London Mathematical Society ISSN 1461–1570

ARITHMETIC E_8 LATTICES WITH MAXIMAL GALOIS ACTION

ANTHONY VÁRILLY-ALVARADO AND DAVID ZYWINA

Abstract

We construct explicit examples of E_8 lattices occurring in arithmetic for which the natural Galois action is equal to the full group of automorphisms of the lattice, i.e., the Weyl group of E_8. In particular, we give explicit elliptic curves over $\mathbb{Q}(t)$ whose Mordell–Weil lattices are isomorphic to E_8 and have maximal Galois action.

Our main objects of study are del Pezzo surfaces of degree 1 over number fields. The geometric Picard group, considered as a lattice via the negative of the intersection pairing, contains a sublattice isomorphic to E_8. We construct examples of such surfaces for which the action of Galois on the geometric Picard group is maximal.

1. *Introduction*

In this paper we construct explicit examples of E_8 lattices coming from arithmetic for which the Galois action is as large as possible. Recall that a *lattice* is a free abelian group equipped with a $\mathbb{Z}$-valued non-degenerate symmetric bilinear form. The E_8 lattice is the unique, positive definite, even, unimodular lattice of rank 8. As the notation suggests, it is also the root lattice of the E_8 root system (which is the largest exceptional root system). The *Weyl group* of E_8, denoted $W(E_8)$, is the group of automorphisms of the E_8 lattice; it is a finite group of order 696,729,600.

Suppose that E is a non-isotrivial elliptic curve over $\mathbb{Q}(t)$. Then the group $E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ is free abelian of finite rank and has a natural pairing called the *canonical height pairing* (see [**20**, Theorem III.4.3]). The group $E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ equipped with this pairing is a lattice, called the *Mordell–Weil lattice* of E. The natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ preserves the lattice structure.

Let us now give an example of an E_8 lattice occurring in arithmetic.

THEOREM 1.1. *Let $a(t), b(t), c(t) \in \mathbb{Z}[t]$ be polynomials of degrees at most 2, 4, and 6, respectively, which satisfy the following congruences:*

$$\begin{aligned} a(t) &\equiv 70t \pmod{105},\\ b(t) &\equiv 84t^4 + 7t^3 + 98t^2 + 84t + 98 \pmod{105},\\ c(t) &\equiv 65t^6 + 42t^5 + 21t^4 + 77t^3 + 63t^2 + 56t + 30 \pmod{105}. \end{aligned}$$

Let E be the elliptic curve over $\mathbb{Q}(t)$ given by the Weierstrass model

$$y^2 = x^3 + a(t)x^2 + b(t)x + c(t). \tag{1.1}$$

Received 15 July 2008, revised 7 January 2009; *published* 5 November 2009.
2000 Mathematics Subject Classification 14J26 (primary); 11H56, 11G05 (secondary).

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

Then the group $E(\overline{\mathbb{Q}}(t))$ is free of rank 8 and as a Mordell–Weil lattice it is isomorphic to the E_8 lattice. The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\overline{\mathbb{Q}}(t))$ as the full group $W(E_8)$.

Remark 1.2.

(i) Mordell–Weil lattices of type E_8 have been extensively studied by Shioda (see [**18, 19**]). In fact, Shioda [**18**, Theorem 7.2] has shown that *every* Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $W(E_8)$ arises from the Mordell–Weil lattice of an elliptic curve $E/\mathbb{Q}(t)$. Theorem 1.1 thus gives explicit examples of this theory.

(ii) If the Mordell–Weil lattice of $E/\mathbb{Q}(t)$ is isomorphic to the E_8 lattice, then the 240 roots of the lattice are $\overline{\mathbb{Q}}(t)$-rational points of the form

$$x = a_2t^2 + a_1t + a_0 \qquad y = b_3t^3 + b_2t^2 + b_1t + b_0, \tag{1.2}$$

where $a_i, b_j \in \overline{\mathbb{Q}}$ for all i and j. Conversely, any $\overline{\mathbb{Q}}(t)$-point of this form is a root of the lattice; see [**17**, §10]. The field extension of $\mathbb{Q}$ obtained by adjoining all the coefficients a_i and b_j is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to a subgroup of $W(E_8)$.

Theorem 1.1 can thus be used, in principle, to write down explicit Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to $W(E_8)$: first substitute the expressions of (1.2) into (1.1). We then obtain a polynomial in the variable t, which is identically zero if $(x, y) \in E(\overline{\mathbb{Q}}(t))$. This will give a series of relations among the a_i and b_j. We can then use elimination theory to distill these relations to a single polynomial in, say, the variable a_1. The Galois group of the splitting field of this polynomial will be isomorphic to $W(E_8)$. The polynomial we obtained by this method is too large to be included here.

Another method for obtaining a polynomial whose splitting field has Galois group isomorphic to $W(E_8)$ can be found in [**13**]. This approach uses an algebraic group of E_8 type.

1.1. *Del Pezzo Surfaces*

A *del Pezzo surface X of degree* 1 over a number field k is a surface over k that when base extended to an algebraic closure $\overline{k}$ of k is isomorphic to $\mathbb{P}^2_{\overline{k}}$ blown up at 8 points in general position.

An E_8 lattice naturally arises from a del Pezzo surface X of degree 1 as follows. Let $X_{\overline{k}} = X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, \overline{k}$. The intersection pairing on $\mathrm{Pic}(X_{\overline{k}}) \cong \mathbb{Z}^9$ gives this group a lattice structure. Let $K_X^{\perp}$ denote the orthogonal complement in $\mathrm{Pic}(X_{\overline{k}})$ of the canonical class K_X with respect to the intersection pairing. We give $K_X^{\perp}$ a lattice structure by endowing it with the form that is the negative of the intersection pairing. As a lattice, $K_X^{\perp}$ is isomorphic to the E_8 lattice. We denote by $\mathrm{O}(K_X^{\perp})$ the group of lattice automorphisms of $K_X^{\perp}$. It is thus isomorphic to $W(E_8)$.

There is a natural action of $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Pic}(X_{\overline{k}})$ that respects the intersection pairing and fixes K_X. We thus obtain a Galois representation

$$\phi_X\colon\ \mathrm{Gal}(\overline{k}/k) \to \mathrm{O}(K_X^{\perp}).$$

We will construct explicit examples of X such that ϕ_X is surjective, that is, such that the action of Galois on $K_X^{\perp}$ is maximal. Ekedahl [**9**] and Erné [**10**] have made the analogous constructions for del Pezzo surfaces of degree 3 and 2, respectively (for the

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

general definition of del Pezzo surfaces, see §2). The reader will see their influence here. In [**18**], Shioda also constructs explicit examples for del Pezzo surfaces of degrees 2 and 3, using the theory of Mordell–Weil lattices.

We can now state our main result.

THEOREM 1.3. *Let f be a sextic polynomial in the weighted graded ring $\mathbb{Z}[x, y, z, w]$, where the variables x, y, z, w have weights $1, 1, 2, 3$ respectively, such that*

$$f \equiv 40x^6 + 63x^5y + 84x^4y^2 + 28x^3y^3 + 42x^2y^4 + 49xy^5 + 75y^6 + 84x^4z + 7x^3yz + 98x^2y^2z + 84xy^3z + 98y^4z + 35xyz^2 + z^3 + w^2 \pmod{105}. \tag{1.3}$$

Then $X := \operatorname{Proj}(\mathbb{Q}[x, y, z, w]/(f))$ is a del Pezzo surface of degree 1 over $\mathbb{Q}$ and the homomorphism

$$\phi_X \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{O}(K_X^{\perp})$$

is surjective. Equivalently, if L_X is the fixed field of $\ker(\phi_X)$ in $\overline{\mathbb{Q}}$, then

$$\operatorname{Gal}(L_X/\mathbb{Q}) \cong W(E_8).$$

Letting the polynomials f that satisfy (1.3) vary, the corresponding fields L_X give infinitely many linearly disjoint extensions of $\mathbb{Q}$ with Galois group isomorphic to $W(E_8)$.

Remark 1.4.

(i) Suppose that k is a finitely generated extension of $\mathbb{Q}$. By Theorem 1.3, there is a del Pezzo surface $X/\mathbb{Q}$ of degree 1 such that $\operatorname{Gal}(L_X/\mathbb{Q}) \cong W(E_8)$, and such that k and L_X contain no isomorphic subfields except $\mathbb{Q}$ (the proof of Theorem 1.3 will give a constructive way to find such an X). Therefore X_k is a del Pezzo surface of degree 1 over k, and the homomorphism $\phi_{X_k} \colon \operatorname{Gal}(\overline{k}/k) \to \mathrm{O}(K_{X_k}^{\perp})$ is surjective.

(ii) The finite subgroups of $\mathrm{GL}_8(\mathbb{Q})$ with maximal cardinality are isomorphic to $W(E_8)$ (this depends on unpublished results in group theory, see [**1**]). Thus our examples have maximal Galois action amongst all rank 8 lattices.

1.2. *Genus 4 curves*

We shall now describe certain genus 4 curves that arise from del Pezzo surfaces of degree 1. These curves have been studied by Zarhin, and our examples complement his. For details, see [**21**].

Let X be a del Pezzo surface of degree 1 over a field k of characteristic 0. The surface X has a distinguished involution called the *Bertini involution*; it is the unique automorphism of X which induces an action of $-I$ on $K_X^{\perp} \subseteq \operatorname{Pic}(X_{\overline{k}})$. The fixed locus of the Bertini involution consists of a curve C and a rational point. The curve C is smooth, irreducible, non-hyperelliptic, and has genus 4.

Let $J(C)$ be the Jacobian of C, and let $J(C)[2]$ be the 2-torsion subgroup of $J(C)(\overline{k})$. The group $J(C)[2]$ is an 8-dimensional vector space over $\mathbb{F}_2$ and is equipped with the *Weil pairing*

$$\langle\ ,\ \rangle \colon J(C)[2] \times J(C)[2] \to \{\pm 1\} \cong \mathbb{F}_2.$$

The pairing $\langle\ ,\ \rangle$ is an alternating nondegenerate bilinear form. The Galois group $\operatorname{Gal}(\overline{k}/k)$ acts on $J(C)[2]$ and preserves the Weil pairing. The following lemma describes the structure of $J(C)[2]$.

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

LEMMA 1.5 ([**21**, Theorem 2.10 and Remark 2.12]). *There is an isomorphism of* $\mathrm{Gal}(\overline{k}/k)$*-modules*

$$J(C)[2] \cong K_X^{\perp}/2K_X^{\perp},$$

which preserves the corresponding $\mathbb{F}_2$*-valued pairings.*

Recall that $K_X^{\perp} \cong E_8$, so the Galois action on $J(C)[2]$ factors through the group $W(E_8)/\{\pm I\}$. We may thus use our examples from Theorem 1.3 to give examples of such curves with maximal Galois action.

