Arithmetic of affine del Pezzo surfaces
Lyczak, J.T.

Author: Lyczak, J.T.
Title: Arithmetic of affine del Pezzo surfaces
Issue Date: 2019-10-01

Chapter 4

Order 5 obstructions to the integral Hasse principle

In this chapter we will discuss new examples of the Brauer–Manin obstruction to the integral Hasse principle. The most remarkable property of these obstructions is that they come from a single element of order 5. This is exceptional since all other known examples of the Brauer–Manin obstructions use only elements of order 2 and 3.

The results in this chapter all use an element of order 5 which can occur in the Brauer group of ample log K3 surfaces of dP_5 type described in Proposition 3.2.5. So let us write $U = X \backslash C$ where X is an ordinary del Pezzo surface of degree 5 over $\mathbb{Q}$ and C is an effective anticanonical divisor. In Proposition 3.2.5 we have seen that U has a non-trivial algebraic Brauer group for a specific action of the absolute Galois group G_k on the geometric Picard group $\operatorname{Pic} \bar{X}$. We will first study this action and the induced action on the -1-classes. We will see for example that $\operatorname{Pic} \bar{X}$ will be isomorphic to $\operatorname{Pic} X_K$ for a specific number field K of degree 5.

The next step in producing our examples is recovering an ample log K3 surface U over $\mathbb{Q}$ from this action or even from only its splitting field K. We use the construction described in [29] to first construct a del Pezzo surface X of degree 5 over $\mathbb{Q}$. We start off with a conic Γ_0 on the projective plane $\mathbb{P}^2_{\mathbb{Q}}$ and five distinct geometric points P_i on the conic with a specific action of Galois. We blow up these five points and recover an ordinary del Pezzo surface $\beta\colon B \to \mathbb{P}^2_{\mathbb{Q}}$ of degree 4. The strict transform Γ of Γ_0 along the blowup morphism β is a -1-curve on B. We contract this curve along the morphism $B \to X$ to obtain an ordinary del Pezzo surface of degree 5 over $\mathbb{Q}$. Now for any smooth anticanonical curve $C \subseteq X$ we see that $U = X \backslash C$ is an ample log K3 surface with an algebraic Brauer group modulo constants of order 5. These are the surfaces for which we will consider the set of integral points.

However, U is a surface over $\mathbb{Q}$ and it does not make sense to consider $\mathbb{Z}$-

points; the set of integral points on a scheme over a number field depends on the choice of model over the ring of integers. We can obtain a model $\mathcal{U}/\mathbb{Z}$ for U in the following natural way: the anticanonical map embeds the ordinary del Pezzo surface X into $\mathbb{P}^5_{\mathbb{Q}}$ which restricts to an embedding $U \to \mathbb{A}^5_{\mathbb{Q}}$. Consider a set of equations defining the subscheme $U \subseteq \mathbb{A}^5_{\mathbb{Q}}$. We rescale these equations such that they have integral coefficients. These equations now define a subscheme $\mathcal{U} \subseteq \mathbb{A}^5_{\mathbb{Z}}$ which is affine over $\mathbb{Z}$.

In order to study the geometry of the model $\mathcal{U}$ it is useful to have another description. In the above construction of $\mathcal{X}$ we first blew up points and contracted a curve defined over $\mathbb{Q}$ and then passed to a scheme over the integers. We will now reverse the steps of this process: first we pass over to the integers and then we blow up the projective plane over the integers in a subscheme which is flat of relative dimension zero over $\mathbb{Z}$. We obtain a scheme $\mathcal{B}$ over $\mathbb{Z}$ whose fibres are peculiar del Pezzo surfaces over either a finite field or the rational numbers. We proceed by contracting a subscheme $\Gamma \subseteq \mathcal{B}$ over $\mathbb{Z}$ to obtain a scheme $\mathcal{X}$ over $\mathbb{Z}$. This does not mean that Γ is contracted to a single point, but rather that the image of Γ in $\mathcal{X}$ is a relative point of $\mathcal{X} \to \mathbb{Z}$. This implies that a fibre of Γ over a prime $\ell \in \mathbb{Z}$ is a curve of negative self-intersection on a peculiar del Pezzo surface $\mathcal{B}_\ell$, and the morphism $\mathcal{B}_\ell \to \mathcal{X}_\ell$ is the contraction of this curve to obtain another del Pezzo surface. The scheme $\mathcal{X}$ will naturally embed in $\mathbb{P}^5_{\mathbb{Z}}$. Now consider the complement $\mathcal{U} \subseteq \mathbb{A}^5_{\mathbb{Z}}$ of a hyperplane section $\mathcal{H} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ in $\mathcal{X}$.

We will show that this relative affine surface $\mathcal{U}/\mathbb{Z}$ is naturally isomorphic to the subscheme $\mathcal{U} \subseteq \mathbb{A}^5_{\mathbb{Z}}$ constructed above. The first construction gives us explicit equations while the second construction makes it easier to understand the geometry of the closed fibres of $\mathcal{U}$ over $\mathbb{Z}$.

Now that we have constructed a scheme $\mathcal{U}$ which is affine over $\mathbb{Z}$ we can consider the integral points on $\mathcal{U}$. Using our explicit geometric construction we study the fibres of $\mathcal{U}$ over $\mathbb{Z}$; almost all of which are ample log K3 surfaces of dP_5 type. We proceed by computing the invariant map at a prime ℓ using our description of the fibre $\mathcal{U}_\ell$ and the factorization of ℓ in the number field K. By combining all these local results we obtain several examples of order 5 Brauer–Manin obstructions to the integral Hasse principle.

4.1 The interesting Galois action

In this chapter we will construct an affine scheme $\mathcal{U} \subseteq \mathbb{A}^5_{\mathbb{Z}}$ which has a Brauer–Manin obstruction to the integral Hasse principle. This obstruction is given by an element of order 5 in the Brauer group $\operatorname{Br} U$ of the generic fibre $U = \mathcal{U}_{\mathbb{Q}}$. In all our examples we will construct $\mathcal{U}$ in such a way such that $U = X \backslash C$ is an ample log K3 surface of dP_5 type. The existence of an element of order 5 in $\operatorname{Br} U / \operatorname{Br} \mathbb{Q}$ is then implied by Proposition 3.2.5 for a specific action of $G_{\mathbb{Q}}$ on $\operatorname{Pic} \bar{X}$.

Let X be any del Pezzo surface of degree 5 over a field k. We recall some results about the action of Galois on the geometric Picard group $\operatorname{Pic} \bar{X}$. We defined

W_4 as the group of intersection-preserving automorphisms of $\operatorname{Pic}\bar{X}$ which map the anticanonical class to itself. If C is geometrically irreducible this induces an action of W_4 on $\operatorname{Pic}\bar{U}$. In Proposition 3.2.5 we have seen that there is a special conjugacy class $\mathcal{W}$ of subgroups of W_4. This conjugacy class $\mathcal{W}$ is precisely the set of all subgroups of $W \subseteq W_4$ with the property that the cohomology group $\mathrm{H}^1(W, \operatorname{Pic}\bar{U})$ is non-trivial. We will study the action of such a subgroup W on $\operatorname{Pic}\bar{X}$, $\operatorname{Pic}\bar{U}$ and the -1-curves on X more closely in this section. Let us first define this interesting action.

DEFINITION 4.1.1. Let X be an ordinary del Pezzo surface of degree 5 over a field k. Let K be the minimal Galois extension of k over which all -1-curves on X are defined. We say that X is *interesting* if $[K\colon k] = 5$. A log K3 surface of dP_5 type $U = X \backslash C$ is called *interesting* if X is an interesting del Pezzo surface and C is geometrically irreducible.

The field K is called the *splitting field* of the interesting surfaces X and U.

Consider an interesting log K3 surface $U = X \backslash C$. By definition of a log K3 surface we see that C is smooth. The curve C is also geometrically irreducible since U is interesting. The results in this chapter are also true for the complement of a geometrically irreducible anticanonical curve C on an ordinary del Pezzo surface X of degree 5. To be able to use the language of log K3 surface we do keep the superfluous condition that C is smooth.

The following lemma shows that an interesting action corresponds to a unique conjugacy class of subgroups of W_4.

LEMMA 4.1.2. *Consider an interesting del Pezzo surface X over a field k. The action of G_k on* $\operatorname{Pic}\bar{X}$ *is uniquely determined up to conjugacy.*

On an interesting del Pezzo surface there are two Galois orbits of geometric -1-curves, each of size 5. *The sum of the -1-curves in one such orbit is an anticanonical divisor.*

Proof. Let K be the minimal Galois extension of k such that all -1-curves on X are defined over K. Since X is interesting the extension K/k is of degree 5.

We have seen in Proposition 2.3.1 that there is a basis $(L_0, L_1, L_2, L_3, L_4)$ of $\operatorname{Pic}\bar{X} \cong \mathbb{Z}^5$ such that $L_0^2 = 1$, $L_0 \cdot L_i = 0$ and $L_i^2 = -1$ for $i \neq 0$. The -1-classes are the classes L_i for $i \neq 0$ and $L_{ij} := L_0 - L_i - L_j$ for $1 \leq i < j \leq 4$. The intersection graph of the -1-curves on a generalized del Pezzo surface of degree 5 is the so-called Petersen graph shown in Figure II.

Let us first prove that $\mathrm{Gal}(K/k)$ does not fix any of the ten geometric -1-curves. If it does fix a -1-curve L consider the three -1-curves L intersects. The Galois action then permutes these three -1-curves since the action preserves the intersection pairing. However there are no non-trivial group homomorphisms $\mathbb{Z}/5\mathbb{Z} \to S_3$ so the action of Galois actually fixes these three -1-curves. Since the graph in Figure II is connected we conclude that all geometric -1-curves are defined over k contradicting the minimality of K. So no geometric -1-curve is fixed by G_k and there must be two orbits of size 5. After choosing a possible different basis of $\operatorname{Pic}\bar{X}$ we see that these two orbits are the two regular pentagons

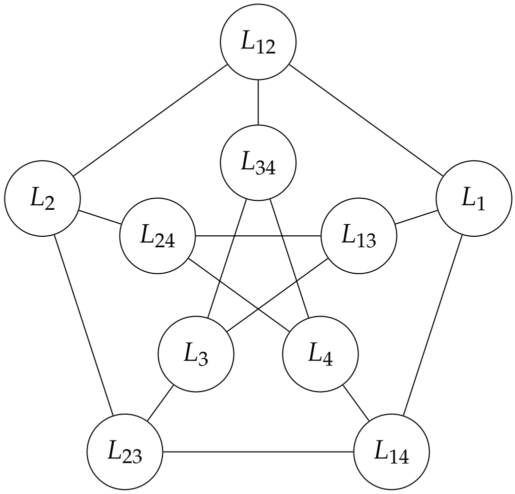

Figure II: The intersection graph of -1-curves on a generalized del Pezzo surface of degree 5.

in Figure II and that there is a $\sigma \in \mathrm{Gal}(K/k)$ which acts on the outer pentagon by rotating counter-clockwise. Since σ preserves the intersection pairing it will also rotate the inner pentagon counter-clockwise. This determines the action of σ on the -1-classes

$$L_1 \mapsto L_{12} \mapsto L_2 \mapsto L_{23} \mapsto L_{14} \mapsto L_1,$$
$$L_3 \mapsto L_4 \mapsto L_{13} \mapsto L_{34} \mapsto L_{24} \mapsto L_3.$$

This proves that $L_0 = L_{12} + L_1 + L_2$ gets mapped to $2L_0 - L_1 - L_2 - L_3$. Since a different choice of such a basis differs by an automorphism in W_4 by Proposition 2.3.5 this determines an action of G_k on $\operatorname{Pic} \bar{X}$ up to conjugacy.

For the last statement one needs to check that both the divisor classes of $L_1 + L_{12} + L_2 + L_{23} + L_{14}$ and $L_3 + L_4 + L_{13} + L_{34} + L_{24}$ equal the anticanonical class $3L_0 - L_1 - L_2 - L_3 - L_4$. □

If we consider a log K3 surface of geometrically irreducible dP_5 type over a number field k we can compute its algebraic Brauer group modulo constants using Proposition 1.6.5. The following proposition shows that the action of G_k on $\operatorname{Pic} \bar{X}$ is interesting precisely when $\mathrm{Br}_1 U / \mathrm{Br}\, k$ is non-trivial. We conclude that the actions mentioned in Proposition 3.2.5 are precisely the interesting ones.

PROPOSITION 4.1.3. *Let $U = X \backslash C$ be a log K3 surface of geometrically irreducible dP_5 type over a number field k. We have*

$$\mathrm{Br}_1 U / \mathrm{Br}\, k \cong \begin{cases} \mathbb{Z}/5\mathbb{Z} & \text{if } U \text{ is interesting;} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let the action of G_k on $\operatorname{Pic} \bar{X}$ factor through the minimal subgroup W of W_4. Lemma 3.2.2 states that $\operatorname{Br}_1 U / \operatorname{Br} k$ only depends on the conjugacy class of $W \subseteq W_4$ and that for precisely one conjugacy class of subgroups of W_4 the algebraic Brauer group modulo constants is non-trivial. We have seen that every interesting action of G_k on $\operatorname{Pic} \bar{X}$ factors through the same conjugacy class of subgroups of W_4 of order 5. This means that it will suffice to prove that $\operatorname{Br}_1 U / \operatorname{Br} k$ is non-trivial for interesting del Pezzo surfaces. So suppose that X is an interesting del Pezzo surface over k. We will fix a basis $(L_0, L_1, L_2, L_3, L_4)$ of $\operatorname{Pic} \bar{X}$ as in the proof of Lemma 4.1.2.

