi \in \mathrm{PGL}_3(\overline{k})$ and a $t_0 \in \mathbb{P}^1(\overline{k})$ such that $\Phi\colon E_{t_0} \to E'$ and $\phi = \Phi|_{E[3]}$. Since $\sigma \circ \phi = \phi \circ \sigma$ for all $\sigma \in G_k$,

$$\sigma(\Phi)(\sigma(S)) = \sigma \circ \Phi(S) = \sigma \circ \phi(S) = \phi \circ \sigma(S) = \Phi(\sigma(S))$$

for all $S \in E[3]$, so Propositions 6.1 and 6.2 imply that $\sigma(\Phi) = \Phi$. Therefore Lemma 8.1 implies that $\Phi \in \mathrm{PGL}_3(k)$. Hence $t_0 \in \mathbb{P}^1(k)$ and $E' \cong_k E_{t_0}$. ■

9 Characteristic two

So far we assumed k to be a perfect field of characteristic different from two and three. There is a natural idea how to adapt the proof of Theorem 1.1 to characteristic two: replace the explicitly given Hesse pencil by what it actually describes, namely the pencil of cubics with the nine points of order 3 on the initial elliptic curve as base points. This was done by one of us in her bachelor's project [15], and we briefly describe the results here.

9.1 Elliptic curves in characteristic two

Any elliptic curve E over a field of characteristic 2 can be given as follows, see [13, p. 409]:

$$\begin{aligned} &j(E) \neq 0\colon\ y^2 + xy = x^3 + a_2x^2 + a_6, && \Delta = a_6, && j(E) = 1/a_6,\\ &j(E) = 0\colon\ y^2 + a_3y = x^3 + a_4x + a_6, && \Delta = a_3^4, && j(E) = 0. \end{aligned}$$

If k is a field of characteristic 2, then the Hessian of any homogeneous polynomial $F \in k[X,Y,Z]$ of degree 3 equals zero, as is easily verified. We will show that given an elliptic curve E over k, say by a special equation as above, the curves in the pencil with base points $E[3]$ all have $E[3]$ as flex points, compare Corollary 2.2 for the classical situation. In [9], Glynn defines a Hessian for any curve $C = \mathcal{Z}(F)$ with $F \in k[X,Y,Z]$ homogeneous of degree 3 (characteristic two). In fact our construction coincides with his, although we put more emphasis on how it is obtained from considering 3-division polynomials. Note that the subject of flex points on cubic curves in characteristic two is in fact very classical: compare with, e.g., Dickson's paper [5] published in 1915.

9.2 The case $j(E) \neq 0$

We may and will assume that E is given by

$$y^2 + xy = x^3 + a_2x^2 + a_6, \qquad \Delta = a_6, \qquad j = 1/a_6.$$

Define $\mathrm{Hess}(E)$ as the plane curve defined by

$$y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0.$$

The Hesse pencil $\mathcal{E}$ in this case is given by

$$t\big(y^2 + xy + x^3 + a_2x^2 + a_6\big) + y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0.$$

In the next paragraphs, we will show that the Hessian and Hesse pencil have the desired properties. Firstly, the analog of Proposition 2.1 holds:

Proposition 9.1. *If P is a point on an elliptic curve E with equation $y^2 + xy = x^3 + a_2x^2 + a_6$, then P is a flex point of E if and only if $P \in E \cap \mathrm{Hess}(E)$.*

Proof. The point O is a flex point on both E and $\mathrm{Hess}(E)$ hence the result holds for O. Next take any other flex point of E, i.e., a point $P \neq O$ with $3P = O$. Put $P = (x, y)$. Note that $x \neq 0$, because any point $(0, y) \in E$ has order two. A small calculations (compare x-coordinates of $-P$ and $2P$) shows P is a flex point precisely when

$$\begin{aligned} &(E1) \quad 0 = x^2 + \left(\frac{y}{x}\right)^2 + \frac{y}{x} + a_2, \\ &(E2) \quad y + x = \left(x + \frac{y}{x} + 1\right)\left(x^2 + \left(\frac{y}{x}\right)^2 + x + \frac{y}{x} + a_2\right) + x^2. \end{aligned}$$

Using the equation defining E, one rewrites $(E1)$ as

$$0 = y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x. \tag{9.1}$$

The proposition now follows from a straightforward calculation. ■

Note that in fact $P = (x, y)$ is a flex point on E if and only if $P \in E$ satisfies equation (9.1). Now we show the analog of Corollary 2.2.