PROPOSITION 1.6. *Let* f *be a sextic polynomial in the weighted graded ring* $\mathbb{Z}[x, y, z]$*, where the variables* x, y, z *have weights* $1, 1, 2$ *respectively, such that*

$$\begin{aligned} f \equiv\ & 40x^6 + 63x^5y + 84x^4y^2 + 28x^3y^3 + 42x^2y^4 + 49xy^5 + 75y^6 + 84x^4z \\ & + 7x^3yz + 98x^2y^2z + 84xy^3z + 98y^4z + 35xyz^2 + z^3 \pmod{105}. \end{aligned}$$

Define the curve $C := \mathrm{Proj}(\mathbb{Q}[x, y, z]/(f))$ *and let* $J(C)$ *be its Jacobian. The curve* C *is smooth, geometrically irreducible, non-hyperelliptic, and has genus* 4*. There is an isometry*

$$J(C)[2] \cong E_8/2E_8$$

under which the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *acts as the full group* $W(E_8)/\{\pm I\}$*.*

The Jacobian $J(C)$ *has no non-trivial endomorphisms over* $\overline{\mathbb{Q}}$*, i.e.,*

$$\mathrm{End}(J(C)_{\overline{\mathbb{Q}}}) = \mathbb{Z}.$$

In particular, $J(C)$ *is an absolutely simple abelian four-fold.*

Proof. Let $f_1 := f + w^2 \in \mathbb{Z}[x, y, z, w]$; for the del Pezzo surfaces associated to f_1 in Theorem 1.3, the automorphism $[x : y : z : w] \mapsto [x : y : z : -w]$ is the Bertini involution. The curves in the proposition are in the fixed locus of the Bertini involution of the appropriate del Pezzo surface. That the Galois action is maximal is then a consequence of Theorem 1.3 and Lemma 1.5. The last statements of the proposition follow from [**21**, Theorem 4.3]. □

1.3. *Overview*

Let us briefly outline the contents of this paper.

In §2, we summarize some of the basic theory of del Pezzo surfaces, focusing on the aspects relevant to our application. In particular, in §2.5 and §2.6 we describe how given a del Pezzo surface of degree 1 as a blow-up of $\mathbb{P}^2_k$, one can write down an explicit (weighted) sextic polynomial defining this surface; i.e., the anticanonical model.

In §3, we prove a useful criterion to determine whether a subgroup $H \subseteq W(E_8)$ is actually the full group $W(E_8)$. Applied to a del Pezzo surface $X/\mathbb{Q}$ of degree 1, it gives a criterion for the representation ϕ_X to be surjective (Proposition 3.2). In particular, to show that ϕ_X is surjective, it suffices to give a model $\mathcal{X}/\mathbb{Z}$ of X with certain kinds of reduction at three special fibers. For example, one of the conditions is the existence of a prime p for which $\mathcal{X}_{\mathbb{F}_p}$ is a del Pezzo surface of degree 1 and $\phi_{\mathcal{X}_{\mathbb{F}_p}} \colon \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathrm{O}(K^{\perp}_{\mathcal{X}_{\mathbb{F}_p}})$ has image of order 7.

In order to construct the surfaces of Theorem 1.3, we first construct three del Pezzo surfaces of degree 1 over the finite fields $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$, with the properties

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

required by Proposition 3.2 (this explains the congruences modulo $105 = 3{\cdot}5{\cdot}7$). To prove Theorem 1.3, we then exhibit a scheme $\mathcal{X}/\mathbb{Z}$ whose generic fiber is $X/\mathbb{Q}$, and whose special fibers at $3, 5$, and 7 are isomorphic to the del Pezzo surfaces already calculated (see §6).

Our surfaces over $\mathbb{F}_3$ and $\mathbb{F}_5$ will be given explicitly as the blow-up of 8 points in the projective plane (see §4.1 and §4.2). For our example over $\mathbb{F}_7$, we simply write down a candidate surface and then verify that it satisfies the required properties by applying the Lefschetz trace formula (see §5.3).

Finally, in §7, we show how given a del Pezzo surface $X/\mathbb{Q}$ of degree 1, one can associate an elliptic curve $E/\mathbb{Q}(t)$. As a consequence of the work of Shioda, there is a lattice isomorphism $K_X^{\perp} \cong E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ which respects the corresponding Galois actions. Working this out explicitly, we will find that Theorem 1.1 is a direct consequence of Theorem 1.3.

Acknowledgements

We thank Bjorn Poonen and the referee for many helpful comments. Our computations were performed using MAGMA [**2**]; the code is available via http://www.lms.ac.uk/jcm/12/lms2008-010/appendix-a/.

Notation

We now fix some notation and conventions which will hold throughout the paper. For a field k, fix an algebraic closure $\overline{k}$. For S-schemes X and Y, define $X_Y := X \times_S Y$; if $Y = \operatorname{Spec} B$, then we will write X_B for $X_{\operatorname{Spec} B}$. If $\mathscr{F}$ is a sheaf of $\mathscr{O}_X$-modules on a k-scheme X, then the dimension of the k-vector space $H^0(X, \mathscr{F})$ of global sections will be denoted by $h^0(X, \mathscr{F})$.

By a *surface*, we mean a smooth projective geometrically integral scheme of dimension 2 of finite type over a field k. Given a surface X over k, we have an intersection pairing $(\ ,\ )\colon \operatorname{Pic}(X_{\overline{k}}) \times \operatorname{Pic}(X_{\overline{k}}) \to \mathbb{Z}$. We write ω_X for the canonical sheaf of X, and K_X for its class in the Picard group. We will identify $\operatorname{Pic}(X)$ with the Weil divisor class group; in particular, we will use additive notation for the group law on $\operatorname{Pic}(X)$.

Suppose that k is a number field and that v is a finite place of k. Denote the completion of k at v by k_v, the valuation ring of k_v by $\mathcal{O}_v$, and the corresponding residue field by $\mathbb{F}_v$. Let $F_v \in \operatorname{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)$ be the Frobenius automorphism $x \mapsto x^{|\mathbb{F}_v|}$. We will denote the ring of integers of k by $\mathcal{O}_k$. If S is a set of places of k, we write $\mathcal{O}_{k,S}$ for the ring of S-integers of k.

2. *Background on del Pezzo surfaces*

We now review some basic theory concerning del Pezzo surfaces. The standard references on the subject are [**16**], [**7**] and [**14**, III.3]. In some cases, we give proofs of easy 'folklore facts' that are not included in these standard references. The reader acquainted with the theory of del Pezzo surfaces is encouraged to only skim this section, referring back to it as necessary.

2.1. *Del Pezzo surfaces*

DEFINITION 2.1. A *del Pezzo surface* over a field k is a surface X over k with ample anticanonical sheaf ω_X^{-1}. The *degree* of X is the intersection number (K_X, K_X).

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

For a del Pezzo surface X over k of degree d, we have $1 \leqslant d \leqslant 9$. The surface $X_{\overline{k}}$ is isomorphic to either $\mathbb{P}^1_{\overline{k}} \times \mathbb{P}^1_{\overline{k}}$ (which has degree 8) or to the blow-up of $\mathbb{P}^2_{\overline{k}}$ at $r := 9 - d$ closed points. Moreover, in the second case, the r points are in *general position*; that is, no 3 of them lie on a line, no 6 of them lie on a conic, and no 8 of them lie on a cubic with a singularity at one of the points.

For $r \leqslant 8$, the blow-up of r distinct closed points of $\mathbb{P}^2_{\overline{k}}$ in general position is a del Pezzo surface of degree $9 - r$ over $\overline{k}$ [**7**, Theorem 1, p. 27].

2.2. *Structure of the Picard group*

Let X be a del Pezzo surface over k of degree $d \leqslant 6$. The Picard group $\mathrm{Pic}(X_{\overline{k}})$ is a free abelian group of rank $10 - d = r + 1$, and has a basis $\overline{e}_1, \ldots, \overline{e}_r, \overline{\ell}$ such that

$$(\overline{e}_i, \overline{e}_j) = -\delta_{ij}, \quad (\overline{e}_i, \overline{\ell}) = 0, \quad (\overline{\ell}, \overline{\ell}) = 1, \quad \text{and} \quad -K_X = 3\overline{\ell} - \sum_{i=1}^{r} \overline{e}_i.$$

If $X_{\overline{k}}$ is the blow-up of $\mathbb{P}^2_{\overline{k}}$ along a set of closed points $\{P_1, \ldots, P_r\}$ which are in general position, then we may take $\overline{e}_i$ to be the class of the exceptional divisor e_i corresponding to P_i and $\overline{\ell}$ to be the class of the strict transform of a line ℓ in $\mathbb{P}^2_{\overline{k}}$ not passing through any of the P_i. The divisors e_i are isomorphic to $\mathbb{P}^1_{\overline{k}}$.

Definition 2.2. Let $K_X^{\perp}$ be the orthogonal complement of K_X in $\mathrm{Pic}(X_{\overline{k}})$ with respect to the intersection pairing. We give $K_X^{\perp}$ the structure of a lattice by endowing it with the form that is the *negative* of the intersection pairing.

The lattice $K_X^{\perp}$ is isomorphic to the root lattice of type $A_1 \times A_2$, A_4, D_5, E_6, E_7 or E_8 (where r is the sum of the subscripts) [**16**, Theorem 23.9]. The group $\mathrm{O}(K_X^{\perp})$ of lattice automorphisms of $K_X^{\perp}$ is isomorphic to the Weyl group of $K_X^{\perp}$ (see [**16**, Theorem 23.9 and §26.5]).

2.3. *Galois action on the Picard group*

Let X be a del Pezzo surface over k. For each $\sigma \in \mathrm{Gal}(\overline{k}/k)$, let $\tilde{\sigma}\colon \mathrm{Spec}\,\overline{k} \to \mathrm{Spec}\,\overline{k}$ be the corresponding morphism. Then $\mathrm{id}_X \times \tilde{\sigma} \in \mathrm{Aut}(X_{\overline{k}})$ induces an automorphism $(\mathrm{id}_X \times \tilde{\sigma})^*$ of $\mathrm{Pic}(X_{\overline{k}})$. This action of $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Pic}(X_{\overline{k}})$ fixes the canonical class K_X and preserves the intersection pairing. Therefore it factors through the action on $K_X^{\perp}$, inducing a group homomorphism

$$\begin{aligned} \phi_X\colon \mathrm{Gal}(\overline{k}/k) &\to \mathrm{O}(K_X^{\perp}) \\ \sigma &\mapsto (\mathrm{id}_X \times \tilde{\sigma})^*|_{K_X^{\perp}}. \end{aligned}$$

2.4. *Weighted projective spaces*

We quickly recall some basic definitions for weighted projective spaces; a good general reference is [**8**]. Fix a field k and positive integers $q_0, \ldots, q_n$. Let $k[x_0, \ldots, x_n]$ be the polynomial ring in the variables $x_0, \ldots, x_n$ graded with weights $q_0, \ldots, q_n$, respectively. We define the weighted projective space $\mathbb{P}_k(q_0, \ldots, q_n)$ to be the k-scheme $\mathrm{Proj}(k[x_0, \ldots, x_n])$.