In general, since $C \subseteq X$ is geometrically irreducible we find the following exact sequence of Galois modules

$$0 \to \mathbb{Z} \xrightarrow{j} \operatorname{Pic} \bar{X} \to \operatorname{Pic} \bar{U} \to 0,$$

where j maps n to $-nK_X$. This shows that $\operatorname{Pic} \bar{U} \cong \operatorname{Pic} \bar{X}/\mathbb{Z}C \cong \mathbb{Z}^4$, since the anticanonical divisor class $-K_X = 3L_0 - L_1 - L_2 - L_3$ is primitive. So $\operatorname{Pic} \bar{U}$ is torsion free and from the inflation–restriction sequence we conclude that the inflation homomorphism induces an isomorphism

$$\mathrm{H}^1(\operatorname{Gal}(K/k), \operatorname{Pic} U_K) \xrightarrow{\inf} \mathrm{H}^1(G_k, \operatorname{Pic} \bar{U}).$$

Given the basis of $\operatorname{Pic} \bar{X}$ we saw in the proof of Lemma 4.1.2 the specific action of a generator $\sigma \in \operatorname{Gal}(K/k)$ on $\operatorname{Pic} \bar{X}$. We will compute the action of σ on the quotient $\operatorname{Pic} \bar{U}$ of $\operatorname{Pic} \bar{X}$. The classes $[L_0]$, $[L_1]$, $[L_2]$ and $[L_3]$ in $\operatorname{Pic} U_K$ form a basis and in this basis the class of L_4 becomes $[L_4] = 3[L_0] - [L_1] - [L_2] - [L_3]$. So σ acts on $\operatorname{Pic} \bar{U}$ as

$$\sigma = \begin{pmatrix} 2 & 1 & 1 & 3 \\ -1 & -1 & 0 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & 0 & -1 & -1 \end{pmatrix}$$

By results on group cohomology of cyclic groups [58, Theorem 6.2.2] we see that we get

$$\mathrm{H}^1(G, \operatorname{Pic} \bar{U}) \cong \ker(1 + \sigma + \sigma^2 + \sigma^3 + \sigma^4)/\operatorname{Im}(1 - \sigma).$$

Since $1 + \sigma + \sigma^2 + \sigma^3 + \sigma^4 = 0$ and the image of $1 - \sigma$ is generated by $(1, 0, 0, 2)$, $(0, 1, 0, 4)$, $(0, 0, 1, 4)$ and $(0, 0, 0, 5)$ we find

$$\operatorname{Br}_1 U / \operatorname{Br} k \cong \mathbb{Z}/5\mathbb{Z}. \qquad \square$$

Consider an interesting log K3 surface U. On the compactification X of U we have three important effective anticanonical divisors. First of all $C = X \backslash U$, but also the two divisors supported on -1-curves as described in Lemma 4.1.2. We will associate to these effective divisors anticanonical sections using [33, II, Proposition 7.7b] and we will use these elements to construct explicit generators of $\operatorname{Br}_1 U / \operatorname{Br} k$ for an interesting log K3 surface $U = X \backslash C$.

LEMMA 4.1.4. *Let $U = X\backslash C$ be an interesting log K3 surface over a number field k. Let K be the corresponding Galois extension of degree 5 of k. Fix a generator σ of* $\mathrm{Gal}(K/k) \cong \mathbb{Z}/5\mathbb{Z}$. *Let $h \in \mathrm{H}^0(X, \omega_X^\vee)$ be a global section whose divisor of zeroes is C, and let l_1 and l_2 be sections in $\mathrm{H}^0(X, \omega_X^\vee)$ associated to the two anticanonical divisors supported in geometric -1-curves from Lemma 4.1.2.*

The cyclic $\kappa(X)$-algebras

$$\left(\frac{l_1}{h}, \sigma\right) \quad \text{and} \quad \left(\frac{l_2}{h}, \sigma\right)$$

are similar over $\kappa(X)$, their class lies in the subgroup $\mathrm{Br}\, U \subseteq \mathrm{Br}\, \kappa(X)$ and generates $\mathrm{Br}_1\, U / \mathrm{Br}\, k$.

Proof. As $\mathrm{div}_U(\frac{l_1}{h})$ and $\mathrm{div}_U(\frac{l_2}{h})$ are orbits of -1-curves defined over K it follows from Lemma 1.7.3 that the cyclic algebras lie in the subgroup $\mathrm{Br}\, U$. From Proposition 1.3.2 we see that the algebras $\left(\frac{l_1}{h}, \sigma\right) \otimes \left(\frac{l_2}{h}, \sigma\right)^{\mathrm{opp}}$ and $\left(\frac{l_1}{l_2}, \sigma\right)$ are similar. Now $\mathrm{div}_U(\frac{l_1}{l_2})$ is the norm of a principal divisor on U since this is even the case on X. Indeed, the divisors $L_{14} + L_1 - L_2$ and L_{24} are linearly equivalent on X, and their norms $\mathrm{Nm}_{K/k}(L_{14} + L_1 - L_2)$ and $\mathrm{Nm}_{K/k}(L_{24})$ are the divisors of zeroes of l_1 and l_2. It follows again from Lemma 1.7.3 that $\left(\frac{l_1}{l_2}, \sigma\right)$ is trivial in $\mathrm{Br}\, U$, and hence that the two cyclic algebras lie in the same class.

We have seen in Proposition 1.3.2 that $\mathcal{A}$ is split by the degree 5 extension K. Now Corollary 1.2.13 implies that $\mathcal{A}$ is either trivial or of order 5. Suppose that the class of $\mathcal{A}$ is trivial. Then by Lemma 1.7.3 any -1-curve L on U_K in the support of $\mathrm{div}_U l_1$ is principal, i.e. there is a $g \in \kappa(U_K)$ such that $\mathrm{div}_U g = L$. Consider g as a function on X. Then $\mathrm{div}_X g = L + nC$ for some non-negative integer n, since C is geometrically irreducible. We conclude that

$$0 = K_X \cdot \mathrm{div}_X g = K_X \cdot L + n K_X \cdot C = -1 + 5n,$$

which is a contradiction. $\square$

The anticanonical sections l_1 and l_2 are so important we will repeat their definition.

DEFINITION 4.1.5. Let $X \subseteq \mathbb{P}^5_k$ be an anticanonically embedded interesting del Pezzo surface of degree 5. Let $l_1, l_2 \in \mathcal{O}_{\mathbb{P}^5_k}(1)$ be the linear forms over k in six variables which restrict to the anticanonical sections supported on geometric -1-curves from Lemma 4.1.4.

Note that l_1 and l_2 are only defined up multiplication by an element of $k^\times$. From now on we will denote the class in Lemma 4.1.4 by $\mathcal{A} \in \mathrm{Br}_1(U)$ which is uniquely defined up to an element in $\mathrm{Br}\, k$. Fix for the moment an interesting del Pezzo surface X. We will consider the class $\mathcal{A}_h$ on U_h as h varies over all hyperplane sections. We have seen that $\mathcal{A}_h$ is of order 5 if h cuts out a geometrically irreducible curve. The next lemma shows that this only fails for specific choices of h.

LEMMA 4.1.6. *Let $X \subseteq \mathbb{P}^5_k$ be an interesting del Pezzo surface over a field k. A hyperplane section given by the vanishing of an $h \in \mathrm{H}^0(\mathbb{P}^5_k, \mathcal{O}(1))$ fails to be geometrically irreducible if and only if h is a scalar multiple of either l_1 or l_2.*

Proof. Consider a hyperplane section $C \subseteq X$. Let D be a k-irreducible component of C and consider a geometric -1-curve L. It follows that $L \cdot \bar{D} = \sigma(L) \cdot \bar{D}$ and as the Galois orbit of L is an anticanonical divisor, we find

$$5 \geq -K_X \cdot D = 5L \cdot \bar{D} > 0,$$

since the degree of $D \subseteq \mathbb{P}^5_k$ is positive and at most the degree of C, which equals 5. This proves that $L \cdot \bar{D} = 1$ for all geometric -1-curves L and hence $C - D$ is an effective divisor of degree 0. We conclude that $C = D$ and this proves that any anticanonical section C is irreducible over k.

If C is not geometrically irreducible, then it must have at least two geometrically irreducible components of the same degree d since the Galois group acts on the set of geometrically irreducible components of C. Since C is of degree 5 we find $2d \leq 5$ and hence d is either 1 or 2. But in both cases we see that C contains a geometrically irreducible curve of degree 1, which must be a geometric -1-curve L. Then C also contains all conjugates of L and hence C is the Galois orbit of a geometric -1-curve. This proves that C is defined by the vanishing of either l_1 or l_2. □

4.2 Constructions of degree 5 del Pezzo surfaces

We have seen that the action of Galois on the -1-curves on an ordinary del Pezzo surface X over a field k determines many arithmetic properties of X. In this section we will describe the results in [29] which state that for ordinary del Pezzo surfaces of degree 5 a stronger result is true. Namely, there is a correspondence between isomorphism classes of ordinary del Pezzo surfaces X over k and conjugacy classes of group homomorphisms $G_k \to W_4$.

An isomorphism class of X over k induces an action of G_k on $\operatorname{Pic} \bar{X}$. Now let W be the minimal subgroup of the Weyl group W_4 such that the action of G_k on the geometric Picard group factors through W. This gives us a homomorphism from $G_k \to W \to W_4$. We will follow [29] in constructing an ordinary del Pezzo surface X of degree 5 over a field k starting from a homomorphism $G_k \to W_4$. Let us first show that W_4 is a well understood finite group.

LEMMA 4.2.1. *The group W_4 is isomorphic to S_5 and this isomorphism is unique up to conjugacy.*

Proof. We have seen in Proposition 2.3.5 that W_4 is isomorphic to the automorphism group of the intersection graph of the -1-classes of a generalized del Pezzo surface of degree 5. This graph is the Petersen graph shown in Figure II. The computation of the automorphism group of this graph is more easily done using the following interpretation. Consider the graph whose vertices are the ten subsets $\{a, b\} \in \{1, 2, 3, 4, 5\}$ with precisely two elements. The vertices $\{a, b\}$ and $\{c, d\}$ are connected precisely if the two sets are disjoint. This graph is easily seen to be isomorphic to the Petersen graph.

It is clear that the elements of S_5 induce different natural automorphisms on this graph. Also, from an automorphism of the graph we can recover a permutation of $\{1, 2, 3, 4, 5\}$; for example, the image of the element 1 is the unique element in the intersections of the images of $\{1, 2\}$ and $\{1, 3\}$.

The last statement follows from the fact that every automorphism of S_5 is inner. $\square$

Now fix an isomorphism $W_4 \cong S_5$. We have remarked that such an isomorphism is unique up to conjugation. For our applications this will mean that the actual choice of this isomorphism does not matter as long we consistently use the same one.

DEFINITION 4.2.2. Let k be a field. Let $\xi\colon G_k \to S_5$ be a group homomorphism and let $m \in k[T]$ be a monic and square free polynomial of degree 5 with roots α_i for $1 \leq i \leq 5$. We say that m is a *seed* for ξ if $\sigma \in G_k$ acts on $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ as $\xi(\sigma)$ acts on the set of indices $\{1, 2, 3, 4, 5\}$.

The following results shows that seeds always exist.

LEMMA 4.2.3. *In the notation of Definition 4.2.2, there is a seed $m \in k[T]$ for each group homomorphism $\xi\colon G_k \to S_5$.*

Proof. See Lemma 15 in [29]. $\square$

Note that whether m is a seed of ξ depends on the indexing of the roots of m. A different choice for the indices will produce a seed for an S_5-conjugate of ξ. This shows that we should consider m to be a seed of the S_5-conjugacy class of group homomorphisms $G_k \to S_5$.

Also note that we are actually interested in homomorphisms from G_k to W_4. Using an isomorphism between W_4 and S_5, which is unique up to conjugacy, we see can define a *seed* of a conjugacy class of homomorphisms $G_k \to W_4$.

We can use this terminology to produce ordinary del Pezzo surface X of degree 5.

Step 1. Suppose that a homomorphism $\xi\colon G_k \to S_5$ is given. Fix a seed m for ξ.
Step 2. Consider the projective plane $\mathbb{P}^2_k$ over k together with the five distinct points $P_i = (\alpha_i\colon \alpha_i^2\colon 1)$. Let $Q \subseteq k[x, y, z]$ be the subset of quintic homogeneous polynomials which are singular at each P_i.

LEMMA 4.2.4. *The k-linear subspace $Q \subseteq k[x, y, z]$ is of dimension* 6.

Proof. See Theorem 5 in [29]. $\square$

Step 3. Fix a k-basis $q_0, q_1, \ldots, q_5 \in Q$ and define a rational map $\vartheta\colon \mathbb{P}^2_k \dashrightarrow \mathbb{P}^5_k$ by $[x\colon y\colon z] \mapsto [q_i(x, y, z)]_i$. Let $X \subseteq \mathbb{P}^5_k$ be the closure of the image of ϑ.

PROPOSITION 4.2.5. *The scheme $X \subseteq \mathbb{P}^5_k$ over k constructed above is an ordinary del Pezzo surface of degree 5 over k which is anticanonically embedded. The morphism ϑ defines a birational morphism $\mathbb{P}^2_k \to X$ which we will also denote by ϑ.*

We will call X the ordinary del Pezzo surface of degree 5 over k associated to the seed m.