Proposition 9.2. *If P is a flex point on an elliptic curve E given by $y^2 + xy = x^3 + a_2x^2 + a_6$, then P is also a flex point on the Hesse pencil $\mathcal{E}$.*

Proof. It follows directly from the construction of $\mathcal{E}$ that P is indeed a point on it. To prove that P is also a flex point on $\mathcal{E}$, one shows that the tangent line to $\mathcal{E}$ at P intersects $\mathcal{E}$ at P with multiplicity 3. This is a straightforward calculation for which we refer to [15]. Clearly the point O is also a point on the Hesse pencil and it is also a flex point, as can be shown in the same way. ■

9.3 The case $j(E) = 0$

In the remaining case $j(E) = 0$ we may and will assume that E is given as

$$y^2 + a_3y = x^3 + a_4x + a_6, \qquad \Delta = a_3^4, \qquad j = 0.$$

Now define $\mathrm{Hess}(E)$ by

$$xy^2 + a_3xy + a_4x^2 + (a_3^2 + a_6)x + a_4^2 = 0,$$

so the Hesse pencil $\mathcal{E}$ becomes

$$t(y^2 + a_3y + x^3 + a_4x + a_6) + xy^2 + a_3xy + a_4x^2 + (a_3^2 + a_6)x + a_4^2 = 0.$$

In this case as well, the analogs of Proposition 2.1 and Corollary 2.2 hold:

Proposition 9.3. *If P is a point on the elliptic curve E given by $y^2 + a_3y = x^3 + a_4x + a_6$, then P is a flex point if and only if $P \in E \cap \mathrm{Hess}(E)$.*

Proof. For O the exact same argument holds as when $j(E) \neq 0$. A calculation shows that $P = (x, y) \in E$ is a flex point precisely when

$$a_3^2x = x^4 + a_4^2.$$

Using the equation of the elliptic curve this is rewritten as

$$0 = a_3^2x + x(y^2 + a_3y + a_4x + a_6) + a_4^2 = xy^2 + (a_3^2 + a_6)x + a_4x^2 + a_3xy + a_4^2. \quad ■$$

Proposition 9.4. *If P is a flex point on the elliptic curve E given by $y^2+a_3y=x^3+a_4x+a_6$, then it is also a flex point on the Hesse pencil $\mathcal{E}$.*

Proof. The reasoning is the same as for the case $j(E)\neq 0$. The straightforward calculation is presented in detail in [15]. ■

Using the properties shown above of our Hesse pencil in characteristic two, we can now almost completely follow the reasoning of the earlier sections since most arguments do not involve the characteristic of k. Only for the analog of Proposition 7.1 the proof needs to be adjusted in characteristic two, because here actual calculations are done with the Hesse pencil. We state it in the present situation.

Proposition 9.5. *Let E and E' be elliptic curves given by a Weierstrass equation defined over k. If $\phi\colon E[3]\to E'[3]$ is an isomorphism which respects the Weil-pairings, then there exists a linear change of coordinates $\Phi\colon E_{t_0}\to E'$ for some $t_0\in\mathbb{P}^1(\bar{k})$ such that $\Phi|_{E[3]}=\phi$.*

The remainder of this section consists of proving Proposition 9.5.

9.4 The case $j(E)\neq 0$

We first determine the Weierstrass form of the Hesse pencil in the present case.