The $\mathbb{Z}$-grading on the variables $x_0, \ldots, x_n$ gives rise to an action of $\mathbb{G}_m$ on $\mathbb{A}_k^{n+1} = \mathrm{Spec}(k[x_0, \ldots, x_n])$ via the k-algebra homomorphism

$$\begin{aligned} k[x_0, \ldots, x_n] &\to k[x_0, \ldots, x_n] \otimes k[t, t^{-1}] \\ x_i &\mapsto x_i \otimes t^{q_i}. \end{aligned}$$

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

The open subscheme $U = \mathbb{A}_k^{n+1} \setminus \{0\}$ is stable under this action. The universal geometric quotient $U/\mathbb{G}_m$ exists and coincides with $\mathbb{P}_k(q_0, \ldots, q_n)$. The set of $\overline{k}$-valued points of $\mathbb{P}_k(q_0, \ldots, q_n)$ can be described as

$$\mathbb{P}_k(q_0, \ldots, q_n)(\overline{k}) = \left(\overline{k}^{n+1} - \{(0, \ldots, 0)\}\right)/\sim,$$

where $(a_0, \ldots, a_n) \sim (a_0', \ldots, a_n')$ if there exists a $\lambda \in \overline{k}^\times$ such that $a_i = \lambda^{q_i} a_i'$ for all i. We denote the equivalence class of $(a_0, \ldots, a_n)$ by $[a_0 : \ldots : a_n]$. A homogeneous ideal I of $k[x_0, \ldots, x_n]$ (with respect to the above grading) determines a closed subscheme $V(I) := \operatorname{Proj}(k[x_0, \ldots, x_n]/I)$ of $\mathbb{P}_k(q_0, \ldots, q_n)$. The set of $\overline{k}$-valued points of $V(I)$ is

$$V(I)(\overline{k}) = \{[a_0 : \ldots : a_n] \in \mathbb{P}_k(q_0, \ldots, q_n)(\overline{k}) : f(a_0, \ldots, a_n) = 0 \text{ for all homogeneous } f \in I\}.$$

2.5. *The anticanonical model*

Besides the blow-up description, there is another useful model of a del Pezzo surface. For any k-scheme X and line bundle $\mathscr{L}$ on X, we may construct the graded k-algebra

$$R(X, \mathscr{L}) := \bigoplus_{m \geqslant 0} H^0(X, \mathscr{L}^{\otimes m}).$$

When $\mathscr{L} = \omega_X^{-1}$, we call $R(X, \omega_X^{-1})$ the *anticanonical ring* of X. If X is a del Pezzo surface over k, then $X \cong \operatorname{Proj} R(X, \omega_X^{-1})$ [14, Theorem III.3.5]. The k-scheme $\operatorname{Proj} R(X, \omega_X^{-1})$ is known as the *anticanonical model* of X.

PROPOSITION 2.3. *Let X be a del Pezzo surface of degree 1 over a field k, and let x, y, z, w be variables with weights $1, 1, 2, 3$ respectively. Then there is an isomorphism of graded k-algebras*

$$R(X, \omega_X^{-1}) \cong k[x, y, z, w]/(f),$$

where f is a sextic in $k[x, y, z, w]$. The surface X is thus isomorphic to the smooth sextic hypersurface $V(f)$ in $\mathbb{P}_k(1, 1, 2, 3)$.

Conversely, if $f \in k[x, y, z, w]$ is a sextic polynomial such that $V(f)$ is smooth, then $V(f)$ is a del Pezzo surface of degree 1.

Proof. See [14, Theorem III.3.5]. □

We now briefly outline how, given a blow-up model of a del Pezzo surface X of degree 1 over a field k, one can find a sextic polynomial f as in Proposition 2.3; details can be found in [6, pp. 1199–1201] and [14, Theorem III.3.5].

Fix a graded k-algebra $R = \bigoplus_{m \geqslant 0} R_m$ that is isomorphic to $R(X, \omega_X^{-1})$. In Proposition 2.6 below, our algebra R will be expressed in terms of the blow-up description of X. By [14, Corollary III.3.2.5], for each integer $m > 0$

$$\dim_k(R_m) = h^0(X, \omega_X^{-m}) = \frac{m(m+1)}{2} + 1.$$

(1) Choose a basis $\{x, y\}$ for the k-vector space R_1.

(2) The elements x^2, xy, y^2 of R_2 are linearly independent. Since $\dim_k(R_2) = 4$, we may choose $z \in R_2$ such that $\{x^2, xy, y^2, z\}$ is a basis of R_2.

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

(3) The elements $x^3, x^2y, xy^2, y^3, xz, yz$ of R_3 are linearly independent. Since $\dim_k(R_3) = 7$, we may choose $w \in R_3$ such that $\{x^3, x^2y, xy^2, y^3, xz, yz, w\}$ is a basis of R_3.

(4) Since $\dim_k(R_6) = 22$, the 23 elements

$$\{x^6, x^5y, x^4y^2, x^3y^3, x^2y^4, xy^5, y^6, x^4z, x^3yz, x^2y^2z, xy^3z, y^4z, x^2z^2, xyz^2, y^2z^2, z^3, x^3w, x^2yw, xy^2w, y^3w, xzw, yzw, w^2\}$$

must be linearly dependent over k. Let $f(x, y, z, w) = 0$ be a nonzero linear relation among these elements.

(5) Viewing f as a sextic polynomial in weighted variables x, y, z, w, we have an isomorphism of graded k-algebras, $R(X, \omega_X^{-1}) \cong R \cong k[x, y, z, w]/(f)$.

Remark 2.4. If k is a field of characteristic not equal to 2 or 3, then in step (5) above, we may complete the square with respect to the variable w and the cube with respect to the variable z to obtain an equation involving only the monomials

$$\{x^6, x^5y, x^4y^2, x^3y^3, x^2y^4, xy^5, y^6, x^4z, x^3yz, x^2y^2z, xy^3z, y^4z, z^3, w^2\}.$$

LEMMA 2.5. *Let X be a del Pezzo surface of degree* 1 *defined over a field k. The linear system $|-K_X|$ has a single base point O, and this point is defined over k. We call O the* anticanonical point *of X. If X is the locus of a sextic $f(x, y, z, w)$ in $\mathbb{P}_k(1, 1, 2, 3)$, then the linear system $|-K_X|$ gives rise to the rational map*

$$X \dashrightarrow \mathbb{P}^1_k,\ [x : y : z : w] \mapsto [x : y].$$

Proof. For the first statement, see [**7**, p. 40]. If X is a sextic $f(x, y, z, w) = 0$ in $\mathbb{P}_k(1, 1, 2, 3)$ then the functions x and y form a basis for $H^0(X, \omega_X^{-1})$ (see [**15**, Proof of Theorem 3.36(6)]). □

2.6. *Blow-up and anticanonical models*

The following proposition shows how, given a del Pezzo surface X of degree 1 as a blow-up of $\mathbb{P}^2_k$, one may recover information about the action of Galois on $\mathrm{Pic}(X_{\overline{k}})$, as well as the anticanonical ring, in terms of the blow-up data.

PROPOSITION 2.6. *Let k be a perfect field. Fix a* $\mathrm{Gal}(\overline{k}/k)$*-stable set*

$$S := \{P_1, \ldots, P_8\}$$

of eight distinct closed points in $\mathbb{P}^2_{\overline{k}} = \mathrm{Proj}(\overline{k}[x_0, x_1, x_2])$ that are in general position. Let $\mathscr{I} \subseteq \mathscr{O}_{\mathbb{P}^2_k}$ be the coherent ideal sheaf associated to the closed subset S of $\mathbb{P}^2_k$ with its reduced-induced subscheme structure. Let X be the del Pezzo surface of degree 1 *over k obtained by blowing up $\mathbb{P}^2_k$ along $\mathscr{I}$.*

(i) *For each $\sigma \in \mathrm{Gal}(\overline{k}/k)$, the order of $\phi_X(\sigma)$ is equal to the order of the action of σ on the set S, the trace of $\phi_X(\sigma)$ is equal to the number of P_i fixed by σ, and the determinant of $\phi_X(\sigma)$ is equal to the sign of the permutation of the P_i.*

(ii) *There is an isomorphism of graded k-algebras,*

$$R(X, \omega_X^{-1}) \cong \bigoplus_{m \geqslant 0} H^0(\mathbb{P}^2_k, \mathscr{I}^m(3m)).$$

The vector space $H^0(\mathbb{P}^2_k, \mathscr{I}^m(3m))$ is the set of homogenous degree $3m$ polynomials in $k[x_0, x_1, x_2]$ that have m-fold vanishing at each P_i.

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

Proof. Let $\pi\colon X \to \mathbb{P}^2_k$ be the blow-up of $\mathbb{P}^2_k$ along $\mathscr{I}$, and let $\overline{e}_i$ be the class of the exceptional divisor e_i of $X_{\overline{k}}$ corresponding to P_i. Then

$$\mathrm{Pic}(X_{\overline{k}}) = \mathbb{Z}\overline{e}_1 \oplus \cdots \oplus \mathbb{Z}\overline{e}_8 \oplus \mathbb{Z}\overline{\ell},$$

where $\mathrm{Gal}(\overline{k}/k)$ fixes the class $\overline{\ell}$ of ℓ and permutes the e_i the same way it permutes the P_i. On the other hand, $\mathrm{Pic}(X_{\overline{k}}) = K_X^{\perp} \oplus \mathbb{Z}\cdot K_X$, and $\mathrm{Gal}(\overline{k}/k)$ acts via ϕ_X on $K_X^{\perp}$ and fixes K_X. Part (i) follows by comparing these two descriptions of the action of $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Pic}(X_{\overline{k}})$.

Let $\tilde{\mathscr{I}} \subseteq \mathcal{O}_X$ be the ideal sheaf of $e_1 \cup \cdots \cup e_8$ with the reduced-induced subscheme structure. We claim that the invertible sheaf

$$\tilde{\mathscr{I}} \otimes_{\mathcal{O}_X} \pi^*(\mathcal{O}_{\mathbb{P}^2_k}(3))$$

is isomorphic to the anticanonical sheaf of X. To prove this it suffices to work over an algebraic closure $\overline{k}$, in which case the invertible sheaves $\pi^*(\mathcal{O}_{\mathbb{P}^2_k}(3))$ and $\tilde{\mathscr{I}}$ correspond to the divisor classes of $3\overline{\ell}$ and $-(\overline{e}_1 + \cdots + \overline{e}_8)$ in $\mathrm{Pic}(X_{\overline{k}})$, respectively. The claim is then immediate since $-K_X = 3\overline{\ell} - (\overline{e}_1 + \cdots + \overline{e}_8) \in \mathrm{Pic}(X_{\overline{k}})$.

We thus have the following isomorphisms of graded k-algebras (we shall write $\mathbb{P}^2$ instead of $\mathbb{P}^2_k$ to avoid clutter),

$$\begin{aligned}
R(X, \omega_X^{-1}) &\cong \bigoplus_{m \geqslant 0} H^0(X, (\tilde{\mathscr{I}} \otimes_{\mathcal{O}_X} \pi^*(\mathcal{O}_{\mathbb{P}^2}(3)))^{\otimes m}) \\
&\cong \bigoplus_{m \geqslant 0} H^0(X, \tilde{\mathscr{I}}^m \otimes_{\mathcal{O}_X} \pi^*(\mathcal{O}_{\mathbb{P}^2}(3m))) \\
&= \bigoplus_{m \geqslant 0} H^0(\mathbb{P}^2, \pi_*(\tilde{\mathscr{I}}^m \otimes_{\mathcal{O}_X} \pi^*(\mathcal{O}_{\mathbb{P}^2}(3m)))) \\
&\cong \bigoplus_{m \geqslant 0} H^0(\mathbb{P}^2, \pi_*(\tilde{\mathscr{I}}^m)(3m)),
\end{aligned}$$

where the last isomorphism follows from the projection formula [**12**, Exercise II.5.1].

The morphism $\mathcal{O}_{\mathbb{P}^2} \to \pi_*\mathcal{O}_X$ coming from π, is an isomorphism of $\mathcal{O}_{\mathbb{P}^2}$-modules (this can be checked on stalks, using the fact that π gives an isomorphism between $X - \pi^{-1}(S)$ and $\mathbb{P}^2 - S$, and that a regular function on e_i must be constant). We will identify $\mathcal{O}_{\mathbb{P}^2}$ and $\pi_*\mathcal{O}_X$, and in particular, we may view $\pi_*(\tilde{\mathscr{I}})$ as an ideal of $\mathcal{O}_{\mathbb{P}^2}$.