Proof. See Theorem 5 in [29]. □

We now have produced an ordinary del Pezzo surface of degree 5 over k from a homomorphism $G_k \to S_5$. If we on the other hand start off with an ordinary del Pezzo surface X of degree 5 over a field k we have seen that the action of G_k on $\operatorname{Pic} \bar{X}$ defines a homomorphism $G_k \to S_5$. We would like these maps to be inverses to each other. One sees that for this to be true one would have to consider isomorphism classes of ordinary del Pezzo surfaces, because isomorphic surfaces have isomorphic actions of Galois on the set of -1-curves. Also, seeds can be defined for S_5-conjugacy classes of group homomorphisms $G_k \to S_5$. The following proposition shows that up to these equivalences the maps constructed above are actually inverses to each other.

Recall that we have fixed an isomorphism between S_5 and the automorphism group of $\operatorname{Pic} \bar{X}$.

PROPOSITION 4.2.6. *Let k be a perfect field. The map from the set of isomorphism classes of ordinary del Pezzo surfaces of degree 5 over k to the set of conjugacy classes of homomorphisms $G_k \to S_5$ defined by sending an ordinary del Pezzo surface X over k to the action of G_k on the -1-curves is a bijection.*

The inverse is given by mapping a homomorphism $\xi \colon G_k \to S_5$ to the isomorphism class of the ordinary del Pezzo surface of degree 5 over k associated to a seed of ξ.

Proof. See Lemma 14 in [29]. □

We will now describe another construction of a del Pezzo surface X' using a seed m. In Proposition 4.2.9 we will see that X' is isomorphic to the del Pezzo surface X associated m. For now we will write X and X' to distinguish the two constructions. Again we consider the five distinct points $P_i = (\alpha_i \colon \alpha_i^2 \colon 1)$ on $\mathbb{P}^2_k$ associated to the seed m which lie on a unique conic $\Gamma_0 \subseteq \mathbb{P}^2_k$. Let B be the blow up of $\mathbb{P}^2_k$ in the Galois-invariant set $\{P_i\}$ and let Γ be the strict transform of Γ_0 along $B \to \mathbb{P}^2_k$. By Corollary 2.7.14 B is an ordinary del Pezzo surface of degree 4 over k. Also, $\Gamma \subseteq B$ is a -1-curve by Lemma 2.7.9. If we contract this -1-curve using Proposition 2.2.5 we obtain an ordinary del Pezzo surface X' of degree 5.

Let us make this more precise. We will consider a line $\Lambda_0 \subseteq \mathbb{P}^2_k$ which does not meet any of the points P_i and pull it back to the effective divisor $\Lambda \subseteq B$. A careful study of the proof of Castelnuovo's theorem used in Proposition 2.2.5 shows that the morphism $B \to X'$ which contracts $\Gamma \subseteq B$ is the morphism associated to the complete linear system of the line bundle $\Lambda + 2\Gamma$.

PROPOSITION 4.2.7. *The composition $B \xrightarrow{\beta} \mathbb{P}^2_k \overset{\vartheta}{\dashrightarrow} X \subseteq \mathbb{P}^5_k$ extends to a morphism on the whole of B. This morphism $\rho\colon B \to X \subseteq \mathbb{P}^5_k$ corresponds to the complete linear system of the divisor $\Delta = \Lambda + 2\Gamma$. Furthermore, the only curve contracted by this morphism is Γ.*

Proof. This proposition is proved in the proof of Theorem 5 of [29]. □

Note that Γ_0 is the conic defined by the equation $x^2 = yz$. We will also fix an equation for Λ_0. It is clear that the line $z = 0$ does not meet any of the points P_i. We can now prove the following corollary.

COROLLARY 4.2.8. *The morphism β is a birational morphism and induces an isomorphism $\beta^*\colon \kappa(\mathbb{P}^2_k) \to \kappa(B)$. This isomorphism identifies the following two linear subspaces*

$$\frac{1}{z(x^2 - yz)^2} Q \subseteq \kappa(\mathbb{P}^2_k) \quad \textit{and} \quad \mathrm{H}^0(B, \mathcal{L}(\Delta)) \subseteq \kappa(B).$$

Proof. Define the divisor $\Delta_0 = \Lambda_0 + 2\Gamma_0$ on $\mathbb{P}^2_k$. We see that

$$\beta^*\Delta_0 = \Delta + 2E_\beta$$

where E_β is the sum of the five exceptional curves of the blowup morphism $\beta\colon B \to \mathbb{P}^2_k$. The spaces of global sections $\mathrm{H}^0(\mathbb{P}^2_k, \mathcal{L}(\Delta_0))$ and $\mathrm{H}^0(B, \mathcal{L}(\beta^*\Delta_0))$ embed naturally in the respective function fields $\kappa(\mathbb{P}^2_k)$ and $\kappa(B)$. The isomorphism β^* on these function fields respects these linear subspaces and we have a natural morphism

$$\beta^*\colon \mathrm{H}^0(\mathbb{P}^2_k, \mathcal{L}(\Delta_0)) \to \mathrm{H}^0(B, \mathcal{L}(\beta^*\Delta_0)).$$

By definition we have $Q \subseteq \mathrm{H}^0(\mathbb{P}^2_k, \mathcal{O}(5))$ and the isomorphism $\mathcal{O}(5) \to \mathcal{L}(\Delta_0)$ is uniquely defined up to multiplication by an invertible element of $\mathcal{O}_{\mathbb{P}^2_k}(\mathbb{P}^2_k) = k$. This implies that Q corresponds to the linear subsystem

$$\frac{1}{z(x^2 - yz)^2} Q \subseteq \mathrm{H}^0(\mathbb{P}^2_k, \mathcal{L}(\Delta_0)) \subseteq \kappa(\mathbb{P}^2_k)$$

for any isomorphism $\mathcal{O}(5) \to \mathcal{L}(\Delta_0)$. The morphisms ϑ and ρ are defined by the respective linear systems

$$\frac{1}{z(x^2 - yz)^2} Q \subseteq \mathrm{H}^0(\mathbb{P}^2_k, \mathcal{L}(\Delta_0)) \quad \text{and} \quad \mathrm{H}^0(B, \mathcal{L}(\Delta)) \subseteq \mathrm{H}^0(B, \mathcal{L}(\Delta) \otimes \mathcal{L}(2E_\beta)).$$

$$\begin{tikzcd} & B \arrow[dl, "\rho"'] \arrow[dd, "\beta"] \\ \mathbb{P}^5_k & \\ & \mathbb{P}^2_k \arrow[ul, dashed, "\vartheta"] \end{tikzcd} \tag{4.1}$$

From the commutative diagram in (4.1) we see that these linear systems are identified under the isomorphism

$$\beta^* \colon \mathrm{H}^0(\mathbb{P}^2_k, \mathcal{L}(\Delta_0)) \to \mathrm{H}^0(B, \mathcal{L}(\Delta) \otimes \mathcal{L}(2E_\beta)). \qquad \square$$

PROPOSITION 4.2.9. *Consider the surfaces X and X' over k constructed from the same seed m. They are isomorphic over k.*

These surfaces are isomorphic as subschemes of $\mathbb{P}^5_k$ up to an automorphism of $\mathbb{P}^5_k$.

Proof. The schemes X and X' are the respective closures of the images of the maps $\mathbb{P}^2_k \dashrightarrow \mathbb{P}^5_k$ and $B \to \mathbb{P}^5_k$ defined by choosing bases of Q and $\mathrm{H}^0(B, \mathcal{L}(\Delta))$. If we pick bases corresponding to each other using the isomorphism in Corollary 4.2.8 then X and X' are the same subscheme of $\mathbb{P}^5_k$. If we make a different choice of basis of Q then we recover an isomorphic k-scheme X, but the embedding $X \subseteq \mathbb{P}^5_k$ changes by an automorphism of $\mathbb{P}^5_k$. The same holds for X' and the result follows. $\square$

Let us turn our attention back to interesting del Pezzo surfaces over k. We can use the correspondence in Proposition 4.2.6 to classify interesting del Pezzo surfaces over a field k.

PROPOSITION 4.2.10. *Let k be a perfect field and fix an algebraic closure $\bar{k}$. The map which sends an isomorphism class of interesting del Pezzo surfaces over k to its splitting field $K \subseteq \bar{k}$ is a bijection to the set of degree 5 Galois extensions of k contained in $\bar{k}$.*

Proof. Let us first show that we have a correspondence between degree 5 Galois extensions $K \subseteq \bar{k}$ and conjugacy classes of homomorphisms $G_k \to S_5$ whose image is of order 5.

To any homomorphism $\xi \colon G_k \to S_5$ whose image is of order 5, we can consider the kernel which corresponds to a Galois extensions K/k of degree 5.

Now consider a Galois extension K/k of degree 5 and let $G_K \subseteq G_k$ be the corresponding subgroup of index 5. We can construct a group homomorphism $G_k \to G_k/G_K \to S_5$, by sending a generator of G_k/G_K to any element $s \in S_5$ of order 5. Since every element of order 5 in S_5 is of the same cycle type, a different choice of $s \in S_5$ produces a conjugate homomorphism $G_k \to S_5$. So we have assigned a conjugacy class of homomorphisms $G_k \to S_5$ with an image of order 5 to a degree 5 Galois extension K/k.

It is easily checked that both procedures are inverse to each other.

Let us now prove the proposition by constructing an inverse to the described map. So again, let K be a degree 5 Galois extension of k and let $\xi \colon G_k \to S_5$ be a homomorphism in the corresponding conjugacy class of homomorphisms as above. By Proposition 4.2.6 we can produce a del Pezzo surface X by choosing a seed m of ξ, whose action on the -1-curves is uniquely determined by ξ. By construction of ξ we see that the action of G_k on $\operatorname{Pic} \bar{X}$ is non-trivial, but the corresponding action of G_K on $\operatorname{Pic} \bar{X}$ is trivial. By definition we see that X is an interesting del Pezzo surface.

It is clear that these maps define a correspondence between interesting del Pezzo surfaces over k and degree 5 Galois extensions of k. □

DEFINITION 4.2.11. Let K/k be a Galois extension of degree 5. The isomorphism class of interesting del Pezzo surfaces of degree 5 over k which are split by K is denoted by $\mathrm{dP}_5(K)$.

So the isomorphism class of an interesting del Pezzo surface over a field k is uniquely determined by the splitting field K. We have also seen two constructions for del Pezzo surfaces in such an isomorphism class. We will be interested in how the geometric -1-curves can be found on such a surface.

PROPOSITION 4.2.12. *Let m be a seed for a general homomorphism $\xi\colon G_k \to S_k$. Consider the five points $P_i = (\alpha_i : \alpha_i^2 : 1)$ constructed from the roots of m, and let $\vartheta\colon \mathbb{P}^2_k \dashrightarrow X$ be the birational map from Proposition 4.2.5. Define $L_{ij} \subseteq \mathbb{P}^2_{\bar{k}}$ as the line through P_i and P_j for $i \neq j$.*

The strict transform of L_{ij} along ϑ is a -1-curve on $\bar{X}$.

Proof. See Theorem 5 in [29]. □

Note that this allows us to produce all 10 curves on $\bar{X}$ of self-intersection -1. For interesting del Pezzo surfaces this implies the following result.

PROPOSITION 4.2.13. *Let X be an interesting del Pezzo surface of degree 5 over a field k. Consider the divisors*

$$\mathcal{L}_1 = \sum_{i=1}^{5} L_{i,i+1} \quad \textit{and} \quad \mathcal{L}_2 = \sum_{i=1}^{5} L_{i,i+2}$$

on $\mathbb{P}^2_k$ where the indices are considered modulo 5. These are quintic plane curves singular at the P_i, so they correspond to hyperplane sections of $X \subseteq \mathbb{P}^5_k$. These are precisely the anticanonical sections given by l_1 and l_2.

Proof. The group G_k permutes the points P_i cyclically by definition. We see that $\mathcal{L}_1$ and $\mathcal{L}_2$ are defined over k. This means that each divisor pulls back to a divisor supported on a Galois-invariant set of five -1-curves on $\bar{X}$. The only such sets are cut out by l_1 and l_2. □

4.3 Models of interesting del Pezzo surfaces

Let K be a cyclic number field of degree 5 and let $X \subseteq \mathbb{P}^5_{\mathbb{Q}}$ be the anticanonical image of the del Pezzo surface over $\mathbb{Q}$ of degree 5 associated to the field extension $K/\mathbb{Q}$. We will construct a model $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ such that the generic fibre $\mathcal{X}_{\mathbb{Q}} \subseteq \mathbb{P}^5_{\mathbb{Q}}$ is isomorphic to X.

Note that although X only depends on the degree 5 extension K the model $\mathcal{X}$ will definitely depend on an explicit generator $\alpha \in K$. We will start by fixing an element $\alpha \in K$ such that $\mathbb{Q}(\alpha) = K$ and we will then give two constructions for $\mathcal{X}$. The first construction will be very useful in determining explicit equations for $\mathcal{X}$ as a subscheme of $\mathbb{P}^5_{\mathbb{Z}}$; the second is of a more geometrical nature and makes it easier to understand the fibres $X = \mathcal{X}_{\mathbb{Q}}$ and $\mathcal{X}_\ell$ for a prime ℓ.

4.3.1 Explicit equations for $\mathcal{X}_\alpha$

As said above we can construct a model $\mathcal{X}/\mathbb{Z}$ of X over $\mathbb{Q}$ for each $\alpha \in K$. To simplify the construction we will assume that α is integral.

Step 1. Start with a cyclic extension $K/\mathbb{Q}$ of degree 5 and fix a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Next choose an element $\alpha \in \mathcal{O}_K$ such that $\mathbb{Q}(\alpha) = K$ and let α_i denote the conjugates of α. We will write m_α and m_{α^2} for the minimal polynomials of α and α^2 over $\mathbb{Z}$. Let $Z \subseteq \mathbb{P}^2_{\mathbb{Q}}$ be the reduced subscheme defined by the homogeneous ideal

$$(x^2 - yz, z^5 m_\alpha(x/z), z^5 m_{\alpha^2}(y/z)) \subseteq \mathbb{Q}[x,y,z].$$

This subscheme is zero-dimensional and supported in the five distinct points $P_i = (\alpha_i : \alpha_i^2 : 1)$ on the projective plane defined over K.