Rewrite its equation (as introduced in Section 9.2) as

$$(t+1)y^2z+(t+1)xyz+xy^2+x^2y+(t+a_2)x^3+a_2(t+1)x^2z+a_6xz^2+ta_6z^3=0.$$

By a suitable change of coordinates this can be brought in Weierstrass form $\eta^2\zeta+b_1\xi\eta\zeta=\xi^3+b_2\xi^2\zeta+b_6\zeta^3$. This is quite analogous to what was sketched in the proof of Proposition 5.1; see [15] for a detailed description and [3] for a more general setup. The stated equation is found with

$$b_1=(t+1)^2,\qquad b_2=a_2(t+1)^4+a_6t(t+1),\qquad b_6=a_6(t^4+t^3+t^2+t+a_6)^3.$$

Denote this family of curves by $\mathcal{E}^W$ and let an individual curve in the pencil be denoted by E_t^W, then

$$j\big(E_t^W\big)=b_1^6/b_6=\frac{(t+1)^{12}}{a_6\big(t^4+t^3+t^2+t+a_6\big)^3}.$$

If $t=1$, the transformations needed to obtain the above Weierstrass form do not work. In this case one transforms the fiber of given pencil, so the curve E_1 with equation

$$xy^2+x^2y+(1+a_2)x^3+a_6xz^2+a_6z^3=0,$$

into the other Weierstrass form in characteristic 2:

$$\eta^2\zeta+b_3\eta\zeta^2=\xi^3+b_4\xi\zeta^2+b_6\zeta^3.$$

Explicitly, this results in the equation

$$\eta^2\zeta+a_6\eta\zeta^2+\xi^3+a_6^2\xi\zeta^2+a_6^2(1+a_2)\zeta^3=0.$$

In this way one obtains for every t a projective, linear transformation $E_t\to E_t^W$. Let us denote this transformation by A_t.

Proof of Proposition 9.5 for the case $j(E) \neq 0$. Given another elliptic curve E' with j-invariant j_0', we want to determine t for which our Hesse pencil has the same j-invariant. First, let us assume that j_0' is nonzero and not equal to j_0. Then

$$j_0' = j\bigl(E_t^W\bigr) \;\Leftrightarrow\; (t+1)^{12} = j_0' a_6 \bigl(t^4 + t^3 + t^2 + t + a_6\bigr)^3.$$

Define the polynomial

$$G = (t+1)^{12} + j_0' a_6 \bigl(t^4 + t^3 + t^2 + t + a_6\bigr)^3.$$

The zeros of this polynomial are precisely all t_0 such that $j\bigl(E_{t_0}^W\bigr) = j_0'$. The discriminant of G equals $a_6^{44} j_0'^{14}$, which is nonzero, because j_0' and a_6 are nonzero. We conclude that precisely 12 values $t_0 \in \bar{k}$ exist which give the desired j-invariant.

For every t_0, there is an isomorphism A_{t_0} between E_{t_0} and $E_{t_0}^W$, induced by the change of coordinates seen above. For every t_0 which is moreover a zero of G, there is an isomorphism Ψ_{t_0} between $E_{t_0}^W$ and E', because these curves have equal j-invariants. Lastly, there exist 2 automorphisms σ of E' [13, p. 410]. Taking the composition of these three isomorphisms and restricting to the 3-torsion group $E_{t_0}[3]$, which equals $E[3]$, we obtain $12 \times 2 = 24$ isomorphisms $\phi_{t_0,\sigma}$; they are described as

$$\phi_{t_0,\sigma} = \sigma \circ \Psi_{t_0} \circ A_{t_0}|_{E_{t_0}[3]} \colon\; E[3] \to E'[3].$$

These 24 isomorphisms are pairwise distinct and respect the Weil-pairing (see Section 7, observe that this argument is independent of the characteristic of k).

Now consider the case $j_0' = j_0 \neq 0$. Then $j_0' a_6 = 1$ since $j_0 = 1/a_6$. Our polynomial G therefore has degree 11 and discriminant $a_6^{30} \neq 0$. So this gives us 11 pairwise distinct $t \in \bar{k}$ such that $j\bigl(E_t^W\bigr) = j_0$. Another curve with this j-invariant is $E_\infty = E$. So again we find 12 distinct t's and in the same way as above, we find 24 isomorphisms respecting the Weil-pairing.