The ideal sheaves $\pi_*(\tilde{\mathscr{I}})$ and $\mathscr{I}$ both correspond to closed subschemes of $\mathbb{P}^2$ with support $\{P_1, \ldots, P_8\}$. Since $\mathscr{I}$ corresponds to the reduced-induced subscheme structure on $\{P_1, \ldots, P_8\}$, we find that $\pi_*(\tilde{\mathscr{I}}) \subseteq \mathscr{I}$. The ideal sheaf $\pi^*(\mathscr{I})$ has support $e_1 \cup \cdots \cup e_8$. Since $\tilde{\mathscr{I}}$ corresponds to the reduced-induced subscheme structure on $e_1 \cup \cdots \cup e_8$, we find that $\pi^*(\mathscr{I}) \subseteq \tilde{\mathscr{I}}$ and hence

$$\mathscr{I} = \pi_*\pi^*(\mathscr{I}) \subseteq \pi_*(\tilde{\mathscr{I}})$$

(the equality follows from the projection formula). Therefore $\pi_*(\tilde{\mathscr{I}}) = \mathscr{I}$. For any $m \geqslant 1$, we have $\pi_*(\tilde{\mathscr{I}}^m) = \pi_*(\tilde{\mathscr{I}})^m$ (these sheaves have support $\{P_1, \ldots, P_8\}$ so it suffices to check on the stalks at each P_i). Thus $\pi_*(\tilde{\mathscr{I}}^m) = \pi_*(\tilde{\mathscr{I}})^m = \mathscr{I}^m$ for each $m \geqslant 1$, and hence

$$R(X, \omega_X^{-1}) \cong \bigoplus_{m \geqslant 0} H^0(\mathbb{P}^2, \mathscr{I}^m(3m)). \qquad \square$$

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

2.7. *Reductions of del Pezzo surfaces*

LEMMA 2.7. *Let v be a finite place of a number field k. Suppose that $\mathcal{X}$ is a smooth $\mathcal{O}_v$-scheme such that $X := \mathcal{X}_{k_v}$ and $\mathcal{X}_{\mathbb{F}_v}$ are both del Pezzo surfaces of the same degree $d \leqslant 6$. Given $\sigma \in \mathrm{Gal}(\overline{k}_v/k_v)$, restrict σ to the maximal unramified extension of k_v in $\overline{k}_v$ and let $\overline{\sigma} \in \mathrm{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)$ be the corresponding automorphism of residue fields. There exists an isomorphism of lattices*

$$\beta\colon K_X^{\perp} \xrightarrow{\sim} K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}$$

such that for any $\sigma \in \mathrm{Gal}(\overline{k}_v/k_v)$ we have

$$\phi_X(\sigma) = \beta^{-1}\phi_{\mathcal{X}_{\mathbb{F}_v}}(\overline{\sigma})\beta.$$

Proof. Fix an integral divisor V of X. Let $\overline{V}$ be the Zariski closure of V in $\mathcal{X}$. Since $\overline{V}$ is an $\mathcal{O}_v$-scheme, we may consider its reduction $\overline{V}_{\mathbb{F}_v}$. Extending $V \mapsto \overline{V}_{\mathbb{F}_v}$ by additivity defines a group homomorphism $\alpha\colon \mathrm{Pic}(X) \to \mathrm{Pic}(\mathcal{X}_{\mathbb{F}_v})$ called the *specialization map* (see [**11**, §20.3]). By [**11**, Corollary 20.3], α preserves intersection pairings. From our description of the intersection pairing on $\mathrm{Pic}(X_{\overline{k}_v})$ in §2.2, we find that the intersection pairing is nondegenerate and hence α is injective.

We claim that $\alpha(K_X) = K_{\mathcal{X}_{\mathbb{F}_v}}$. There is a commutative diagram [**11**, §20.3.1],

$$\begin{array}{ccc} & \mathrm{Pic}(\mathcal{X}) & \\ {\scriptstyle j^*}\swarrow & & \searrow{\scriptstyle i^*} \\ \mathrm{Pic}(X) & \xrightarrow{\quad\alpha\quad} & \mathrm{Pic}(\mathcal{X}_{\mathbb{F}_v}), \end{array}$$

where $j\colon X \to \mathcal{X}$ and $i\colon \mathcal{X}_{\mathbb{F}_v} \to \mathcal{X}$ are the morphisms coming from the respective fiber products. Thus it is enough to show that $j^*(K_{\mathcal{X}}) = K_X$ and $i^*(K_{\mathcal{X}}) = K_{\mathcal{X}_{\mathbb{F}_v}}$. Since pull-backs commute with tensor operations [**12**, Ex. II.5.16(e)], it suffices to prove that

$$\Omega^1_{\mathcal{X}/\mathcal{O}_v} \times_{\mathcal{O}_v} k_v \cong \Omega^1_{X/k_v} \quad \text{and} \quad \Omega^1_{\mathcal{X}/\mathcal{O}_v} \times_{\mathcal{O}_v} \mathbb{F}_v \cong \Omega^1_{\mathcal{X}_{\mathbb{F}_v}/\mathbb{F}_v};$$

these isomorphisms follow from the compatibility of relative differentials with base extension [**12**, II.8.10]. Therefore $\alpha(K_X) = K_{\mathcal{X}_{\mathbb{F}_v}}$.

Since α preserves intersection pairings and $\alpha(K_X) = K_{\mathcal{X}_{\mathbb{F}_v}}$, we have an injection of lattices

$$\beta := \alpha|_{K_X^{\perp}}\colon K_X^{\perp} \hookrightarrow K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}.$$

Since X and $\mathcal{X}_{\mathbb{F}_v}$ are del Pezzo surfaces of the same degree, we know that $\beta(K_X^{\perp})$ and $K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}$ are isomorphic lattices. However, the root lattice $K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}$ has no sublattice isomorphic to itself. So $\beta(K_X^{\perp}) = K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}$, and thus β is an isomorphism.

Take any $\sigma \in \mathrm{Gal}(\overline{k}_v/k_v)$. For an integral divisor V of X, one finds that $\overline{\sigma(V)}_{\mathbb{F}_v} = \overline{\sigma}(\overline{V}_{\mathbb{F}_v})$; equivalently, α commutes with the respective Galois actions. It is then an immediate consequence that $\beta\phi_X(\sigma) = \phi_{\mathcal{X}_{\mathbb{F}_v}}(\overline{\sigma})\beta$. □

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

LEMMA 2.8. *Let X be a del Pezzo surface of degree $d \leqslant 6$ over a number field k. Let S be a finite set of places of k. Let $\mathcal{X}$ be a smooth $\mathcal{O}_{k,S}$-scheme for which $X = \mathcal{X}_k$, and let $v \notin S$ be a finite place of k such that $\mathcal{X}_{\mathbb{F}_v}$ is also a del Pezzo surface of degree d. Then there is a lattice isomorphism $\theta\colon K_X^{\perp} \xrightarrow{\sim} K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}$ and an automorphism $\sigma \in \mathrm{Gal}(\overline{k}/k)$ such that*

$$\phi_X(\sigma) = \theta^{-1}\phi_{\mathcal{X}_{\mathbb{F}_v}}(F_v)\theta.$$

Proof. In the notation of Lemma 2.7, choose $\sigma \in \mathrm{Gal}(\overline{k}_v/k_v)$ with $\overline{\sigma} = F_v$. Applying Lemma 2.7 with $\mathcal{X}_{\mathcal{O}_v}$, we know there is a lattice isomorphism $\beta\colon K_{X_{k_v}}^{\perp} \xrightarrow{\sim} K_{\mathcal{X}_{\mathbb{F}_v}}^{\perp}$ for which

$$\phi_{X_{k_v}}(\sigma) = \beta^{-1}\phi_{\mathcal{X}_{\mathbb{F}_v}}(F_v)\beta.$$

Now fix an embedding $\iota\colon \overline{k} \hookrightarrow \overline{k}_v$. This gives an inclusion $\mathrm{Gal}(\overline{k}_v/k_v) \hookrightarrow \mathrm{Gal}(\overline{k}/k)$, and hence we may also view σ as an automorphism of $\overline{k}$. The embedding ι induces an isomorphism $\gamma\colon \mathrm{Pic}(X_{\overline{k}}) \xrightarrow{\sim} \mathrm{Pic}(X_{\overline{k}_v})$ which preserves the intersection pairing and the canonical class. Therefore $\gamma|_{K_X^{\perp}}$ is a lattice isomorphism from $K_X^{\perp}$ to $K_{X_{k_v}}^{\perp}$ such that

$$\phi_X(\sigma) = (\gamma|_{K_X^{\perp}})^{-1}\phi_{X_{k_v}}(\sigma)\gamma|_{K_X^{\perp}}.$$

The lemma follows by setting $\theta := \beta\gamma|_{K_X^{\perp}}$. □

3. *Group theory*

We wish to find a del Pezzo surface X of degree 1 with surjective homomorphism

$$\phi_X\colon \mathrm{Gal}(\overline{k}/k) \to \mathrm{O}(K_X^{\perp}).$$

To accomplish this, we will need a convenient criterion to determine whether a subgroup of $\mathrm{O}(K_X^{\perp}) \cong W(E_8)$ is the full group.

The Weyl group $W(E_8)$ may be viewed as a subgroup of $\mathrm{GL}(E_8) \cong \mathrm{GL}_8(\mathbb{Z})$, so we can talk about the trace, determinant, and characteristic polynomials of elements (or conjugacy classes) of $W(E_8)$. The *order* of a conjugacy class is the order of any element in the conjugacy class as a group element; this should not be confused with the *cardinality* of a conjugacy class which is the number of elements it contains. The goal of this section is to prove the following group theoretic proposition.

PROPOSITION 3.1. *Let H be a subgroup of $W(E_8)$. Suppose that the following conditions hold:*

i. *there exists an element in H of order 7,*
ii. *there exists an element in H of order 3 and trace 5,*
iii. *there exists an element in H of order 3 and trace -4,*
iv. *there exists an element in H with determinant -1.*

Then $H = W(E_8)$.

In terms of our application to del Pezzo surfaces, we have the following criterion.

PROPOSITION 3.2. *Let X be a del Pezzo surface of degree 1 over a number field k. Let S be a finite set of places of k, and let $v_1, v_2, v_3 \notin S$ be finite places of k. Suppose there exists a smooth $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ such that the following conditions hold:*

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

(i) $X = \mathcal{X}_k$,

(ii) $\mathcal{X}_{\mathbb{F}_{v_1}}$, $\mathcal{X}_{\mathbb{F}_{v_2}}$, *and* $\mathcal{X}_{\mathbb{F}_{v_3}}$ *are del Pezzo surfaces of degree* 1,

(iii) $\phi_{\mathcal{X}_{\mathbb{F}_{v_1}}}(F_{v_1})$ *has order* 7,

(iv) $\phi_{\mathcal{X}_{\mathbb{F}_{v_2}}}(F_{v_2})$ *has order* 6 *and determinant* -1, *and* $\phi_{\mathcal{X}_{\mathbb{F}_{v_2}}}(F_{v_2})^2$ *has trace* 5,

(v) $\phi_{\mathcal{X}_{\mathbb{F}_{v_3}}}(F_{v_3})$ *has order* 3 *and trace* -4.

Then $\phi_X\colon \mathrm{Gal}(\overline{k}/k) \to \mathrm{O}(K_X^{\perp})$ *is surjective.*

Proof. By the assumptions of the proposition and Lemma 2.8, there are $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Gal}(\overline{k}/k)$ such that $\phi_X(\sigma_1)$ has order 7, $\phi_X(\sigma_2)$ has order 6 and determinant -1, $\phi_X(\sigma_2)^2$ has order 3 and trace 5, and $\phi_X(\sigma_3)$ has order 3 and trace -4.