Step 2. Let $\mathcal{Q} \subseteq \mathbb{Z}[x,y,z]$ be the subset consisting of all quintic polynomials $q \in \mathbb{Z}[x,y,z]$ such that the associated degree 5 curve $C \subseteq \mathbb{P}^2_{\mathbb{Q}}$ is singular at the five points P_i, i.e. C_K has multiplicity at least 2 at each point P_i.

Note that $\mathcal{Q}$ is the intersection of $\mathbb{Z}[x,y,z]$ and Q in $\mathbb{Q}[x,y,z]$.

LEMMA 4.3.1. *The subset $\mathcal{Q} \subseteq \mathbb{Z}[x,y,z]$ is a free $\mathbb{Z}$-module of rank* 6 *and $\mathbb{Z}[x,y,z]/\mathcal{Q}$ is torsion free.*

Proof. Since $\mathbb{Z}[x,y,z]$ is a free $\mathbb{Z}$-module and $\mathbb{Z}$ is a principal ideal domain, we find that the sub-$\mathbb{Z}$-module $\mathcal{Q}$ is also a free $\mathbb{Z}$-module. We have seen in Lemma 4.2.4 that $\mathcal{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a 6-dimensional vector space over $\mathbb{Q}$ so $\mathcal{Q}$ is a free of rank 6 over $\mathbb{Z}$.

Now one has to check that if $nq \in \mathcal{Q}$ for an integer $n \neq 0$ and $q \in \mathbb{Z}[x,y,z]$, then $q \in \mathcal{Q}$. Since $nq \in \mathcal{Q}$ and $n \neq 0$ we see that q is a quintic polynomial. It is clear that q is singular at the points P_i precisely when nq has this property. $\square$

Step 3. Fix a basis $q_0, q_1, \ldots, q_5 \in \mathcal{Q}$ and define the rational map $\vartheta \colon \mathbb{P}^2_{\mathbb{Z}} \dashrightarrow \mathbb{P}^5_{\mathbb{Z}}$ by $[x : y : z] \mapsto [q_i(x,y,z)]_i$.

DEFINITION 4.3.2. The closure of the image of the rational map $\vartheta \colon \mathbb{P}^2_{\mathbb{Z}} \dashrightarrow \mathbb{P}^5_{\mathbb{Z}}$ defined by $q_0, q_1, \ldots, q_5$ is denoted by $\mathcal{X}_\alpha$ or simply $\mathcal{X}$ if no confusion is possible. Denote the generic fibre of $\mathcal{X}_\alpha$ by X_α or X.

Note that as a $\mathbb{Z}$-scheme $\mathcal{X}$ only depends on α. As a subscheme of $\mathbb{P}^5_{\mathbb{Z}}$ it does depend on the choice of basis of $\mathcal{Q}$. This construction does however show that for a given α the closed embedding $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ is unique up to an automorphism of $\mathbb{P}^5_{\mathbb{Z}}$.

The following theorem tells us that this construction does what we want.

THEOREM 4.3.3. *The scheme $\mathcal{X}_\alpha \subseteq \mathbb{P}^5_{\mathbb{Z}}$ is integral. The generic fibre of $\mathcal{X}/\mathbb{Z}$ is isomorphic to* $\mathrm{dP}_5(K)$ *and every fibre of $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ over a finite prime ℓ of $\mathbb{Z}$ is a singular del Pezzo surface of degree* 5 *anticanonically embedded. A fibre $\mathcal{X}_\ell$ over a prime ℓ is an ordinary del Pezzo surface precisely when the reduction of Z modulo ℓ is reduced.*

The above construction is convenient for computing explicit equations defining $\mathcal{X}$ as a subscheme of $\mathbb{P}^5_{\mathbb{Z}}$. The MAGMA code which takes $\alpha \in K$ as an input and computes the equations for $\mathcal{X}$ can be found at [39]. The computation uses the following result which follows from the theorem.

COROLLARY 4.3.4. *Consider the generic fibre $X \subseteq \mathbb{P}^5_{\mathbb{Q}}$ of $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$. The scheme $\mathcal{X}$ is the flat closure of X in $\mathbb{P}^5_{\mathbb{Z}}$.*

Proof. It is clear that $\mathcal{X}$ is a closed subscheme of $\mathbb{P}^5_{\mathbb{Z}}$ which contains X. The result follows from the fact that $\mathcal{X}$ is an integral scheme. The closure of a subscheme of the generic fibre is always flat by [33, Proposition III.9.7]. □

To prove Theorem 4.3.3 we will consider a different construction of $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$. We will prove that both constructions coincide while studying the fibres $\mathcal{X}_{\alpha,\ell}$ of $\mathcal{X}_\alpha$.

4.3.2 Geometric construction of $\mathcal{X}_\alpha$

The construction of $\mathcal{X}_\alpha$ using the quintic polynomials is reminiscent of the construction we have seen for X_α. Now consider the other construction of X_α; start with five distinct points on the projective plane. Blow up these points and consider the strict transform of the conic through the five points. This conic turns into a -1-curve on the blowup. Now contract this -1-curve.

We will repeat this construction on the projective plane over the integers.

DEFINITION 4.3.5. Define Γ_0 and Λ_0 as the subschemes of $\mathbb{P}^2_{\mathbb{Z}}$ defined by the respective equations $x^2 - yz = 0$ and $z = 0$. Let $\mathcal{Z} \subseteq \mathbb{P}^2_{\mathbb{Z}}$ be the closure of the zero-dimensional scheme $Z \subseteq \mathbb{P}^2_{\mathbb{Q}} \subseteq \mathbb{P}^2_{\mathbb{Z}}$.

Since we assumed that α is integral one can show that $\mathcal{Z}$ is actually defined by the ideal

$$(x^2 - yz, z^5 m_\alpha(x/z), z^5 m_{\alpha^2}(y/z)) \subseteq \mathbb{Z}[x,y,z].$$

If one thinks of $\mathbb{P}^2_{\mathbb{Z}}$ as a family of projective planes over $\mathbb{F}_\ell$ and $\mathbb{Q}$, then Λ_0 and Γ_0 are respectively a line and a conic on each fibre. In this setup $\mathcal{Z}$ is a family over $\mathbb{Z}$ of five relative points on Γ_0. These five points on the fibre $\mathbb{P}^2_{\mathbb{F}_\ell}$ over ℓ are the points P_i on $\mathbb{P}^2_{\mathbb{Q}}$ reduced modulo a prime $\mathfrak{l}$ of K which divides ℓ. It is possible that two points P_i and P_j reduce to the same point modulo $\mathfrak{l}$. This information is captured by $\mathcal{Z}_\ell$ which is a zero-dimensional scheme of degree 5 for all ℓ. The fact that $\Gamma_{0,\ell}$ passes through $\mathcal{Z}_\ell$ helps to identify $\mathcal{Z}_\ell$ in the following way: fix a prime ℓ and mark each point $Q \in \Gamma_{0,\ell}(\mathbb{F}_{\mathfrak{l}}) \subseteq \mathbb{P}^2_{\mathbb{F}_\ell}(\mathbb{F}_{\mathfrak{l}})$ with the $n(Q)$ number of points $P_i \in \mathbb{P}^2_{\mathbb{Q}}$ which reduce to Q. Then $\mathcal{Z}_\ell$ is the unique zero-dimensional degree 5 subscheme of $\Gamma_{0,\ell}$ whose degree at each point $Q \in \Gamma_{0,\ell}(\mathbb{F}_l)$ equals precisely $n(Q)$.

PROPOSITION 4.3.6. *The subscheme $\mathcal{Z}$ lies on Γ_0. The subscheme Λ_0 does not meet $\mathcal{Z}$. The fibre $\mathcal{Z}_\ell$ over a finite prime ℓ is a zero-dimensional subscheme of $\mathbb{P}^2_{\mathbb{F}_\ell}$ of degree* 5.

Proof. We know that Z is a subscheme of Γ_0 and this implies that $\mathcal{Z}$ also lies on Γ_0. The second statement uses the defining equations for Λ_0 and $\mathcal{Z}$, and the fact that α is an integral element of K.

We see, for example from Proposition III.9.7 in [33], that $\mathcal{Z} \to \mathbb{Z}$ is a flat morphism. This proves that the Hilbert Polynomial P_ℓ of the fibre $\mathcal{Z}_\ell$ over a prime $\ell \in \mathbb{Z}$ is independent of ℓ [33, Theorem III.9.9]. We know that over the generic point $(0) \in \operatorname{Spec} \mathbb{Z}$ the fibre $Z = \mathcal{Z}_{\mathbb{Q}}$ is zero-dimensional of degree 5 and this proves that the result is true for all fibres. $\square$

We see that on each fibre $\mathbb{P}^2_{\mathbb{F}_\ell}$ we have a zero-dimensional subscheme $\mathcal{Z}_\ell$ which lies on the conic $\Gamma_{0,\ell}$. Because the intersection number between a line L and the conic $\Gamma_{0,\ell}$ equals 2 we conclude from Definition 2.7.2 that $\mathcal{Z}_\ell \subseteq \mathbb{P}^2_{\mathbb{F}_\ell}$ lies in almost general position. We will consider the peculiar del Pezzo surface we get by blowing up $\mathcal{Z}_\ell$.

DEFINITION 4.3.7. Let $\mathcal{B}$ be the blowup $\operatorname{Bl}_{\mathcal{Z}} \mathbb{P}^2_{\mathbb{Z}}$. Write Λ and Γ for the strict transforms of Λ_0 and Γ_0 along the blowup $\beta\colon \mathcal{B} \to \mathbb{P}^2_{\mathbb{Z}}$. Define the divisor $\Delta = \Lambda + 2\Gamma$ on $\mathcal{B}$.

PROPOSITION 4.3.8. *Let ℓ be a rational prime. The fibre $\mathcal{B}_\ell$ is integral and isomorphic to the blowup of $\mathbb{P}^2_{\mathbb{F}_\ell}$ in $\mathcal{Z}_\ell$.*

For the generic fibre we have a similar statement which follows from the fact that blowing up commutes with flat base change. This shows that the blowup $\beta_{\mathbb{Q}}$ on the generic fibre $B \to \mathbb{P}^2_{\mathbb{Z}}$, where $B = \mathcal{B}_{\mathbb{Q}}$ is the generic fibre of $\mathcal{B}$, is the blowup in the zero-dimensional subscheme Z.

Proof of Proposition 4.3.8. Let us first deduce some preliminary results. Let $\mathcal{E} \subseteq \mathcal{B}$ be the exceptional divisor of the blowup $\mathcal{B} \to \mathbb{P}^2_{\mathbb{Z}}$. Since $\mathbb{P}^2_{\mathbb{Z}}$ is a Cohen–Macaulay scheme and $\mathcal{Z} \subseteq \mathbb{P}^2_{\mathbb{Z}}$ is locally defined by a regular embedding we deduce that $\mathcal{E} \to \mathcal{Z}$ is locally a $\mathbb{P}^1$-bundle. Since $\mathcal{Z}$ is faithfully flat over $\operatorname{Spec} \mathbb{Z}$ we see that the same is true for $\mathcal{E}$. These results also allow us to prove that both $\mathcal{Z}$ and $\mathcal{E}$ are Cohen–Macaulay schemes. Following the proof of Theorem II.8.24 in [33] we conclude that $\mathcal{B}$ is Cohen–Macaulay as well.

Define $F = \mathbb{P}^2_{\mathbb{F}_\ell}$ to be the fibre of $\mathbb{P}^2_{\mathbb{Z}}$ over ℓ. The blowup $\operatorname{Bl}_{\mathcal{Z}_\ell} F$ is the scheme-theoretic closure of $F \backslash \mathcal{Z}_\ell$ in $\mathcal{B}_\ell$ by [24, Proposition IV-21]. We will first show that $\mathcal{B}_\ell$ is irreducible. This proves that $\operatorname{Bl}_{\mathcal{Z}_\ell} F$ is isomorphic to the topological closure of $F \backslash \mathcal{Z}_\ell$ in $\mathcal{B}_\ell$ with its reduced scheme structure, since F is reduced. Then we continue by proving that $\mathcal{B}_\ell$ is also reduced and we conclude that the closed embedding $\operatorname{Bl}_{\mathcal{Z}_\ell} F \to \mathcal{B}_\ell$ is actually an isomorphism.

So we will first prove that $\mathcal{B}_\ell$ is integral. By Krulls Hauptidealsatz we see that every irreducible component of $\mathcal{B}_\ell$ is of codimension 1 in $\mathcal{B}$, and the same holds for irreducible components of $\mathcal{E}_\ell$ in $\mathcal{E}$. Since $\mathcal{E}$ is of pure codimension 1 in $\mathcal{B}$, we see that $\mathcal{E}_\ell$ is of pure codimension 2 in $\mathcal{B}$. This proves that the generic point of an irreducible component of $\mathcal{B}_\ell$ does not lie in $\mathcal{E}_\ell$ and since $\mathcal{B}_\ell \backslash \mathcal{E}_\ell \cong F \backslash \mathcal{Z}_\ell$ is irreducible we conclude that $\mathcal{B}_\ell$ is irreducible.