If $j_0' = 0$, the only t-value with $j(E_t) = 0$ is $t = 1$. Because E' has j-invariant zero and k has characteristic 2, its automorphism group has 24 elements [13, p. 410]. So again we find 24 isomorphisms respecting the Weil-pairing.

We now complete the proof of Proposition 9.5 for the case $j(E) \neq 0$ by the exact same argument as presented in the proof of Proposition 7.1. ■

9.5 The case $j(E) = 0$

For $j(E) = 0$ the calculations are slightly more involved. Bringing the Hesse pencil

$$t\bigl(y^2z + a_3yz^2 + x^3 + a_4xz^2 + a_6z^3\bigr) = xy^2 + a_3xyz + a_4x^2z + \bigl(a_3^2 + a_6\bigr)xz^2 + a_4^2z^3$$

in Weierstrass form, one obtains $\mathcal{E}^W$ of the form

$$\eta^2\zeta + \xi\eta\zeta + \xi^3 + b_2\xi^2\zeta + b_6\zeta^3 = 0$$

with b_2, b_6 explicit rational expressions in the a_j. The j-invariant of E_t^W for $t \neq 0$ is

$$j\bigl(E_t^W\bigr) = \frac{{a_3}^8}{\bigl(t^4 + a_3^2t + a_4^2\bigr)^3}.$$

If $t = 0$, so if $E_t = E_0$ is the Hessian curve, the transformations needed here are not valid. Therefore we treat this case separately. The Hessian here is given by

$$xy^2 + a_3xyz + a_4x^2z + \bigl(a_3^2 + a_6\bigr)xz^2 + a_4^2z^3 = 0.$$

This results in the Weierstrass equation

$$\eta^2\zeta + a_3^2\xi\eta\zeta + \xi^3 + \left(a_3^4 + a_6a_3^2\right)\xi^2\zeta + a_3^4a_4^6\zeta^3 = 0$$

with j-invariant $\frac{a_3^8}{a_4^6}$. We conclude that for every t including $t = 0$, the j-invariant of E_t^W is given by

$$j\left(E_t^W\right) = \frac{{a_3}^8}{\left(t^4 + a_3^2t + a_4^2\right)^3}.$$

Moreover, again we have a projective linear automorphism $A_t\colon E_t \to E_t^W$.

Proof of Proposition 9.5 if $j(E) = 0$. Again, we want to show that for every j_0', there exist 24 different isomorphisms. First, assume that $j_0' \neq 0$. Define

$$G := a_3^8 + j_0'\left(t^4 + a_3^2t + a_4^2\right)^3,$$

which has degree 12 and discriminant $a_3^{176}j_0'^{14} = \Delta(E)^{44}j_0'^{14}$. Therefore G has 12 pairwise distinct zeros, which are all solutions t_0 such that $j\left(E_{t_0}^W\right) = j_0'$. Again, together with the 2 automorphisms σ, we find 24 isomorphisms.

Now assume that $j_0' = 0$. In this case, the curve in the Hesse pencil we are looking for, is E itself: this curve has j-invariant zero. And again the automorphism group has order 24 so also in this case, we find 24 isomorphisms again, and the proof of Proposition 9.5 in this case is completed using the same reasoning as before (compare the proof of Proposition 7.1). ■

Using Proposition 9.5 one concludes that Theorem 1.1 holds in characteristic two as well, using the reasoning as presented in Section 8.

10 Comparison with the literature

Theorem 1.1 is part of a more general problem: Given an elliptic curve E over a field k and an integer n, describe the universal family of elliptic curves $\mathcal{E}$ such that for each member $\mathcal{E}_{t_0}$ the Galois representations on $E[n]$ and $\mathcal{E}_{t_0}[n]$ are isomorphic and the isomorphism is symplectic. For various n explicit families are known in the literature.

In [12] Rubin and Silverberg construct for any elliptic curve over $\mathbb{Q}$ such an explicit family for $n = 3$ and $n = 5$. Their proofs are motivated by the theory of modular curves. Our Theorem 1.1 corresponds roughly to [12, Theorem 4.1] and [12, Remark 4.2].