Recall that $K_X^{\perp}$ is isomorphic to the E_8 lattice, and $\mathrm{O}(K_X^{\perp}) \cong W(E_8)$. Thus applying Proposition 3.1, we find that $\phi_X(\mathrm{Gal}(\overline{k}/k)) = \mathrm{O}(K_X^{\perp})$. □

Remark 3.3. Let X be a del Pezzo surface of degree 1 over a number field k. Using the Chebotarev density theorem, it is easy to see that if ϕ_X is surjective, then there is a model $\mathcal{X}$ and places v_1, v_2, v_3 satisfying the conditions in Proposition 3.2.

Let $W^+(E_8)$ be the subgroup of $W(E_8)$ consisting of the elements with positive determinant. We have an exact sequence

$$1 \to W^+(E_8) \to W(E_8) \xrightarrow{\det} \{\pm 1\} \to 1. \tag{3.1}$$

Since $-I$ is an element of $W(E_8)$, there is an exact sequence

$$1 \to \{\pm I\} \to W^+(E_8) \xrightarrow{\varphi} G \to 1, \tag{3.2}$$

where $G := W^+(E_8)/\{\pm I\}$ and φ is the quotient map. In [**3**, Ch. VI §4 Ex. 1], it is sketched out that G is isomorphic to a certain simple nonabelian group $O_8^+(2)$. We will use the *Atlas of finite groups* [**5**, p. 85], which we will henceforth refer to simply as *the Atlas*, as a source of information concerning the group $G \cong O_8^+(2)$. In the notation of the Atlas, $W(E_8)$ is isomorphic to $2.O_8^+(2).2$.

Lemma 3.4. *Given a conjugacy class C of $W^+(E_8)$ of order* 3, *$\varphi(C)$ is a conjugacy class of G of order* 3*; this induces a bijection between the conjugacy class of order* 3 *of $W^+(E_8)$ with those of G.*

The group $W^+(E_8)$ and G both have exactly five conjugacy classes of order 3. *In both cases these five conjugacy classes have cardinalities* 2240, 2240, 2240, 89600, *and* 268800.

Proof. Let C be a conjugacy class of $W^+(E_8)$ of order 3. The homomorphism φ is surjective, so $\varphi(C)$ is indeed a conjugacy class of G. Since $\ker\phi = \{\pm I\}$, $\varphi(C)$ must also have order 3.

Let $\mathscr{C}$ be a conjugacy class of G of order 3. Choose $g \in W^+(E_8)$ such that $\varphi(g) \in \mathscr{C}$. Then either g or $(-I)g$ has order 3 (the other element having order 6). It is now clear that there are two conjugacy classes C of $W^+(E_8)$ such that $\varphi(C) = \mathscr{C}$, one of order 3 and one of order 6. The correspondence stated in the lemma is now apparent.

For any conjugacy class C of $W^+(E_8)$ of order 3, $|C| = |\varphi(C)|$. The last statement of the lemma on the number and size of conjugacy classes of G of order 3 can then be read off the Atlas (the Atlas gives the cardinality of the centralizer of any element of

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

a conjugacy class of G, from this one can calculate the cardinality of the conjugacy class itself). □

LEMMA 3.5. *The group $W(E_8)$ has exactly four conjugacy classes of order 3. These conjugacy classes $\{C_i\}_{i=1,\dots,4}$ can be numbered so that*

$$|C_1| = 2240, \quad \operatorname{tr}(C_1) = 5 \qquad |C_2| = 4480, \quad \operatorname{tr}(C_2) = -4$$
$$|C_3| = 89600, \quad \operatorname{tr}(C_3) = -1 \qquad |C_4| = 268800, \quad \operatorname{tr}(C_4) = 2.$$

Proof. A description of the conjugacy classes of $W(E_8)$ in terms of 'admissible diagrams' can be found in [4]. A conjugacy class of $W(E_8)$ of order 3 must have one of the following four characteristic polynomials:

$$(x^2+x+1)(x-1)^6,\ (x^2+x+1)^2(x-1)^4,\ (x^2+x+1)^3(x-1)^2\ ,\ (x^2+x+1)^4$$

(and hence have trace 5, 2, −1, or −4 respectively). In terms of the conventions of [4, §6], these characteristic polynomials correspond to the 'admissible diagrams' A_2, A_2^2, A_2^3 and A_2^4. The lemma is then a consequence of Table 11 in [4]. □

Proof of Proposition 3.1. Define $\mathscr{H} = \varphi(H \cap W^+(E_8))$. Note that any element in $W(E_8)$ of odd order has determinant +1. By assumption (i) of the proposition, there is an $h \in H$ of order 7. The homomorphism φ has kernel $\{\pm I\}$, so $\varphi(h)$ is an element of order 7 in $\mathscr{H}$.

By (iv) there is a $w \in H$ such that $\det(w) = -1$, and by (ii) and (iii) there are $h_1, h_2 \in H \cap W^+(E_8)$ of order 3 such that $\operatorname{tr}(h_1) = 5$ and $\operatorname{tr}(h_2) = -4$. Let $\mathscr{C}_1$, $\mathscr{C}_2$ and $\mathscr{C}_3$ be the conjugacy classes of $W^+(E_8)$ of order 3 and cardinality 2240 (here we are using Lemma 3.4). By Lemma 3.5 and cardinality considerations, we have (after possibly renumbering the $\mathscr{C}_i$) $C_1 = \mathscr{C}_1$ and $C_2 = \mathscr{C}_2 \cup \mathscr{C}_3$.

Since $W^+(E_8)$ is a normal subgroup of $W(E_8)$, the set $w\mathscr{C}_2 w^{-1}$ is also a conjugacy class of $W^+(E_8)$ (of trace −4). Since $\mathscr{C}_2$ is not a conjugacy class of $W(E_8)$, we deduce that $\mathscr{C}_3 = w\mathscr{C}_2 w^{-1}$. So $h_1 \in C_1 = \mathscr{C}_1$, and the set $\{h_2, wh_2w^{-1}\}$ contains elements from both of the conjugacy classes $\mathscr{C}_2$ and $\mathscr{C}_3$. Therefore $\varphi(h_1)$, $\varphi(h_2)$, $\varphi(wh_2w^{-1}) \in \mathscr{H}$ are representatives of the three conjugacy classes of order 3 and cardinality 2240 in G.

Now consider any maximal proper subgroup M of G. The Atlas gives a description of the maximal proper subgroups of G.

Suppose that $|M| > 155520$. By checking the permutation character of G associated with M given in the Atlas, one verifies that M does not contain elements from all three of the conjugacy classes of order 3 and cardinality 2240 in G. However, we have just shown that $\mathscr{H}$ contains elements from each of these three conjugacy classes, hence $\mathscr{H} \not\subseteq M$.

If $|M| \leqslant 155520$, then the Atlas shows that $7 \nmid |M|$ and in particular M does not have any elements of order 7. Since $\mathscr{H}$ has an element of order 7, $\mathscr{H} \not\subseteq M$.

Since $\mathscr{H}$ is not contained in any of the proper maximal subgroups of G, we must have

$$\varphi(H \cap W^+(E_8)) = \mathscr{H} = G.$$

Suppose that $-I \notin H \cap W^+(E_8)$. Since $\varphi(H \cap W^+(E_8)) = G$ and $(H \cap W^+(E_8)) \cap \ker\varphi = \{1\}$, the map $\varphi\colon W^+(E_8) \to G$ induces an isomorphism $H \cap W^+(E_8) \cong G$. Using our description of $W(E_8)$ as a subgroup of $\mathrm{GL}(E_8)$, we get an injective group

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

homomorphism $G \hookrightarrow W(E_8) \subseteq \mathrm{GL}(E_8)$. Hence there exists an *injective* complex representation of G,

$$\rho\colon G \hookrightarrow \mathrm{GL}(E_8 \otimes_{\mathbb{Z}} \mathbb{C}) \cong \mathrm{GL}_8(\mathbb{C}).$$

The character table of G in the Atlas, shows that G has no non-trivial irreducible representations of degree less than 28, and so any eight dimensional complex representation of G is trivial. This contradicts the injectivity of ρ, and we conclude that $-I$ is an element of $H \cap W^+(E_8)$.

Since $-I \in H \cap W^+(E_8)$ and $\varphi(H \cap W^+(E_8)) = G$, the exact sequence (3.2) shows that $H \cap W^+(E_8) = W^+(E_8)$. Finally, since $H \supseteq W^+(E_8)$ and $\det(H) = \{\pm 1\}$ (by assumption (iv)), the exact sequence (3.1) shows that $H = W(E_8)$. □

4. *Examples: from blow-up to anticanonical models*

The graded ring in Proposition 2.6(ii) is amenable to computation, and in particular we may implement the procedure outlined after Proposition 2.3. Thus, given a Galois stable set of 8 points in general position, we have a method for finding the corresponding del Pezzo surface of degree 1 as a sextic in weighted projective space. We will give two examples of this. The first will be of a surface X over $\mathbb{F}_3$ such that $\phi_X(F_3)$ has order 7. The second will be a surface X over $\mathbb{F}_5$ such that $\phi_X(F_5)$ has order 6 and determinant -1, and such that $\phi_X(F_5)^2$ has trace 5. We will use these surfaces to construct a del Pezzo surface of degree 1 over $\mathbb{Q}$ satisfying parts (iii) and (iv) of Proposition 3.2. The calculations amount simply to linear algebra over finite fields, and are easily implemented on a computer. We have provided enough details so that the careful reader may verify all our claims.

4.1. *An example over $\mathbb{F}_3$*

Let α be a root of the irreducible polynomial $t^7 + 2t^2 + 1 \in \mathbb{F}_3[t]$. Let $F_3\colon \overline{\mathbb{F}}_3 \to \overline{\mathbb{F}}_3$ be the Frobenius map $x \mapsto x^3$, and define the following set of eight points in $\mathbb{P}^2_{\overline{\mathbb{F}}_3}$:

$$S := \{[1,0,0]\} \cup \{[1 : F_3^i(\alpha) : F_3^i(\alpha^4)] : 0 \leqslant i \leqslant 6\}.$$

A direct computation shows that the points in S are in general position. Let $\mathscr{I}$ be the coherent sheaf of ideals in $\mathbb{P}^2_{\mathbb{F}_3}$ corresponding to the reduced-induced structure of S. Denote by $\pi\colon X \to \mathbb{P}^2_{\mathbb{F}_3}$ the blow-up along $\mathscr{I}$. Since F_3 fixes $[1:0:0]$ and acts transitively on the other seven points of S, it follows from Proposition 2.6(i) that $\phi_X(F_3)$ has order 7.

We now use Proposition 2.6(ii) and the procedure outlined after Proposition 2.3 to calculate a defining equation for X. The polynomials

$$x = x_0^2x_1 + x_0x_2^2 + 2x_1^3 \quad \text{and} \quad y = x_0^2x_2 + 2x_0x_1^2 + 2x_1x_2^2$$

form a basis of $H^0(\mathbb{P}^2_{\mathbb{F}_3}, \mathscr{I}(3))$. Let

$$\begin{aligned} z = {} & x_0^6 + x_0^3x_1^3 + 2x_0^2x_1^2x_2^2 + 2x_0^2x_2^4 + x_0x_1^5 + 2x_0x_1^3x_2^2 \\ & + x_0x_1^2x_2^3 + x_0x_1x_2^4 + 2x_1^6 + 2x_1^5x_2 + x_1^4x_2^2; \end{aligned}$$

then $\{x^2, xy, y^2, z\}$ is a basis of $H^0(\mathbb{P}^2_{\mathbb{F}_3}, \mathscr{I}^2(6))$.