To prove that $\mathcal{B}_\ell$ is also reduced we first note that it is Cohen–Macaulay since it is a Cartier divisor on the Cohen–Macaulay scheme $\mathcal{B}$. In particular $\mathcal{B}_\ell$ satisfies Serre's condition S_1 and we see that being reduced is equivalent to being generically reduced. The result now follows from the fact that $\mathcal{B}_\ell$ is birational to the reduced scheme F. $\square$

This shows that the each $\mathcal{B}_\ell$ is a peculiar del Pezzo surface over $\mathbb{F}_\ell$. Let $\rho_\ell \colon \tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell$ be the associated generalized del Pezzo surface, i.e. the minimal desingularization of $\mathcal{B}_\ell$. We will show that actually all -2-curves on $\tilde{\mathcal{B}}_\ell$ are contracted by ρ_ℓ. This proves that $\mathcal{B}_\ell$ is even a singular del Pezzo surface over $\mathbb{F}_\ell$. For all but a finite number of primes ℓ the fibre $\mathcal{B}_\ell$ will even be an ordinary del Pezzo surface. In this case the morphism ρ_ℓ will actually be an isomorphism and we can identify $\tilde{\mathcal{B}}_\ell$ and $\mathcal{B}_\ell$. This will in particular be the case for the generic fibre $\mathcal{B}_\mathbb{Q}$.

We will also look into the divisor Γ_ℓ on $\mathcal{B}_\ell$ by computing the self-intersection of the strict transform of $\tilde{\Gamma}_\ell$ on $\tilde{\mathcal{B}}_\ell$.

COROLLARY 4.3.9. *The fibres of $\mathcal{B}/\mathbb{Z}$ are singular del Pezzo surfaces of degree* 4. *The strict transform $\tilde{\Gamma}_\ell$ of Γ_ℓ is a -1-curve on the minimal desingularization $\tilde{\mathcal{B}}_\ell$ of $\mathcal{B}_\ell$ and so is $\Gamma_\mathbb{Q}$ on $\mathcal{B}_\mathbb{Q}$.*

As mentioned above, we will show that actually all but finitely many fibres of $\mathcal{B} \to \operatorname{Spec} \mathbb{Z}$ are ordinary del Pezzo surfaces.

Proof. We will prove the corollary for fibres over finite primes ℓ. The statements over the generic fibre $(0) \in \operatorname{Spec} \mathbb{Z}$ are similar or even simpler.

By Proposition 4.3.8 we see that $\mathcal{B}_\ell$ is isomorphic to $\mathrm{Bl}_{\mathcal{Z}_\ell}(\mathbb{P}^2_{\mathbb{F}_\ell})$. We know that $\mathcal{Z}_\ell$ lies on the conic $\Gamma_{0,\ell} \subseteq \mathbb{P}^2_{\mathbb{F}_\ell}$. It follows from Proposition 2.7.15 that $\mathrm{Bl}_{\mathcal{Z}_\ell}(\mathbb{P}^2_{\mathbb{F}_\ell})$ is a singular del Pezzo surface.

Now consider $\Gamma_{0,\ell} \subseteq \mathbb{P}^2_{\mathbb{F}_\ell}$. We know that $\deg(\Gamma_{0,\ell} \cap \mathcal{Z}_\ell) = \deg \mathcal{Z}_\ell = 5$, so the strict transform $\tilde{\Gamma}_\ell \subseteq \tilde{\mathcal{B}}_\ell$ of the conic $\Gamma_{0,\ell}$ has self-intersection -1 by Lemma 2.7.9. $\square$

We would like to contract Γ_ℓ. Of course we can contract $\tilde{\Gamma}_\ell$ on $\tilde{\mathcal{B}}$, but this only descends to $\mathcal{B}_\ell$ if $\tilde{\Gamma}_\ell$ does not meet any -2-curves on $\tilde{\mathcal{B}}_\ell$.

LEMMA 4.3.10. *The divisor Γ_ℓ does not pass through any singular points on $\mathcal{B}_\ell$.*

Proof. We will prove that on the minimal desingularization $\tilde{\mathcal{B}}_\ell$ the -1-curve $\tilde{\Gamma}_\ell$ does not meet any -2-curves.

Fix a basis $L_0, \dots, L_5$ as in Proposition 2.3.1 for the geometric Picard group of the generalized del Pezzo surface $\tilde{\mathcal{B}}_\ell$. Note that by Corollary 4.3.9 all -2-curves on $\tilde{\mathcal{B}}_\ell$ are contracted by $\tilde{\beta}\colon \tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell \to \mathbb{P}^2_{\mathbb{Z}}$. So any -2-curve lies in the support of the exceptional divisor $E_{\tilde{\beta}}$ and we conclude that it must be linear equivalent to a divisor of the form $L_i - L_j$ for distinct and positive i and j. The class of $\tilde{\Gamma}_\ell$ is $2L_0 - L_1 - L_2 - L_3 - L_4 - L_5$ which proves that the intersection number of $\tilde{\Gamma}_\ell$ with any -2-curve is zero. $\square$

We will now consider the image of the map to a projective space associated to the divisor $\Delta = \Lambda + 2\Gamma$ on $\mathcal{B}$.

PROPOSITION 4.3.11. *The $\mathbb{Z}$-module $\mathrm{H}^0(\mathcal{B}, \Delta)$ is free of rank 6. The composition*

$$\delta\colon \mathcal{B} \to \mathbb{P}^2_{\mathbb{Z}} \overset{\vartheta}{\dashrightarrow} \mathcal{X}$$

is a map associated to the complete linear system of the divisor Δ.

The map δ extends to a birational morphism $\mathcal{B} \to \mathcal{X}$. Furthermore, δ is an isomorphism on an open dense subset of each fibre of $\mathcal{B}$ over $\mathbb{Z}$.

We will prove this proposition in the next section, together with Theorem 4.3.3.

4.3.3 Comparison of the two constructions

We have seen two ways to construct $\mathcal{X}$; as the scheme-theoretic closure of the image of $\vartheta\colon \mathbb{P}^2_{\mathbb{Z}} \dashrightarrow \mathbb{P}^5_{\mathbb{Z}}$ and as the scheme-theoretic closure of the image of a map associated to the complete linear system of the divisor Δ on $\mathcal{B}$. In this section we will prove Theorem 4.3.3 and Proposition 4.3.11. We will first prove the following proposition which is the integral version of Corollary 4.2.8.

PROPOSITION 4.3.12. *Consider the blowup morphism $\beta\colon \mathcal{B} \to \mathbb{P}^2_{\mathbb{Z}}$. The pullback morphism β^* is an isomorphism on the function fields $\kappa(\mathbb{P}^2_{\mathbb{Z}}) \to \kappa(\mathcal{B})$. This morphism induces an isomorphism on the sub-$\mathbb{Z}$-modules*

$$\frac{1}{z(x^2-yz)^2}\mathcal{Q} \subseteq \kappa(\mathbb{P}^2_{\mathbb{Z}}) \quad \textit{and} \quad \mathrm{H}^0(\mathcal{B}, \mathcal{L}(\Delta)) \subseteq \kappa(\mathcal{B}).$$

Proof. The inclusion of the generic fibre $\mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{Z}}$ induces an isomorphism $\kappa(\mathbb{P}^2_{\mathbb{Q}}) \to \kappa(\mathbb{P}^2_{\mathbb{Z}})$. We will identify these two fields along this isomorphism. In the same way we will identify $\kappa(B)$ and $\kappa(\mathcal{B})$. Since β is a birational morphism of integral schemes it does indeed induce an isomorphism $\kappa(\mathbb{P}^2_{\mathbb{Z}}) \to \kappa(\mathcal{B})$ and we have seen in Corollary 4.2.8 that under this isomorphism we can identify

$$\frac{1}{z(x^2-yz)^2}Q \subseteq \kappa(\mathbb{P}^2_{\mathbb{Q}}) \quad \text{and} \quad \mathrm{H}^0(B, \mathcal{L}(\Delta_{\mathbb{Q}})) \subseteq \kappa(B).$$

Since $\beta_\ell\colon \mathcal{B}_\ell \to \mathbb{P}^2_{\mathbb{F}_\ell}$ is a birational morphism of integral varieties over $\mathbb{F}_\ell$ by Proposition 4.3.8 we see that β induces an isomorphism of the local rings $\mathcal{O}_{\mathcal{B},B_\ell}$

and $\mathcal{O}_{\mathbb{P}^2_{\mathbb{Z}},\mathbb{P}^2_{\mathbb{F}_\ell}}$ which proves that $\beta^*\colon \kappa(\mathbb{P}^2_{\mathbb{Z}}) \to \kappa(\mathcal{B})$ preserves the valuations along the prime divisors $\mathcal{B}_\ell$ on $\mathcal{B}$ and $\mathbb{P}^2_{\mathbb{F}_\ell}$ on $\mathbb{P}^2_{\mathbb{Z}}$.

This implies that β^* identifies the submodule of $\frac{1}{z(x^2-yz)^2}Q$ consisting of the elements with a non-negative valuation along $\mathbb{P}^2_{\mathbb{F}_\ell}$ for all primes ℓ with the submodule of $\mathrm{H}^0(B, \mathcal{L}(\Delta_{\mathbb{Q}}))$ with a no poles along $\mathcal{B}_\ell$ for all ℓ. Let us prove these submodules are precisely $\frac{1}{z(x^2-yz)^2}\mathcal{Q}$ and $\mathrm{H}^0(B, \mathcal{L}(\Delta))$.

By definition we see that $\mathrm{H}^0(\mathcal{B}, \mathcal{L}(\Delta)) \subseteq \mathrm{H}^0(B, \mathcal{L}(\Delta_{\mathbb{Q}})) \subseteq \kappa(\mathcal{B})$ after identifying the function fields of $\mathcal{B}$ and its generic fibre B. This identifies the prime divisors of B with the horizontal prime divisors of $\mathcal{B}$ and we see that $\mathrm{H}^0(\mathcal{B}, \mathcal{L}(\Delta))$ consists precisely of the elements in $\mathrm{H}^0(B, \mathcal{L}(\Delta_{\mathbb{Q}}))$ with a non-negative valuation along the vertical prime divisors $\mathcal{B}_\ell$.

We also have $\frac{1}{z(x^2-yz)^2}\mathcal{Q} \subseteq \frac{1}{z(x^2-yz)^2}Q \subseteq \kappa(\mathbb{P}^2_{\mathbb{Z}})$ using the identification of $\kappa(\mathbb{P}^2_{\mathbb{Z}})$ with $\kappa(\mathbb{P}^2_{\mathbb{Q}})$. Let $\frac{q}{z(x^2-yz)^2}$ be a quotient of quintics in $\mathbb{Q}[x,y,z]$, it can be written as $c\frac{q'}{z(x^2-yz)^2}$ with $c \in \mathbb{Q}$ and $q' \in \mathbb{Z}[x,y,z]$ a quintic polynomial with coprime coefficients. The valuation along $\mathbb{P}^2_{\mathbb{F}_\ell}$ is now simply the valuation of c at ℓ. This means that a $\frac{q}{z(x^2-yz)^2}$ has non-negative valuation along all vertical fibres if and only if q actually has integral coefficients. □

This allows us to prove Proposition 4.3.11.

Proof of Proposition 4.3.11. The scheme $\mathcal{X}_\alpha \subseteq \mathbb{P}^5_{\mathbb{Z}}$ is defined as the image of a rational map $\vartheta\colon \mathbb{P}^2_{\mathbb{Z}} \dashrightarrow \mathbb{P}^5_{\mathbb{Z}}$ defined by the chosen basis elements $q_i \in \mathcal{Q}$. By definition we have $\delta = \vartheta \circ \beta$ and using the identification in Proposition 4.3.12 we see that δ is defined using the basis of $\mathrm{H}^0(\mathcal{B}, \mathcal{L}(\Delta))$ corresponding to the chosen basis of $\mathcal{Q}$. By functoriality of maps to projective spaces coming from divisors [24, Theorem III-37], we see that the morphism $\mathcal{B}_\ell \to \mathbb{P}^5_{\mathbb{F}_\ell}$ coming from the divisor Δ_ℓ is simply the fibre of $\delta\colon \mathcal{B} \to \mathbb{P}^5_{\mathbb{Z}}$.

Let $\gamma_\ell\colon \tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell$ be the minimal desingularization of $\mathcal{B}_\ell$ and define $\tilde{\Gamma}_\ell$, $\tilde{\Lambda}_\ell$ and $\tilde{\Delta}_\ell$ to be the pullbacks of Γ_ℓ, Λ_ℓ and Δ_ℓ along γ_ℓ. By Lemma 2.5.1 we have an isomorphism between the global sections of $\mathcal{L}(\Delta_\ell)$ and $\mathcal{L}(\tilde{\Delta}_\ell)$. This proves that the composition $\delta'_\ell = \delta_\ell \circ \gamma_\ell$ is the map associated to the complete linear system of $\tilde{\Delta}_\ell$. We will first prove that δ'_ℓ is actually a morphism, i.e. the linear system of $\tilde{\Delta}_\ell$ is base point free.