Using invariant theory and a generalization of the classical Hesse pencil, Fisher in [6] describes such families for elliptic curves defined over a perfect field of characteristic not dividing $6n$ with $n = 2, 3, 4, 5$. Theorem 1.1 is a special case of [6, Theorem 13.2]. It is unclear whether Fisher's proof of [6, Theorem 13.2] can be adapted to the case of characteristic two. In [7] Fisher moreover treats the cases $n = 7$ and $n = 11$.

The Hesse pencil is used by Kuwata in [10]. For any elliptic curve E over a number field he constructs two families of elliptic curves such that for each member the Galois representation on its 3-torsion is equivalent to the one on $E[3]$. In the first family the isomorphism of the 3-torsion groups is symplectic, whereas in the second family the isomorphism is anti-symplectic. The proofs use classical projective geometry and the classification of rational elliptic surfaces. Theorem 1.1 is essentially [10, Theorem 4.2] (although our proof is more detailed and totally elementary, and moreover we extend the result to characteristic two). Notice that the Weierstrass form of the Hesse pencil in [10, Remark 4.4] is the same as the one in Proposition 5.1 with t replaced by t^{-1} and the x and y coordinates scaled by some power of t.

An overview of results on the classical Hesse pencil is given by Artebani and Dolgachev in [2].

Acknowledgements

It is a pleasure to thank the referees of an earlier draft of this text. Their comments and suggestions were greatly appreciated. We also thank Matthias Schütt for helpful remarks.

References

[1] Anema A.S.I., The arithmetic of maximal curves, the Hesse pencil and the Mestre curve, Ph.D. Thesis, Rijksuniversiteit Groningen, 2016, available at http://hdl.handle.net/11370/0ef530b1-709b-4285-b68d-016a67e6e928.

[2] Artebani M., Dolgachev I., The Hesse pencil of plane cubic curves, *Enseign. Math.* **55** (2009), 235–273, math.AG/0611590.

[3] Artin M., Rodriguez-Villegas F., Tate J., On the Jacobians of plane cubics, *Adv. Math.* **198** (2005), 366–382.

[4] Bosma W., Cannon J., Playoust C., The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[5] Dickson L.E., Invariantive theory of plane cubic curves modulo 2, *Amer. J. Math.* **37** (1915), 107–116.

[6] Fisher T., The Hessian of a genus one curve, *Proc. Lond. Math. Soc.* **104** (2012), 613–648, math.NT/0610403.

[7] Fisher T., On families of 7- and 11-congruent elliptic curves, *LMS J. Comput. Math.* **17** (2014), 536–564.

[8] Fulton W., Algebraic curves. An introduction to algebraic geometry, 2008, available at http://www.math.lsa.umich.edu/~wfulton/.

[9] Glynn D.G., On cubic curves in projective planes of characteristic two, *Australas. J. Combin.* **17** (1998), 1–20.

[10] Kuwata M., Constructing families of elliptic curves with prescribed mod 3 representation via Hessian and Cayleyan curves, arXiv:1112.6317.

[11] Pascal E., Repertorium der höheren Mathematik: II. Teil: Die Geometrie, B.G. Teubner, Leipzig, 1902 (German translation of Repertorio di matematiche superiori (definizioni, formole, teoremi, cenni bibliografici), II. Geometria, Ulrico Hoepli, Milano, 1900).

[12] Rubin K., Silverberg A., Families of elliptic curves with constant mod p representations, in Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Hong Kong, 1993), *Ser. Number Theory, I*, Int. Press, Cambridge, MA, 1995, 148–161.

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

[14] Top J., Yui N., Explicit equations of some elliptic modular surfaces, *Rocky Mountain J. Math.* **37** (2007), 663–687, math.AG/0307230.

[15] Tuijp A., Hesse pencil in characteristic two, Bachelor's Thesis, Rijksuniversiteit Groningen, 2015, available at http://fse.studenttheses.ub.rug.nl/id/eprint/13074.

[16] Washington L.C., Elliptic curves. Number theory and cryptography, 2nd ed., *Discrete Mathematics and its Applications*, Chapman & Hall/CRC, Boca Raton, FL, 2008.