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

Let

$$\begin{aligned} w = {} & x_0^9 + 2x_0^7x_1x_2 + x_0^5x_1^2x_2^2 + x_0^5x_2^4 + 2x_0^4x_1^2x_2^3 + 2x_0^4x_1x_2^4 + x_0^3x_1^6 + x_0^3x_1^4x_2^2 \\ & + x_0^3x_2^6 + 2x_0^2x_1^6x_2 + 2x_0^2x_1^4x_2^3 + x_0x_1^7x_2 + x_0x_1^6x_2^2 + x_0x_1^5x_2^3 + 2x_0x_1^2x_2^6 \\ & + x_1^5x_2^4 + 2x_1^4x_2^5 + 2x_1^3x_2^6; \end{aligned}$$

then $\{x^3, x^2y, xy^2, y^3, xz, yz, w\}$ is a basis of $H^0(\mathbb{P}^2_{\mathbb{F}_3}, \mathscr{I}^3(9))$. Elementary linear algebra now yields the relation

$$2x^6 + 2x^3y^3 + xy^5 + y^6 + 2x^3yz + x^2y^2z + y^4z + 2xyz^2 + 2z^3 + 2x^3w + y^3w + w^2 = 0$$

in $H^0(\mathbb{P}^2_{\mathbb{F}_3}, \mathscr{I}^6(18))$. The transformation $w \mapsto w - (x^3 + 2y^3)$ gives a new equation

$$x^6 + x^3y^3 + xy^5 + 2x^3yz + x^2y^2z + y^4z + 2xyz^2 + 2z^3 + w^2 = 0.$$

Under the transformation $z \mapsto -z$ the coefficient of z^3 becomes 1 and yields

$$x^6 + x^3y^3 + xy^5 + x^3yz + 2x^2y^2z + 2y^4z + 2xyz^2 + z^3 + w^2 = 0. \tag{4.1}$$

This gives a model for X as a smooth sextic hypersurface in $\mathbb{P}_{\mathbb{F}_3}(1, 1, 2, 3)$.

4.2. *An example over* $\mathbb{F}_5$

Let α be a root of the irreducible polynomial $t^6 + t^4 + 4t^3 + t^2 + 2 \in \mathbb{F}_5[t]$. Define $\beta = \alpha^{5^4+5^2+1}$ and $\gamma = \alpha^{5^3+1}$, so $\mathbb{F}_5(\beta)$ and $\mathbb{F}_5(\gamma)$ are degree 2 and 3 extensions of $\mathbb{F}_5$, respectively. Let $F_5 \colon \overline{\mathbb{F}}_5 \to \overline{\mathbb{F}}_5$ be the Frobenius map $x \mapsto x^5$, and define the following set of eight points in $\mathbb{P}^2_{\overline{\mathbb{F}}_5}$:

$$\begin{aligned} S := \{ & [1,0,0], [3:2:4], [4:2:1], [1:\beta:\beta^3], [1:F_5(\beta):F_5(\beta^3)], \\ & [1:\gamma:\gamma^4], [1:F_5(\gamma):F_5(\gamma^4)], [1:F_5^2(\gamma):F_5^2(\gamma^4)]\}. \end{aligned}$$

A direct computation shows that the points in S are in general position. Let $\mathscr{I}$ be the coherent sheaf of ideals in $\mathbb{P}^2_{\mathbb{F}_5}$ corresponding to the reduced-induced structure of S. Denote by $\pi \colon X \to \mathbb{P}^2_{\mathbb{F}_5}$ the blow-up along $\mathscr{I}$. Since F_5 acts as an order 6 odd permutation on S, it follows from Proposition 2.6(i) that $\phi_X(F_5)$ has order 6 and determinant -1. The automorphism F_5^2 fixes exactly 5 elements of S, that is the three $\mathbb{F}_5$-rational points and the order 2 orbit of $[1:\beta:\beta^3]$; therefore $\phi_X(F_5)^2$ has trace 5.

We now use Proposition 2.6(ii) and the procedure outlined after Proposition 2.3 to calculate a defining equation for X. The polynomials

$$\begin{aligned} x &= x_0^3 + 4x_0x_1^2 + 2x_0x_1x_2 + x_0x_2^2 + x_1^2x_2 + 4x_1x_2^2 \quad \text{and} \\ y &= x_0^2x_1 + 3x_0^2x_2 + 3x_0x_1^2 + x_0x_1x_2 + 3x_0x_2^2 + 4x_1^2x_2 + 3x_1x_2^2 \end{aligned}$$

form a basis of $H^0(\mathbb{P}^2_{\mathbb{F}_5}, \mathscr{I}(3))$. Let

$$\begin{aligned} z = {} & x_0^5x_1 + 2x_0^4x_2^2 + 4x_0^3x_1^3 + 2x_0^3x_1^2x_2 + x_0^3x_1x_2^2 + 4x_0^3x_2^3 + 3x_0^2x_1^4 + x_0^2x_1^3x_2 \\ & + 4x_0^2x_1^2x_2^2 + 3x_0^2x_1x_2^3 + 3x_0^2x_2^4 + x_0x_1^4x_2 + 4x_0x_1^3x_2^2 + 4x_0x_1^2x_2^3 \\ & + 3x_0x_2^5 + 4x_1^4x_2^2 + 4x_1^3x_2^3 + x_1^2x_2^4 + 2x_1x_2^5 + 3x_2^6; \end{aligned}$$

then $\{x^2, xy, y^2, z\}$ is a basis of $H^0(\mathbb{P}^2_{\mathbb{F}_5}, \mathscr{I}^2(6))$. Let

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

$$\begin{aligned} w = {} & x_0^9 + 2x_0^6x_1^2x_2 + 2x_0^6x_1x_2^2 + x_0^6x_2^3 + x_0^5x_1^3x_2 + 3x_0^5x_1^2x_2^2 + 4x_0^5x_1x_2^3 + 3x_0^5x_2^4 \\ & + 4x_0^4x_1^5 + 3x_0^4x_1^3x_2^2 + 2x_0^4x_2^5 + 3x_0^3x_1^5x_2 + x_0^3x_1^4x_2^2 + 3x_0^3x_1^3x_2^3 + 3x_0^3x_1^2x_2^4 \\ & + 4x_0^3x_1x_2^5 + 3x_0^3x_2^6 + 2x_0^2x_1^5x_2^2 + x_0^2x_1^4x_2^3 + x_0^2x_1^3x_2^4 + 4x_0^2x_1^2x_2^5 + 4x_0^2x_1x_2^6 \\ & + 2x_0^2x_2^7 + 2x_0x_1^6x_2^2 + 4x_0x_1^5x_2^3 + x_0x_1^4x_2^4 + 3x_0x_1^3x_2^5 + 4x_0x_1^2x_2^6 + 2x_0x_1x_2^7 \\ & + x_1^6x_2^3 + x_1^5x_2^4 + x_1^4x_2^5 + 2x_1^2x_2^7 + x_2^9; \end{aligned}$$

then $\{x^3, x^2y, xy^2, y^3, xz, yz, w\}$ is a basis of $H^0(\mathbb{P}^2_{\mathbb{F}_5}, \mathscr{I}^3(9))$. Elementary linear algebra now yields the linear relation

$$\begin{aligned} & 2x^6 + 3x^5y + x^4y^2 + 4x^3y^3 + 4x^2y^4 + 4y^6 + 4x^4z + 2x^3yz + x^2y^2z + 2xy^3z \\ & \quad + 3y^4z + 3x^2z^2 + 2y^2z^2 + 2z^3 + 2x^3w + 2x^2yw + 2xy^2w + xzw + w^2 = 0 \end{aligned}$$

in $H^0(\mathbb{P}^2_{\mathbb{F}_5}, \mathscr{I}^6(18))$. Performing the transformations $w \mapsto w - (x^3 + x^2y + xy^2 + 3xz)$ and $z \mapsto z - (x^2 + 4y^2)$, we obtain the equation

$$2x^5y + x^4y^2 + 2x^3y^3 + 3x^2y^4 + xy^5 + 2x^4z + x^3yz + 4x^2y^2z + 2xy^3z + 4y^4z + 2z^3 + w^2 = 0.$$

Multiplying both sides by 4, and rescaling by $[x, y, z, w] \mapsto [x, y, z/2, w/2]$ yields

$$\begin{aligned} & 3x^5y + 4x^4y^2 + 3x^3y^3 + 2x^2y^4 + 4xy^5 + 4x^4z \\ & \quad + 2x^3yz + 3x^2y^2z + 4xy^3z + 3y^4z + z^3 + w^2 = 0. \end{aligned} \tag{4.2}$$

This gives a model for X as a smooth sextic hypersurface in $\mathbb{P}_{\mathbb{F}_5}(1, 1, 2, 3)$.

5. *The Lefschetz trace formula*

In §5.3, we will describe a del Pezzo surface X of degree 1 over $\mathbb{F}_7$ such that $\phi_X(F_7)$ has order 3 and trace -4. This gives a surface satisfying part (v) of Proposition 3.2. To prove these properties of $X/\mathbb{F}_7$ it will suffice, by the Lefschetz trace formula, to compute $|X(\mathbb{F}_7)|$ and $|X(\mathbb{F}_{7^3})|$. The method used in §4 cannot produce this example, since Proposition 2.6 only gives surfaces $X/\mathbb{F}_7$ with $\mathrm{tr}(\phi_X(F_7)) \geqslant 0$.

5.1. *The Lefschetz trace formula*

The following version of the Lefschetz trace formula (specialized to del Pezzo surfaces) is due to Weil.

THEOREM 5.1. *Let $\mathbb{F}_q$ be a finite field with q elements, and let $F_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ be the Frobenius automorphism $x \mapsto x^q$. Let X be a del Pezzo surface over $\mathbb{F}_q$ of degree $d \leqslant 6$. Then*

$$|X(\mathbb{F}_q)| = q^2 + q(\mathrm{tr}(\phi_X(F_q)) + 1) + 1.$$

Remark 5.2. For a proof of Theorem 5.1, see [**16**, §27]. Note that $\mathrm{tr}(\phi_X(F_q)) + 1$ is the trace of the action of F_q on $\mathrm{Pic}(X_{\overline{\mathbb{F}}_q})$.

5.2. *Points on the anticanonical model*

Fix a finite field $\mathbb{F}$. Let X be a del Pezzo surface of degree 1 defined over $\mathbb{F}$ which is given explicitly as a smooth sextic hypersurface

$$w^2 = z^3 + F(x, y)z^2 + G(x, y)z + H(x, y)$$

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

in $\mathbb{P}_{\mathbb{F}}(1,1,2,3)$. Now consider the morphism $\varphi\colon X - \{[0:0:1:1]\} \to \mathbb{P}^1_{\mathbb{F}}$, $[x:y:z:w] \mapsto [x:y]$ of Lemma 2.5. Take any point $P = [a:b] \in \mathbb{P}^1(\mathbb{F})$ with $(a,b) \in \mathbb{F}^2 - \{(0,0)\}$. The fiber of φ above P is isomorphic to the affine curve

$$C_P\colon W^2 = Z^3 + F(a,b)Z^3 + G(a,b)Z^2 + H(a,b)$$

in $\mathbb{A}^2_{\mathbb{F}}$. We thus have

$$|X(\mathbb{F})| = \sum_{P\in\mathbb{P}^1(\mathbb{F})} |C_P(\mathbb{F})| + 1. \tag{5.1}$$

5.3. *An example over $\mathbb{F}_7$*

LEMMA 5.3. *Let X be the closed subscheme of $\mathbb{P}_{\mathbb{F}_7}(1,1,2,3)$ defined by the sextic*

$$w^2 = z^3 + 2x^6 + 2y^6.$$

Then X is a del Pezzo surface of degree 1 over $\mathbb{F}_7$, $\phi_X(F_7)$ has order 3, and $\operatorname{tr}(\phi_X(F_7)) = -4$.