Note that $\Lambda_{0,\ell} + \Gamma_{0,\ell} \subseteq \mathbb{P}^2_{\mathbb{F}_\ell}$ is a cubic plane curve passing through $\mathcal{Z}_\ell$ and this curve is smooth in the support of $\mathcal{Z}_\ell$. Proposition 2.5.4 shows that $\Lambda_\ell + \Gamma_\ell$ is an anticanonical divisor on $\mathcal{B}_\ell$ and $\tilde{\Lambda}_\ell + \tilde{\Gamma}_\ell$ is an anticanonical divisor on $\tilde{\mathcal{B}}_\ell$. Since $\tilde{\mathcal{B}}_\ell$ is a generalized del Pezzo surface of degree 4 we see that the complete linear system of $\tilde{\Lambda}_\ell + \tilde{\Gamma}_\ell$ defines a birational morphism which contracts the -2-curves on $\tilde{\mathcal{B}}_\ell$. In particular, we see that $\mathcal{L}(\tilde{\Lambda}_\ell + \tilde{\Gamma}_\ell)$ is globally generated. This proves that $\mathcal{L}(\tilde{\Lambda}_\ell + \tilde{\Gamma}_\ell + \tilde{\Gamma}_\ell)$ is globally generated away from Γ_ℓ. To see that $\mathcal{L}(\tilde{\Delta}_\ell)$ is globally generated on Γ_ℓ one can proceed as in Step 2 of the proof of

Theorem 5.7 in [33]. For this one needs $\mathrm{H}^1(\tilde{\mathcal{B}}_\ell, \omega^\vee) = 0$. The vanishing of this cohomology group follows for example from the Riemann–Roch theorem for smooth surfaces over a field.

So far we have the commutative diagram shown in (4.2).

$$
\begin{tikzcd}
 & \tilde{\mathcal{B}}_\ell \arrow[dl, "\delta'"'] \arrow[d, "\rho"] \\
\mathcal{X}_\ell & \mathcal{B}_\ell \arrow[l, dashed, "\delta"]
\end{tikzcd}
\tag{4.2}
$$

We will now prove that δ' contracts $\tilde{\Gamma}_\ell$ and all -2-curves on $\tilde{\mathcal{B}}_\ell$. We know that the complete anticanonical linear system on a generalized del Pezzo surface of degree 4 separates points and tangent vectors away from the -2-curves. We have seen that $\tilde{\Lambda}_\ell + \tilde{\Gamma}_\ell$ is an effective anticanonical divisor on $\tilde{\mathcal{B}}_\ell$ and we will write $\tilde{\Delta}_\ell = -K_{\tilde{\mathcal{B}}_\ell} + \tilde{\Gamma}_\ell$. We conclude that the complete linear system of $\tilde{\Delta}_\ell$ separates points and tangent vectors away from the -2-curves and $\tilde{\Gamma}_\ell$. This implies that $\tilde{\Delta}_\ell$ is big and nef and the only possible curves contracted by the associated birational map are the -2-curves and $\tilde{\Gamma}_\ell$. We saw in Lemma 4.3.10 that any -2-curve on $\tilde{\mathcal{B}}_\ell$ does not intersect $\tilde{\Gamma}_\ell$. So for any -2-curve R we have $\tilde{\Delta}_\ell \cdot R = -K_{\tilde{\mathcal{B}}_\ell} \cdot R + \tilde{\Gamma}_\ell \cdot R = 0$. We also have $\tilde{\Delta}_\ell \cdot \tilde{\Gamma}_\ell = -K_{\tilde{\mathcal{B}}_\ell} \cdot \Gamma_\ell + \tilde{\Gamma}_\ell^2 = 1 - 1 = 0$, since $\tilde{\Gamma}_\ell$ is a -1-curve on $\tilde{\mathcal{B}}_\ell$. This proves that δ'_ℓ is the morphism that contracts precisely $\tilde{\Gamma}_\ell$ and the -2-curves on $\tilde{\mathcal{B}}_\ell$. So δ_ℓ is defined off Γ_ℓ.

We also know that ρ_ℓ also contracts all -2-curves. This allows us to deduce that δ_ℓ is defined away from the singularities and we conclude that δ_ℓ is a morphism.

This proof also shows that δ_ℓ is an isomorphism away from Γ_ℓ. $\square$

Now we can prove Theorem 4.3.3.

Proof of Theorem 4.3.3. We see from either construction that the generic fibre of $\mathcal{X}$ is isomorphic to $\mathrm{dP}_5(K)$ by Proposition 4.2.9. We will prove that the fibres $\mathcal{X}_\ell$ are anticanonically embedded del Pezzo surfaces using the second construction of $\mathcal{X}$. We have already seen in Corollary 4.3.9 that the fibres of $\mathcal{B}$ are singular del Pezzo surfaces of degree 4. In the proof of Proposition 4.3.11 we have seen that $\delta_\ell \colon \mathcal{B}_\ell \to \mathcal{X}_\ell$ contracts the curve Γ_ℓ to a point. The composition $\tilde{\mathcal{B}}_\ell \xrightarrow{\rho} \mathcal{B}_\ell \xrightarrow{\delta} \mathcal{X}_\ell$ first contracts the -2-curves and then the curve Γ_ℓ. We can also do so in the opposite order. So let us first contract the -1-curve $\tilde{\Gamma}_\ell$ on $\tilde{\mathcal{B}}_\ell$. This gives us a morphism $\tilde{\delta} \colon \tilde{\mathcal{B}}_\ell \to \tilde{\mathcal{X}}_\ell$ to a generalized del Pezzo surface of degree 5. By Lemma 4.3.10 the -1-curve Γ_ℓ does not meet any -2-curve and so contracting it does not change the set of -2-curves. The pullback of an anticanonical divisor on $\tilde{\mathcal{X}}_\ell$ is the divisor $\tilde{\Delta}_\ell$ on $\tilde{\mathcal{B}}_\ell$ so the anticanonical morphism $\gamma_\ell \colon \tilde{\mathcal{X}}_\ell \to \mathcal{X}_\ell$ makes the diagram in (4.3) commutative.

$$\begin{tikzcd} \tilde{\mathcal{X}}_\ell \arrow[d, "\gamma_\ell"] & \tilde{\mathcal{B}}_\ell \arrow[l, "\tilde{\delta}_\ell"'] \arrow[d, "\rho_\ell"] \\ \mathcal{X}_\ell & \mathcal{B}_\ell \arrow[l, "\delta_\ell"'] \end{tikzcd} \tag{4.3}$$

This proves that $\mathcal{X}_\ell$ is a singular del Pezzo surface of degree 5 over $\mathbb{F}_\ell$.

Note that $\mathcal{X}_\ell$ is the fibre of the scheme $\mathcal{X}$ over $\mathbb{Z}$. On the other hand, the scheme $\tilde{\mathcal{X}}_\ell$ is defined as a scheme over $\mathbb{F}_\ell$ and we have not constructed the scheme $\tilde{\mathcal{X}}$ over $\mathbb{Z}$. Although it exists we will not need it. The same holds for the scheme $\tilde{\mathcal{B}}_\ell$ and for the morphisms ρ_ℓ, γ_ℓ and $\tilde{\delta}_\ell$.

We see that $\mathcal{X}_\ell$ is smooth precisely when $\mathcal{B}_\ell$ is smooth, since the image of the contracted -1-curve Γ_ℓ is a smooth point. We see from Corollary 2.7.14 that $\mathcal{B}_\ell$ is an ordinary del Pezzo surface precisely when $\mathcal{Z}_\ell$ is reduced. So if $\mathcal{Z}_\ell$ is non-reduced we see that $\mathcal{B}_\ell$ is singular. We already saw in Corollary 4.3.9 that $\mathcal{B}_\ell$ is a singular del Pezzo surface, so in this case $\mathcal{B}_\ell$ and hence also $\mathcal{X}_\ell$ are singular del Pezzo surfaces. □

Now that we have our model $\mathcal{X}/\mathbb{Z}$ of $X/\mathbb{Q}$ we would like to extend some objects we have on X to $\mathcal{X}$. Recall the two anticanonical sections l_1 and l_2 on X from Proposition 4.2.13 which cut out the -1-curves. We will redefine l_1 and l_2 as sections of $\mathcal{O}_{\mathbb{P}^5_{\mathbb{Z}}}(1)$.

DEFINITION 4.3.13. The elements $l_1, l_2 \in \mathcal{O}_{\mathbb{P}^5_{\mathbb{Q}}}(1)$ can be rescaled using an element of $\mathbb{Q}^\times$ to obtain elements $l_1, l_2 \in \mathcal{O}_{\mathbb{P}^5_{\mathbb{Z}}}(1)$. We will assume that l_1 and l_2 are rescaled such that they do not vanish on vertical prime divisors of $\mathcal{X}/\mathbb{Z}$.

Before we could think of each l_i as a linear form over $\mathbb{Q}$ in six variables. From now on l_i will be rescaled such that the six coefficients are integral and coprime.

We will now look more closely at the fibre of $\mathcal{X}$ over a prime $\ell \in \mathbb{Z}$. We have seen that this depends on $\mathcal{Z}_\ell$ and this scheme depends heavily on the factorization of ℓ in K. So let us first study the splitting field K more closely.

4.4 The splitting field of the interesting action

The action of Galois on the geometric Picard group of an interesting del Pezzo surface X factors through a quotient $\mathbb{Z}/5\mathbb{Z}$ which must be $\mathrm{Gal}(K/k)$ for a cyclic degree 5 extension of k. We will restrict to the case that the base field k is the field of rational numbers. First we will classify such number fields and then we will look at the arithmetic of monogenic number rings $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$.

4.4.1 Number fields of degree 5

Let K be a Galois extension of $\mathbb{Q}$ of degree 5. By the Kronecker–Weber theorem we get that the field K is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$ for some integer n. So the isomorphism classes of del Pezzo surfaces of degree 5 over $\mathbb{Q}$ split by a degree 5 extension correspond to open subgroups of index 5 in $\widehat{\mathbb{Z}}^\times$. In particular we see that every subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ of index 5 gives us such a surface.

DEFINITION 4.4.1. Consider an open subgroup $N \subseteq \widehat{\mathbb{Z}}^\times$ of index 5 and define $K \subseteq \mathbb{Q}^{\mathrm{cyc}}$ to be the associated number field of degree 5. The isomorphism class of the corresponding del Pezzo surface of degree 5 over $\mathbb{Q}$ will be denoted by $\mathrm{dP}_5(N)$.

If n is a positive integer such that $(\mathbb{Z}/n\mathbb{Z})^\times$ has a unique subgroup N' of index 5, then we get such a subgroup N by taking the pre-image under the projection $\widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. In this situation we will write $\mathrm{dP}_5(n)$ for $\mathrm{dP}_5(N)$.

The *conductor* of a $\mathrm{dP}_5(N)$ is the minimal n such that N is the pullback of a subgroup $N' \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$.

Note that the conductor will always exist since we are considering open subgroups of $\widehat{\mathbb{Z}}^\times$.

The construction of these degree 5 fields also gives us information about the splitting of rational primes.

PROPOSITION 4.4.2. *Let K be the number field associated to the open subgroup N of $\widehat{\mathbb{Z}}^\times$ of index 5 and let n be the conductor. The primes $\ell \in \mathbb{Q}$ which ramify in K are precisely those which divide n.*

Proof. Consider a prime $\mathfrak{l}$ above a prime $\ell \in \mathbb{Z}$. We have the commutative diagram shown in (4.4) from [53, Section 6] relating the global and local reciprocity maps.

$$\begin{tikzcd} \mathbb{Q}_\ell^\times \arrow[rr] \arrow[d] & & \mathrm{Gal}(K_{\mathfrak{l}}/\mathbb{Q}_\ell) \arrow[d] \\ \mathbb{I}_{\mathbb{Q}} \arrow[r] & \widehat{\mathbb{Z}}^\times \arrow[r] & \mathrm{Gal}(K/\mathbb{Q}) \end{tikzcd} \tag{4.4}$$

We have used that the bottom map factors through $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times$. The composite map $\mathbb{Q}_\ell^\times \to \widehat{\mathbb{Z}}^\times$ is on $\mathbb{Z}_\ell^\times$ given by the inclusion $\mathbb{Z}_\ell^\times \hookrightarrow \widehat{\mathbb{Z}}^\times$ [53, Example 5.7].

Let ϕ be the diagonal map $\mathbb{Q}_\ell^\times \to \mathrm{Gal}(K/\mathbb{Q})$. We know that $\mathfrak{l}/\ell$ is unramified exactly when the inertia subgroup of $\mathfrak{l}$ is trivial. This group is equal to $\phi(\mathbb{Z}_\ell^\times)$ by [47, Theorem 1, Section 4.1]. So we see that $\mathfrak{l}$ is unramified precisely when $\#\phi(\mathbb{Z}_\ell^\times) = 1$ or equivalently $\mathrm{Im}(\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times)$ lies in N. Now pick the minimal n such that $N \subseteq \widehat{\mathbb{Z}}^\times$ is the pullback of a subgroup N' of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then we see that $\mathfrak{l}$ is unramified when $\mathrm{Im}(\mathbb{Z}_\ell^\times \to (\mathbb{Z}/n\mathbb{Z})^\times)$ lies in N' which by the minimality of n happens precisely for the ℓ which do not divide n. $\square$

COROLLARY 4.4.3. *In the notation of Proposition 4.4.2, the conductor is the product of distinct primes $p \equiv 1 \mod 5$ and possibly a factor 25.*

For the proof of this corollary we will use the following result.

LEMMA 4.4.4. *Let $p \equiv 1 \mod 5$ be a prime. An element in $\mathbb{Z}_p^\times$ is a fifth power precisely when it is modulo p. The fifth powers in $\mathbb{Z}_5^\times$ are precisely the lifts of the fifth powers modulo* 25.

Proof. The first statement follows directly from Hensel's lemma. For the proof of the second statement one need to work modulo 5^3 to be able to apply Hensel's lemma. The fifth powers in $\mathbb{Z}/125\mathbb{Z}$ are easily checked to be all the classes which reduce to $\pm 1, \pm 7 \mod 25$. □

Proof of Corollary 4.4.3. We saw that ℓ is unramified precisely when the image of $\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times$ is a subgroup of $N \subseteq \widehat{\mathbb{Z}}^\times$. This means that ℓ is ramified exactly if the group homomorphism $\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times/N \cong \mathbb{Z}/5\mathbb{Z}$ is not constant, and hence surjective. The kernel of this morphism is an open index 5 subgroup of $\mathbb{Z}_\ell^\times$. This implies that it is the pullback of an index 5 subgroup of $(\mathbb{Z}/\ell^e\mathbb{Z})^\times$ for some $e \geq 1$ and we find $5 \mid \varphi(\ell^e) = \ell^{e-1}(\ell - 1)$. So the only possible ramified primes are the primes $p \equiv 1 \mod 5$ and 5.