Proof. The scheme X is defined by a smooth sextic, and hence is a del Pezzo surface of degree 1 by Proposition 2.3. Consider an element $g \in \mathrm{O}(K_X^\perp)$. Since $K_X^\perp \cong \mathbb{Z}^8$ and g has finite order, we find that $\operatorname{tr}(g) \leqslant 8$, with equality holding if and only if $g = I$. By Theorem 5.1,

$$|X(\mathbb{F}_7)| = 7^2+7(\operatorname{tr}(\phi_X(F_7))+1)+1 \quad\text{and}\quad |X(\mathbb{F}_{7^3})| = 7^6+7^3(\operatorname{tr}(\phi_X(F_7)^3)+1)+1,$$

and thus the lemma is equivalent to showing that

$$|X(\mathbb{F}_7)| = 7^2 + 7\cdot(-3) + 1 = 29 \quad\text{and}\quad |X(\mathbb{F}_{7^3})| = 7^6 + 7^3\cdot 9 + 1 = 120737.$$

Let $\mathbb{F}$ be an extension of $\mathbb{F}_7$. For $(a,b) \in \mathbb{F}^2 - \{(0,0)\}$, define the affine curve

$$C_{[a,b]}\colon W^2 = Z^3 + 2a^6 + 2b^6$$

in $\mathbb{A}^2_{\mathbb{F}}$. From (5.1),

$$|X(\mathbb{F})| = |C_{[1,0]}(\mathbb{F})| + \sum_{a\in\mathbb{F}} |C_{[a,1]}(\mathbb{F})| + 1. \tag{5.2}$$

For $\mathbb{F} = \mathbb{F}_7$, we have $|C_{[1,0]}(\mathbb{F}_7)| = |C_{[0,1]}(\mathbb{F}_7)| = 8$, and $|C_{[a,1]}(\mathbb{F}_7)| = 2$ for all $a \in \mathbb{F}_7^\times$; so $|X(\mathbb{F}_7)| = 2\cdot 8 + 6\cdot 2 + 1 = 29$.

Now let $\mathbb{F} = \mathbb{F}_{7^3}$. We will use (5.2) to compute $|X(\mathbb{F})|$, but it is useful to note that $|C_{[a,b]}(\mathbb{F})|$ depends only the class of $2a^6 + 2b^6$ in $\mathbb{F}^\times/(\mathbb{F}^\times)^6 \cup \{0\}$. We have a bijection $r\colon \mathbb{F}^\times/(\mathbb{F}^\times)^6 \cup \{0\} \to \mathbb{F}_7$, $a \mapsto a^{(|\mathbb{F}|-1)/6}$. For $i \in \mathbb{F}_7$, let $N_i(\mathbb{F})$ be the the number of $\mathbb{F}$-points of the affine curve $W^2 = Z^3 + \alpha$, where α is any element of $\mathbb{F}$ with $r(\alpha) = i$. It follows that

$$|X(\mathbb{F})| = |C_{[1,0]}(\mathbb{F})| + \sum_{i=0}^{6} |\{a \in \mathbb{F} : r(2a^6+2) = i\}| \cdot N_i(\mathbb{F}) + 1.$$

The right hand side is readily computed, and we find that:

$$\begin{aligned}|X(\mathbb{F}_{7^3})| &= 323 + 0\cdot 343 + 43\cdot 323 + 72\cdot 380 + 72\cdot 360\\ &\quad + 36\cdot 326 + 36\cdot 306 + 84\cdot 363 + 1 = 120737.\end{aligned}$$

□

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

Remark 5.4. We can also verify our previous examples of del Pezzo surfaces over finite fields using this method. For example, consider the surface $X/\mathbb{F}_3$ defined by (4.1). To show that $\phi_X(F_3)$ has order 7, it suffices to check that

$$|X(\mathbb{F}_3)| \neq 3^2+3\cdot 9+1 \quad \text{and} \quad |X(\mathbb{F}_{3^7})| = 3^{14}+3^7\cdot 9+1.$$

Now consider the surface $X/\mathbb{F}_5$ defined by (4.2). One verifies that

$$|X(\mathbb{F}_{5^2})| = 5^4+5^2\cdot 6+1, \quad |X(\mathbb{F}_{5^3})| = 5^6+5^3\cdot 7+1, \quad \text{and} \quad |X(\mathbb{F}_{5^6})| = 5^{12}+5^6\cdot 9+1.$$

It is then apparent that $\phi_X(F_5)$ has order 6 and $\phi_X(F_5)^2$ has trace 5. Since $\phi_X(F_5)^3$ has order 2 and $\operatorname{tr}(\phi_X(F_5)^3) = 6$, we deduce that $\phi_X(F_5)^3$ has eigenvalue $+1$ with multiplicity 7, and -1 with multiplicity 1. Therefore $\det(\phi_X(F_5)) = \det(\phi_X(F_5)^3) = -1$.

6. *Proof of Theorem 1.3*

Let $\mathcal{X} = \operatorname{Proj}(\mathbb{Z}[x,y,z,w]/(f))$; since

$$f \equiv x^6+x^3y^3+xy^5+x^3yz+2x^2y^2z+2y^4z+2xyz^2+z^3+w^2 \pmod 3,$$

we find that $\mathcal{X}_{\mathbb{F}_3}$ is the del Pezzo surface of degree 1 from Example 4.1. In particular, $\phi_{\mathcal{X}_{\mathbb{F}_3}}(F_3)$ has order 7. Since

$$\begin{aligned} f \equiv\ & 3x^5y+4x^4y^2+3x^3y^3+2x^2y^4+4xy^5+4x^4z \\ & +2x^3yz+3x^2y^2z+4xy^3z+3y^4z+z^3+w^2 \pmod 5, \end{aligned}$$

we find that $\mathcal{X}_{\mathbb{F}_5}$ is the del Pezzo surface of degree 1 from Example 4.2. In particular, $\phi_{\mathcal{X}_{\mathbb{F}_5}}(F_5)$ has order 6 and determinant -1, and $\phi_{\mathcal{X}_{\mathbb{F}_5}}(F_5)^2$ has trace 5. Since

$$f \equiv 5x^6+5y^6+z^3+w^2 \pmod 7,$$

we find that $\mathcal{X}_{\mathbb{F}_7}$ is isomorphic to the del Pezzo surface of degree 1 from Lemma 5.3; thus $\phi_{\mathcal{X}_{\mathbb{F}_7}}(F_7)$ has order 3 and trace -4.

Let S be a finite set of primes such that $\mathcal{X}' := \mathcal{X}_{\mathbb{Z}[S^{-1}]}$ is smooth over $\operatorname{Spec}\mathbb{Z}[S^{-1}]$, where $\mathbb{Z}[S^{-1}]$ is the ring of S-units in $\mathbb{Q}$. Since $\mathcal{X}$ has smooth fibers at 3, 5 and 7, we may assume that S is chosen such that $3,5,7 \notin S$. Note that $X = \mathcal{X}'_{\mathbb{Q}}$ is smooth, so it is a del Pezzo surface of degree 1 by Proposition 2.3. By Proposition 3.2, we deduce that $\phi_X\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{O}(K_X^{\perp})$ is surjective.

To prove the final statement of the theorem, it suffices to show that for any number field $k \subseteq \overline{\mathbb{Q}}$, we may find an f such that $L_X \cap k = \mathbb{Q}$. Let $k_1,\dots,k_m$ be all the subfields of k except for $\mathbb{Q}$. By the Chebotarev density theorem, there are distinct rational primes $p_1,\dots,p_m$ greater than 7 such that p_i does not split completely in k_i.

For each i, choose 8 points of $\mathbb{P}^2(\mathbb{F}_{p_i})$ that are in general position; blowing them up gives a del Pezzo surface X_i of degree 1 defined over $\mathbb{F}_{p_i}$. By Proposition 2.6(i), $\phi_{X_i} = I$.

There is a sextic polynomial $f_i \in \mathbb{F}_{p_i}[x,y,z,w]$ such that X_i is isomorphic to the hypersurface $f_i = 0$ in $\mathbb{P}_{\mathbb{F}_{p_i}}(1,1,2,3)$ (the polynomial can be calculated using the results of §2.5 and §2.6. Now let $f \in \mathbb{Z}[x,y,z,w]$ be a sextic which satisfies (1.3), and for each i satisfies $f \equiv f_i \pmod{p_i}$. There is a finite set S of rational primes such that the scheme $\mathcal{X} := \operatorname{Proj}(\mathbb{Z}[S^{-1}][x,y,z,w]/(f))$ is smooth over $\operatorname{Spec}\mathbb{Z}[S^{-1}]$,

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

and S can be chosen so that $3, 5, 7, p_1, \ldots, p_m \notin S$. We have already proven that $X := \mathcal{X}_{\mathbb{Q}}$ is a del Pezzo surface of degree 1 with surjective homomorphism ϕ_X.

If $L_X \cap k \neq \mathbb{Q}$, then $k_i = L_X \cap k$ for some i. Let $\mathrm{Fr}_{p_i} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be any Frobenius automorphism over p_i. Using Lemma 2.7 and $\phi_{\mathcal{X}_{p_i}}(F_{p_i}) = \phi_{X_i}(F_{p_i}) = I$, one proves that $\phi_X(\mathrm{Fr}_{p_i}) = I$. Therefore p_i splits completely in L_X (and hence also in $L_X \cap k = k_i$). This contradicts the assumption that p_i does not split completely in k_i. We conclude that $L_X \cap k = \mathbb{Q}$.

7. *Elliptic curves*

7.1. *Rational elliptic surfaces*

We summarize, making certain simplifying assumptions, some basic facts about Mordell–Weil lattices of rational elliptic surfaces. A full account of the theory can be found in [17].

Let $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ be an elliptic surface with a fixed section $\mathcal{O}$. Assume that

(1) $\mathcal{E}$ is rational
(2) π has at least one singular fiber, and no reducible fibers (in Shioda's notation, $R = \emptyset$).

Let E be the generic fiber of $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$, which is an elliptic curve over the function field $\overline{\mathbb{Q}}(t)$. There is a natural one-to-one correspondence between the $\overline{\mathbb{Q}}(t)$-points of E and the sections of $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$. The image of the section corresponding to a point $P \in E(\overline{\mathbb{Q}}(t))$ will be denoted by (P); it is a divisor of the surface $\mathcal{E}$.