Now let N_ℓ be the kernel of $\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times/N$. To prove the statement, we will show if ℓ is either 5 or $1 \mod 5$ the index 5 subgroup $N_\ell \subseteq \mathbb{Z}_\ell^\times$ must be equal to $\left(\mathbb{Z}_\ell^\times\right)^5$. Since N_ℓ is of index 5, we see that $\left(\mathbb{Z}_\ell^\times\right)^5 \subseteq N_\ell$. For $\ell \equiv 1 \mod 5$ we see that $\mathbb{Z}_\ell^\times/(\mathbb{Z}_\ell^\times)^5 \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^5$ is an isomorphism by Lemma 4.4.4. This implies that N_ℓ and $\left(\mathbb{Z}_\ell^\times\right)^5$ are both of index 5 in $\mathbb{Z}_\ell^\times$. So N_ℓ is the subgroup of fifth powers in $\mathbb{Z}_\ell^\times$ and by Lemma 4.4.4 it is the inverse image of the fifth powers modulo ℓ.

For $\ell = 5$ we can compute the index of $\left(\mathbb{Z}_5^\times\right)^5$ in $\mathbb{Z}_5^\times$ in a similar manner to conclude that N_5 can only be the pullback of the subgroup of fifth powers modulo 25 along the reduction morphism $\mathbb{Z}_5^\times \to \mathbb{Z}/25\mathbb{Z}$. □

Now consider the surfaces for which the conductor has only one prime divisor p. If $p \equiv 1 \mod 5$ then the conductor must be equal to p by Corollary 4.4.3. In this case there is a unique such number field K since the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. So for each prime $p \equiv 1 \mod 10$ there is an isomorphism class $\mathrm{dP}_5(p)$ of interesting del Pezzo surfaces over $\mathbb{Q}$. In the last section we will also consider a surface in the isomorphism class $\mathrm{dP}_5(25)$. This class exists because also $\mathrm{Gal}(\mathbb{Q}(\zeta_{25})/\mathbb{Q}) \cong (\mathbb{Z}/25\mathbb{Z})^\times$ has a unique subgroup of index 5.

4.4.2 Number rings $\mathbb{Z}[\alpha]$ of degree 5

We have seen that an interesting del Pezzo surface X is uniquely determined by its splitting field K. The model $\mathcal{X}$ over $\mathbb{Z}$ however depends on the choice of $\alpha \in \mathcal{O}_K$. Many arithmetic and geometric properties of $\mathcal{X}$ can be described in terms of the number ring $\mathbb{Z}[\alpha]$. Let us look at the primes of $\mathbb{Z}[\alpha]$ and relate this to the possible factorizations of m_α modulo a prime ℓ.

Recall that the *inertia degree* of a prime $\mathfrak{l}$ of a number ring $R \subseteq \mathcal{O}_K$ over a prime $\ell \in \mathbb{Z}$ is defined as the degree of the residue field $\mathbb{F}_\mathfrak{l} = R/\mathfrak{l}$ as a field extension of $\mathbb{F}_\ell$.

THEOREM 4.4.5. *Let $m \in \mathbb{Z}[s]$ be an irreducible monic polynomial with integral coefficients. Let $\alpha \in \bar{\mathbb{Q}}$ be a root of m and let ℓ be a prime. Pick monic polynomials $m_i \in \mathbb{Z}[s]$ whose reductions modulo ℓ are irreducible and pairwise distinct such that there exist integral numbers $e_i > 0$ with the property that*

$$m \equiv \prod_i m_i^{e_i} \mod \ell.$$

(a) The prime ideals of $\mathbb{Z}[\alpha]$ which lie above ℓ are $\mathfrak{l}_i = (\ell, m_i(\alpha))$. The inertia degree of the prime ideal $\mathfrak{l}_i$ over ℓ equals the degree of m_i.

(b) Let $r_i \in \mathbb{Z}[s]$ be the remainder of m upon division by m_i. The ideal $\mathfrak{l}_i$ is invertible precisely if $e_i = 1$ or $r_i \not\equiv 0 \mod \ell^2$.

(c) The identity

$$\ell\mathbb{Z}[\alpha] = \prod_i \mathfrak{l}_i^{e_i}$$

holds if and only if each ideal $\mathfrak{l}_i$ is invertible.

Proof. See Theorem 8.2 in [51]. □

Every prime $\tilde{\mathfrak{l}}$ of K lies above a single prime $\mathfrak{l}$ of $\mathbb{Z}[\alpha]$. The following lemma is useful in going from primes of $\mathbb{Z}[\alpha]$ to primes of K.

LEMMA 4.4.6. *Consider the inclusion $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ and let $\mathfrak{l}$ be an invertible prime of $\mathbb{Z}[\alpha]$. There exists a unique prime $\tilde{\mathfrak{l}}$ of $\mathcal{O}_K$ lying above $\mathfrak{l}$.*

Proof. Let $\tilde{\mathfrak{l}}$ be a prime above $\mathfrak{l}$. We get an extension of local rings $\mathbb{Z}[\alpha]_\mathfrak{l} \subseteq \mathcal{O}_{K,\tilde{\mathfrak{l}}} \subseteq K$. Since $\mathfrak{l}$ is invertible we see that $\mathbb{Z}[\alpha]_\mathfrak{l}$ is a discrete valuation ring with field of fraction K. Since $O_{K,\tilde{\mathfrak{l}}}$ is not a field we conclude that $\mathbb{Z}[\alpha]_\mathfrak{l} = \mathcal{O}_{K,\tilde{\mathfrak{l}}}$. This shows that $\tilde{\mathfrak{l}} = \mathcal{O}_K \cap \mathfrak{l}\,\mathbb{Z}[\alpha]_\mathfrak{l}$ is uniquely determined by $\mathfrak{l}$. □

The following result will also be useful.

LEMMA 4.4.7. *The inertia degree of a prime $\mathfrak{l}$ of $\mathbb{Z}[\alpha]$ is either* 1 *or* 5.

Proof. Let ℓ be the prime $\mathfrak{l} \cap \mathbb{Z}$ and let $\tilde{\mathfrak{l}}$ be a prime of K lying above $\mathfrak{l}$. Since $K/\mathbb{Q}$ is a Galois extension of degree 5 we know that the inertia degree of $\tilde{\mathfrak{l}}$ divides 5. So we have a the following extensions of fields

$$\mathbb{F}_\ell \subseteq \mathbb{F}_\mathfrak{l} \subseteq \mathbb{F}_{\tilde{\mathfrak{l}}}.$$

This proves the statement. □

Note that this also proves that the reduction of m_α modulo a prime ℓ is either irreducible or it splits in linear factors. Note however that these linear factors need not be distinct. The extremal case where $m_\alpha \mod \ell$ is the fifth power of a linear polynomial over $\mathbb{F}_\ell$ will play a special role

4.5 The fibres $\mathcal{X}_\ell$

In Section 4.3 we used the two constructions of the interesting del Pezzo surface X over $\mathbb{Q}$ to produce a model $\mathcal{X}$ of X over $\mathbb{Z}$. In this section we study the fibres of $\mathcal{X}$ over a prime ℓ. We will also come across the fibres $\mathcal{B}_\ell$ of the scheme $\mathcal{B}$ defined in Definition 4.3.7.

4.5.1 The construction of $\mathcal{X}_\ell$

We will start by exhibiting the relation between the fibres $\mathcal{X}_\ell$, $\mathcal{B}_\ell$ and $\mathbb{P}^2_{\mathbb{F}_\ell}$.

PROPOSITION 4.5.1. *Let ℓ be a rational prime and let $\mathfrak{l}$ be a prime of K which divides ℓ. The geometrically irreducible components of $\mathcal{Z}_\ell$ are defined over the residue field $\mathbb{F}_\mathfrak{l}$.*

The fibre $\mathcal{X}_\ell$ can be constructed as follows: we will define generalized del Pezzo surfaces $\mathcal{B}_{\ell,i}$ for $0 \le i \le 5$ of degree $9-i$ over the field $\mathbb{F}_\mathfrak{l}$. Simultaneously we define a curve Γ_i on $\mathcal{B}_{\ell,i}$. We start off with $\mathcal{B}_{\ell,0} = \mathbb{P}^2_{\mathbb{F}_\mathfrak{l}}$ together with $\Gamma_0 = \Gamma_{0,\ell}$. Now consider the reduction Q_i of the point $P_i = (\alpha_i \colon \alpha_i^2 \colon 1)$ modulo $\mathfrak{l}$ on $\mathbb{P}^2_{\mathbb{F}_\mathfrak{l}}$. There is a unique $\mathbb{F}_\mathfrak{l}$-point R_i on $\Gamma_i \subseteq \mathcal{B}_{\ell,i}$ whose image under the morphism $\mathcal{B}_{\ell,i} \to \mathbb{P}^2_{\mathbb{F}_\mathfrak{l}}$ is Q_i. Let $\mathcal{B}_{\ell,i+1}$ be the blowup of $\mathcal{B}_{\ell,i}$ in R_i and let Γ_{i+1} be the strict transform of Γ_i along this blowup. Then $\mathcal{B}_{\ell,5}$ is a generalized del Pezzo surface of degree 4 over $\mathbb{F}_\mathfrak{l}$ which descends to the minimal desingularization $\tilde{\mathcal{B}}_\ell$ of $\mathcal{B}_\ell$ over $\mathbb{F}_\ell$.

The strict transform Γ of Γ_0 to $\mathcal{B}_\ell$ can be contracted to obtain $\mathcal{X}_\ell$. This shows that the composition

$$\tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell \to \mathcal{X}_\ell$$

first contracts the -2-curves and then the -1-curve $\tilde{\Gamma}_\ell$. We can also first contract $\tilde{\Gamma}_\ell$ to obtain a generalized del Pezzo surface $\tilde{\mathcal{X}}_\ell$ of degree 5 and then contract the -2-curves to recover $\mathcal{X}_\ell$.

Proof. Proposition 4.3.8 states that $\mathcal{B}_\ell$ is the blowup of the projective plane in the curvilinear subscheme $\mathcal{Z}_\ell$. We have seen in Lemma 2.7.7 that the composition $\tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell \to \mathbb{P}^2_{\mathbb{F}_\ell}$ decomposes into blowups in closed points at least when the geometrically irreducible components of Z are defined over the base field. This is the case over the field $\mathbb{F}_\mathfrak{l}$.

The fact that $\delta_\ell \colon \mathcal{B}_\ell \to \mathcal{X}_\ell$ is the contraction of the curve Γ_ℓ was shown in the proof of Proposition 4.3.11. □

This result does not only help us to understand the geometry of $\mathcal{X}_\ell$, but also its arithmetic.

LEMMA 4.5.2. *Consider a finite prime ℓ and let r be the number of distinct roots of m_α in $\mathbb{F}_\ell$. Then we have*

$$\#\mathcal{X}(\mathbb{F}_\ell) = \ell^2 + r\ell + 1.$$

Proof. Factor m_α in $\bar{\mathbb{F}}_\ell$ as $\prod(s-\beta_i)^{e_i}$ and consider the blowup $\beta \colon \mathcal{B}_\ell \to \mathbb{P}^2_{\mathbb{F}_\ell}$. This map is an isomorphism away from the points $(\beta_i \colon \beta_i^2 \colon 1)$ and the fibre over each of these points is a projective line defined over $\mathbb{F}_\ell(\beta_i)$. We see that each root of m_α in $\mathbb{F}_\ell$ adds exactly ℓ points and other roots do not change the number of $\mathbb{F}_\ell$-points. Finally we contract the -1-curve Γ_ℓ which is defined over $\mathbb{F}_\ell$ and see that

$$\#\mathcal{X}(\mathbb{F}_\ell) = (\ell^2 + \ell + 1) + r\ell - \ell = \ell^2 + r\ell + 1. \qquad \square$$

4.5.2 The -1-curves on $\mathcal{X}_\ell$

Let us also study the curves of negative self-intersection of $\mathcal{X}_\ell$. We will do this by first considering the s-curves on $\tilde{\mathcal{B}}_\ell$ and on the minimal desingularization $\tilde{\mathcal{X}}_\ell$ of $\mathcal{X}_\ell$.

PROPOSITION 4.5.3. *Let $Q_i \in \mathcal{Z}(\mathbb{F}_\mathfrak{l})$ be the reduction of the point $P_i \in Z(K)$ modulo a prime $\mathfrak{l}$ of K lying above ℓ. These 5 points need not be all distinct.*

Consider the minimal desingularization $\tilde{\mathcal{X}}_\ell$ of the fibre of $\mathcal{X}$ over a prime ℓ. A -1-curve on $\tilde{\mathcal{X}}_\ell$ is the strict transform of the line through Q_i and Q_j along the birational morphisms $\tilde{\mathcal{X}}_\ell \leftarrow \tilde{\mathcal{B}}_\ell \to \mathbb{P}^2_{\mathbb{F}_\ell}$. Let us write $\mathcal{L}_{i,j,\ell}$ for this -1-curve, both on $\tilde{\mathcal{X}}_\ell$ and on $\tilde{\mathcal{B}}_\ell$.