To each point $P \in E(\overline{\mathbb{Q}}(t))$ we associate a fibral divisor $\Phi_P \in \mathrm{Div}(\mathcal{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that for all fibral $F \in \mathrm{Div}(\mathcal{E})$,

$$((P) - (\mathcal{O}) + \Phi_P, F) = 0$$

(recall an irreducible divisor Γ of $\mathcal{E}$ is *fibral* if $\pi|_\Gamma\colon \Gamma \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ is a constant map — such a divisor always exists, see [20, III.8.3]). Let $\mathrm{NS}(\mathcal{E})$ be the Néron–Severi group of $\mathcal{E}$; in our case, this group is finitely generated and torsion free [17, Theorem 1.2]. The map

$$\begin{aligned} \phi\colon E(\overline{\mathbb{Q}}(t)) &\to \mathrm{NS}(\mathcal{E}) \otimes_{\mathbb{Z}} \mathbb{Q} \\ P &\mapsto (P) - (\mathcal{O}) + \Phi_P \end{aligned}$$

is a group homomorphism with kernel $E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ [17, 8.2]. We define a pairing on $E(\overline{\mathbb{Q}}(t))$ using the intersection pairing of $\mathcal{E}$ as follows:

$$\langle \cdot, \cdot \rangle\colon E(\overline{\mathbb{Q}}(t)) \times E(\overline{\mathbb{Q}}(t)) \to \mathbb{Q}, \quad \langle P, Q \rangle = -(\phi(P), \phi(Q)).$$

This pairing is symmetric, bilinear, and coincides with the canonical height pairing on $E(\overline{\mathbb{Q}}(t))$ [20, III.9.3].

Let T be the subgroup of $\mathrm{NS}(\mathcal{E})$ generated by $(\mathcal{O})$ and all the fibers of $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$. By [17, Theorem 1.3], we have a group isomorphism

$$\beta\colon E(\overline{\mathbb{Q}}(t)) \to \mathrm{NS}(\mathcal{E})/T, \quad P \mapsto (P) \bmod T.$$

Let $T' = (T \otimes \mathbb{Q}) \cap \mathrm{NS}(\mathcal{E})$. We have an isomorphism $\beta\colon E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}} \xrightarrow{\sim} T'/T$ by [17, Corollary 5.3]. Hence there is an isomorphism of lattices

$$\beta\colon E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}} \xrightarrow{\sim} \mathrm{NS}(\mathcal{E})/T'. \tag{7.1}$$

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

Remark 7.1. The isomorphism (7.1) holds without the hypothesis that $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ has no reducible fibers, but the map ϕ is harder to define in this case.

7.2. *Galois actions*

Let $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be an elliptic surface with a fixed section $\mathcal{O}$, such that the elliptic surface $\bar{\pi}\colon \mathcal{E}_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$, obtained by base extension, satisfies the hypotheses (1) and (2) of §7.1. Then the isomorphism of lattices (7.1) respects the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-actions [**17**, proof of 8.13]. Hence $E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ and $\mathrm{NS}(\mathcal{E})/T'$ are also isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

7.3. *Elliptic surfaces associated to del Pezzo surfaces of degree* 1

Let X be a del Pezzo surface of degree 1 over $\mathbb{Q}$. We now describe how, given X, one can obtain a rational elliptic surface. The linear system $|-K_X|$ gives rise to a rational map $f\colon X \dashrightarrow \mathbb{P}^1_{\mathbb{Q}}$ that is regular everywhere except at the anticanonical point O (cf. Lemma 2.5). Blowing up X at O, we obtain a surface $\mathcal{E}$. Composing the blow-up map with f gives a morphism $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$, where almost all of the fibers are non-singular genus 1 curves. The morphism π induces an isomorphism between the exceptional divisor of $\mathcal{E}$ corresponding to O and $\mathbb{P}^1_{\mathbb{Q}}$; we thus have a distinguished section $\mathcal{O}\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathcal{E}$ of π. Therefore, $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ with the section $\mathcal{O}$ is an elliptic surface.

Concretely, if X is given by a smooth sextic

$$w^2 = z^3 + F(x,y)z^2 + G(x,y)z + H(x,y)$$

in $\mathbb{P}_{\mathbb{Q}}(1,1,2,3)$, then the anticanonical point is $O = [0:0:1:1]$. In this case, $\mathcal{E}$ is the subscheme of $\mathbb{P}_{\mathbb{Q}}(1,1,2,3) \times \mathbb{P}^1_{\mathbb{Q}} = \mathrm{Proj}(\mathbb{Q}[x,y,z,w]) \times \mathrm{Proj}(\mathbb{Q}[u,v])$ cut out by the equations

$$w^2 = z^3 + F(x,y)z^2 + G(x,y)z + H(x,y) \quad \text{and} \quad vx - uy = 0. \tag{7.2}$$

The map $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ is then given by $([x:y:z:w],[u:v]) \mapsto [u:v]$. Note that for points away from the exceptional divisor we have $[u:v] = [x:y]$.

Let t be the rational function u/v, thus $x = ty$ on $\mathcal{E}$. The generic fiber of π is the curve

$$E\colon w^2 = z^3 + y^2F(t,1)z^2 + y^4G(t,1)z + y^6H(t,1) \tag{7.3}$$

in $\mathrm{Proj}(\mathbb{Q}(t)[y,z,w])$. On the *affine* chart $\mathrm{Spec}(\mathbb{Q}(t)[z/y^2, w/y^3])$ of this weighted ambient space, the curve (7.3) is isomorphic to the affine curve

$$(w/y^3)^2 = (z/y^2)^3 + F(t,1)(z/y^2)^2 + G(t,1)(z/y^2) + H(t,1).$$

Relabelling the variables, we find that the elliptic curve $E/\mathbb{Q}(t)$ is given by the Weierstrass model

$$y^2 = x^3 + F(t,1)x^2 + G(t,1)x + H(t,1).$$

7.4. *Proof of Theorem* 1.1

Let X be a del Pezzo surface as in Theorem 1.3. Let $\pi\colon \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be the elliptic surface obtained by blowing up the anticanonical point of X (see §7.3). The generic fiber of this surface is the elliptic curve $E/\mathbb{Q}(t)$ in the statement of the theorem.

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

Let $\bar{\pi}\colon \mathcal{E}_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ be the base extension of π by $\operatorname{Spec}\overline{\mathbb{Q}} \to \operatorname{Spec}\mathbb{Q}$. The following properties hold:

(1) the surface $\mathcal{E}_{\overline{\mathbb{Q}}}$ is rational (since it is isomorphic to a blow-up of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ at 9 points).

(2) $\bar{\pi}$ has at least one singular fiber (otherwise $\mathcal{E}$ has constant j-invariant [**20**, Ex. 3.35(c)]). Moreover, the fibers of $\bar{\pi}\colon \mathcal{E}_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ are irreducible: using the blow-up model (7.2) of $\mathcal{E}$, the reader may verify that the fiber above the point $[u : v] \in \mathbb{P}^1_{\overline{\mathbb{Q}}}$ is isomorphic to the projectivization of the irreducible curve

$$y^2 = x^3 + F(u,v)x^2 + G(u,v)x + H(u,v).$$

We may thus apply §7.1 to obtain an isomorphism

$$E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}} \xrightarrow{\sim} \mathrm{NS}(\mathcal{E}_{\overline{\mathbb{Q}}})/T'.$$

Furthermore, this isomorphism respects the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (see §7.2). On the other hand, the lattice $K_X^{\perp}$ is isomorphic to $\mathrm{NS}(\mathcal{E}_{\overline{\mathbb{Q}}})/T'$ via the composition of maps

$$K_X^{\perp} \to \mathrm{NS}(\mathcal{E}_{\overline{\mathbb{Q}}}) \to \mathrm{NS}(\mathcal{E}_{\overline{\mathbb{Q}}})/T',$$

where the first map is induced by pullback of divisors along the blow-up map, and the second is the natural quotient map. Therefore we have isomorphisms

$$K_X^{\perp} \cong \mathrm{NS}(\mathcal{E}_{\overline{\mathbb{Q}}})/T' \cong E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$$

of lattices and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Now, $K_X^{\perp}$ is an E_8-lattice with maximal Galois action $W(E_8)$, because X has maximal Galois action on its geometric Picard group by Theorem 1.3. To complete the proof of the theorem, it remains to check that $E(\overline{\mathbb{Q}}(t))_{\mathrm{tors}} = 0$; this is true by [**17**, Theorem 10.4]. □

References

1. N. Berry, A. Dubickas, N. D. Elkies, B. Poonen and C. Smyth, 'The conjugate dimension of algebraic numbers', *Q. J. Math.* 55 (2004) 237–252. 146

2. W. Bosma, J. Cannon, and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–265. 148

3. N. Bourbaki, *Lie groups and Lie algebras* (Springer, Berlin, 2002) Chapters 4–6. 155

4. R. W. Carter, 'Conjugacy classes in the Weyl group', *Compositio Math.* 25 (1972) 1–59. 156

5. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups* (Oxford University Press, Eynsham, 1985). 155

6. P. Cragnolini and P. A. Oliverio, 'Lines on del Pezzo surfaces with $K_S^2 = 1$ in characteristic $\neq 2$', *Comm. Algebra* 27 (1999) 1197–1206. 150

7. M. Demazure, 'Surfaces de Del Pezzo II, III, IV, V', *Séminaire sur les singularités des surfaces*, eds. M. Demazure, H. C. Pinkham and B. Teissier, Lecture Notes in Math. 777 (Springer, Berlin, 1980) 23–69. 148, 149, 151

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press

8. I. Dolgachev, 'Weighted projective varieties', *Group actions and vector fields*, Vancouver, B.C., 1981, Lecture Notes in Math. 956 (Springer, Berlin, 1982) 34–71. 149

9. T. Ekedahl, 'An effective version of Hilbert's irreducibility theorem', *Séminaire de théorie des nombres, Paris 1988–1989*, Progr. Math. 91 (Birkhäuser, Boston, 1990) 241–249. 145

10. R. Erné, 'Construction of a del Pezzo surface with maximal Galois action on its Picard group', *J. Pure Appl. Algebra* 97 (1994) 15–27. 145

11. W. Fulton, *Intersection Theory* (Springer, Berlin, 1998). 153

12. R. Hartshorne, *Algebraic Geometry* (Springer, New York, 1977). 152, 153

13. F. Jouve, E. Kowalski and D. Zywina, 'An explicit integral polynomial whose splitting field has Galois group $W(E_8)$', *J. Théor. Nombres Bordeaux*, to appear. 145

14. J. Kollár, *Rational curves on algebraic varieties* (Springer, Berlin, 1996). 148, 150

15. J. Kollár, K. E. Smith and A. Corti, *Rational and nearly rational varieties* (Cambridge University Press, Cambridge, 2004). 151

16. Yu. I. Manin *Cubic forms: Algebra, geometry, arithmetic* (North-Holland, Amsterdam, 1986). 148, 149, 159

17. T. Shioda, 'On the Mordell–Weil lattices', *Comment. Math. Univ. St. Paul.* 39 (1990) 211–240. 145, 162, 163, 164

18. T. Shioda, 'Theory of Mordell–Weil lattices', *Proceedings of the International Congress of Mathematicians*, Kyoto, 1990, vol. I, II (Math. Soc. Japan, Tokyo, 1991) 473–489. 145, 146

19. T. Shioda, 'Mordell–Weil lattices of type E_8 and deformation of singularities', *Prospects in complex geometry*, Lecture Notes in Math. 1468 (Springer, Berlin, 1991) 177–202. 145

20. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves* (Springer, New York, 1994). 144, 162, 164

21. Yu. G. Zarhin, 'Del Pezzo surfaces of degree 1 and Jacobians', *Math. Ann.* 340 (2008) 407–435. 146, 147

Anthony Várilly-Alvarado varilly@math.berkeley.edu

Department of Mathematics
University of California
Berkeley, CA 94720-3840
USA

David Zywina zywina@math.upenn.edu

Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA

https://doi.org/10.1112/S1461157000001479 Published online by Cambridge University Press