If $Q_i = Q_j$, then $\mathcal{L}_{i,j,\ell}$ is the tangent line at Q_i to $\Gamma_{0,\ell}$.

Proof. Since intersection numbers can only go up when blowing down a -1-curve $\tilde{\mathcal{B}}_\ell \to \tilde{\mathcal{X}}_\ell$ we will first determine the s-curves on the minimal desingularization $\tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell$ of the fibre of $\mathcal{B}$ over ℓ. Consider the composition $\tilde{\beta}\colon \tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell \to \mathbb{P}^2_{\mathbb{F}_\ell}$. By Proposition 2.4.4 we have s-curves in the support of the exceptional divisor $E_{\tilde{\beta}}$. Recall that each component of $E_{\tilde{\beta}}$ has a unique -1-curve. This implies that $\tilde{\Gamma}_\ell$ intersects every component of $E_{\tilde{\beta}}$ in this -1-curve since $\tilde{\Gamma}_\ell$ does not intersect any -2-curves by Lemma 4.3.10. This means that after contracting $\tilde{\Gamma}_\ell$ we lose these -1-curves in the sense that their images on $\tilde{\mathcal{X}}_\ell$ have self-intersection zero. On the other hand, the -2-curves on $\tilde{\mathcal{X}}_\ell$ remain -2-curves when considering their strict transforms on $\tilde{\mathcal{B}}_\ell$.

Any other s-curve on $\tilde{\mathcal{B}}_\ell$ is the strict transform of a line or a conic on $\mathbb{P}^2_{\mathbb{F}_\ell}$. Since we blow up five points we see from Lemma 2.7.9 that apart from $\tilde{\Gamma}_\ell$ there are only -1-curves on $\tilde{\mathcal{B}}_\ell$ and each is the strict transform of a line L with the property that $\deg(L \cap \mathcal{Z}_\ell) = 2$. These are precisely the lines through Q_i and Q_j or the tangent line of $\Gamma_{0,\ell}$ in $Q_i = Q_j$.

For a line L through $Q_i \neq Q_j$ we see that its strict transform $\tilde{L}$ to $\tilde{\mathcal{B}}_\ell$ does not meet $\tilde{\Gamma}_\ell$ since blowing up once separates curves which intersect transversally. For the tangent in $Q_i = Q_j$ we will need to blow up at least two times, which is precisely what happens since P_i and P_j both reduce to $Q_i = Q_j$. This proves that these -1-curves on $\tilde{\mathcal{B}}_\ell$ remain -1-curves on $\tilde{\mathcal{X}}_\ell$ after contracting $\tilde{\Gamma}_\ell$. $\square$

Other important objects are the sections l_1 and l_2. We will now describe the subscheme on $\mathcal{X}_\ell$ and $\mathcal{B}_\ell$ cut out by these forms.

PROPOSITION 4.5.4. *The reduction of l_1 modulo ℓ cuts out an effective divisor of $\mathcal{X}_\ell$ supported in geometric -1-curves.*

Obviously the result also holds for l_2.

Proof. The section l_1 cuts out five geometric -1-curves on the generic fibre X of $\mathcal{X}$. By definition of l_1 over $\mathbb{Z}$ we see that l_1 cuts out the flat closure of these five geometric -1-curves over K in $\mathbb{P}^5_{\mathcal{O}_K}$. Let us consider the closure $\mathcal{L}$ in $\mathbb{P}^5_{\mathcal{O}_K}$ of one of these -1-curves L over $\mathbb{Q}$. The scheme $\mathcal{L}$ is flat over $\mathcal{O}_K$, so the fibre $\mathcal{L}_\mathfrak{l}$ over $\mathfrak{l}$ will be a degree 1 curve on $\mathcal{X}_\mathfrak{l} \subseteq \mathbb{P}^5_{\mathbb{F}_\mathfrak{l}}$ of genus 0. This shows that on the minimal desingularization $(\tilde{\mathcal{X}}_{\mathcal{O}_K})_\mathfrak{l} = \tilde{\mathcal{X}}_\ell \times_{\mathbb{F}_\ell} \mathbb{F}_\mathfrak{l}$ this curve $\mathcal{L}_\mathfrak{l}$ is a -1-curve on $(\tilde{\mathcal{X}}_{\mathcal{O}_K})_\mathfrak{l}$. This proves that l_1 vanishes on five, not necessarily distinct, geometric -1-curves on $\tilde{\mathcal{X}}_\ell$. Since the degree of the divisor of zeroes of l_1 equals five, it vanishes only on these curves. □

Note that this proves that l_1 vanishes on the strict transform along the birational morphisms $\tilde{\mathcal{X}}_\ell \leftarrow \tilde{\mathcal{B}}_\ell \rightarrow \mathbb{P}^2_{\mathbb{F}_\ell}$ of the line through Q_i and Q_{i+1}. Here we consider the indices modulo 5. Similar l_2 vanishes on the strict transform of the line through Q_i and Q_{i+2}.

Understanding the sections which are cut out by l_1 and l_2 on the fibre of $\mathcal{X}/\mathbb{Z}$ over a prime ℓ is also important for the following reason.

LEMMA 4.5.5. *Let Q be a singular $\bar{\mathbb{F}}_\ell$-point on the fibre $\mathcal{X}_\ell$. Then Q lies on the divisor of zeroes of both l_1 and l_2.*

We will see in Proposition 4.5.8 that all singular points on $\mathcal{X}_\ell$ are already defined over the base field $\mathbb{F}_\ell$.

Proof. A singular point Q corresponds to a connected set of -2-curves on $\tilde{\mathcal{X}}_\ell$ or equivalently $\tilde{\mathcal{B}}_\ell$. This is a chain of -2-curves which lies above a geometric point $Q_i = (\beta_i : \beta_i^2 : 1)$ of $\mathcal{Z}_\ell \subseteq \mathbb{P}^2_{\mathbb{F}_\ell}$. Now let e_i be the local degree of $\mathcal{Z}_\ell$ at Q_i. Since there is a singular point above Q_i we have that $e_i > 1$.

If $e_i = 2$, then assume without loss of generality that P_1 and P_2 reduce to the same point $Q_1 = Q_2$ modulo $\mathfrak{l}$, but the points P_3, P_4 and P_5 do not reduce to Q_1 modulo $\mathfrak{l}$. Now l_1 vanishes on the secant $\mathcal{L}_{2,3,\ell}$ and l_2 vanishes on the secant $\mathcal{L}_{1,3,\ell}$. By Corollary 2.7.10 these lines intersect a -2-curve on $\tilde{\mathcal{B}}_\ell$ above Q_1.

If $e_i > 2$, then assume without loss of generality that $Q_1 = Q_2 = Q_3$. This proves that the tangent lines $\mathcal{L}_{1,2,\ell}$ and $\mathcal{L}_{1,3,\ell}$ in Q_i at $\Gamma_{0,\ell}$ are the same line and this line is cut out by both l_1 and l_2. We again use Corollary 2.7.10 to conclude the statement. □

We have now seen that the geometry of the fibre $\mathcal{X}_\ell$ is determined by the factorization of m_α modulo ℓ. We will look into how factors of this factorization determine the singular points on $\mathcal{X}_\ell$.

4.5.3 The singularities of $\mathcal{X}_\ell$

We have seen that $\mathcal{B}_\ell$ and hence $\mathcal{X}_\ell$ is smooth precisely if $\mathcal{Z}_\ell$ is reduced. This result can be directly related to the splitting of m_α in $\bar{\mathbb{F}}_\ell$.

LEMMA 4.5.6. *A fibre $\mathcal{X}_\ell$ is non-singular precisely if m_α is separable over $\bar{\mathbb{F}}_\ell$.*

Proof. We have seen in Theorem 4.3.3 that $\mathcal{X}_\ell$ is an ordinary del Pezzo surface precisely if $\mathcal{Z}_\ell$ is reduced. Now write $m_\alpha = \prod_i (s-\beta_i)^{e_i}$ over $\bar{\mathbb{F}}_\ell$. Recall that $\mathcal{Z}_\ell$ is supported in the points $(\beta_i : \beta_i^2 : 1)$ and the geometrically irreducible component supported in this point is of degree e_i. This shows that $\mathcal{Z}_\ell$ is reduced precisely when m_α is separable in $\bar{\mathbb{F}}_\ell$. $\square$

Although the factorization over $\bar{\mathbb{F}}_\ell$ determines the geometry of $\mathcal{X}_\ell$ we have also seen that arithmetic properties are determined by the factors of m_α over $\mathbb{F}_\ell$. From Lemma 4.4.7 we deduce that m_α is either irreducible modulo ℓ or it splits into, not necessarily distinct, linear factors over $\mathbb{F}_\ell$. Let us describe $\mathcal{X}_\ell$ in both cases.

LEMMA 4.5.7. *Let ℓ be a prime such that m_α is irreducible modulo ℓ. The fibre $\mathcal{X}_\ell$ is a smooth del Pezzo of degree* 5 *with two Galois orbits of exceptional curves of size* 5*.*

Proof. In this case the procedure to determine $\mathcal{X}_\ell$ is similar to how we got X starting with the projective plane over $\mathbb{Q}$; we blow up five conjugate points and then contract the strict transform of the unique conic through these five points. The result follows. $\square$

PROPOSITION 4.5.8. *Suppose that m_α splits into linear factors modulo ℓ. The fibre of $\mathcal{X}$ above ℓ has a singular point of type A_{e_i-1} for each factor with multiplicity $e_i > 1$ in this factorization. In particular we see that there are at most* 2 *singular points on $\mathcal{X}_\ell$ and these are defined over $\mathbb{F}_\ell$.*

Proof. Write $m_\alpha = \prod_i (x-\beta_i)^{e_i}$ where β_i are the distinct roots of m_α in $\mathbb{F}_\ell$. The morphism $\mathcal{B}_\ell \to \mathbb{P}^2_{\mathbb{F}_\ell}$ restricts to an isomorphism on the complement of the points $(\beta_i, \beta_i^2, 1)$. Using the procedure described in Proposition 4.5.1 we see that the fibre above such a point is obtained by contracting the -2-curves from a chain of $e_i - 1$ curves with self-intersection -2 and one -1-curve. This shows that $\mathcal{B}_\ell$ has a singularity of type A_{e_i-1} above the point $(\beta_i, \beta_i^2, 1)$.

Contracting the -1-curve $\Gamma_\ell \subseteq \mathcal{B}_\ell$ does not produce additional singular points or change the type of singularities on $\mathcal{B}_\ell$, since these points do not lie on Γ_ℓ by Lemma 4.3.10.

As a quintic polynomial can have at most 2 multiple irreducible factors we see this is the maximal number of singularities. $\square$

Let us now relate the possible factorization of m_α modulo ℓ to the factorization of ℓ in $\mathcal{O}_K$. Let us first treat the unramified primes.

LEMMA 4.5.9. *Let $\ell \in \mathbb{Z}$ be a prime which is inert in K. The fibre $\mathcal{X}_\ell$ either*

» *is smooth, in the case that m_α is irreducible modulo ℓ, or*

» *has a single singular point which is of type A_4, when m_α is a fifth power of a linear function modulo ℓ.*

In particular, we see that $\mathcal{X}_\ell$ has at most one singular point if ℓ is inert.

Proof. By assumption K has a unique prime $\tilde{\mathfrak{l}}$ lying above ℓ. This implies that $\mathfrak{l} = \tilde{\mathfrak{l}} \cap \mathbb{Z}[\alpha]$ is the unique prime of $\mathbb{Z}[\alpha]$ lying above ℓ. The inertia degree of this prime is either 5 or 1. This corresponds precisely to the two cases described in the lemma. □

LEMMA 4.5.10. *Let $\ell \in \mathbb{Z}$ be a prime which splits completely in K. This implies that m_α splits into linear factors over $\mathbb{F}_\ell$, and $\mathcal{X}_\ell$ is a surface as described in Proposition 4.5.8.*

Proof. As ℓ splits completely we have an isomorphism of residue fields $\mathbb{F}_\ell \to \mathbb{F}_{\tilde{\mathfrak{l}}}$ for any prime $\tilde{\mathfrak{l}}$ of K lying above ℓ. This implies that in the tower $\mathbb{Z} \subseteq \mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ each prime of $\mathcal{O}_K$ which divides ℓ comes from a prime $\mathfrak{l}$ in $\mathbb{Z}[\alpha]$ with the same inertia degree. So all primes $\mathfrak{l}/\ell$ have inertia degree 1 and by the Kummer–Dedekind theorem, Theorem 4.4.5, we see that m_α must split into linear factors modulo ℓ. □

We now consider the case that ℓ is ramified in K. We will usually denote such a prime by p.

LEMMA 4.5.11. *Let p be a prime which is ramified in K. The minimal polynomial m_α is the fifth power of a linear polynomial over $\mathbb{F}_p$. The fibre $\mathcal{X}_p$ is a singular del Pezzo surface of degree* 5 *with a single singular point which is of type A_4. This surface contains precisely one line.*

Proof. We will need to prove that the first statement. The last statements then follow from Propositions 4.5.8 and 4.5.3.

Let $\tilde{\mathfrak{p}}$ be the prime of $\mathcal{O}_K$ dividing p. Since it is ramified and $K/\mathbb{Q}$ is a Galois extension we find $e(\tilde{\mathfrak{p}}/p) = 5$. This proves that p totally ramifies in K and that $\tilde{\mathfrak{p}}$ is the unique prime of $\mathcal{O}_K$ dividing p. Now let $\mathfrak{p}$ be the prime $\tilde{\mathfrak{p}} \cap \mathbb{Z}[\alpha]$ of $\mathbb{Z}[\alpha]$. Since the inertia degree of $\tilde{\mathfrak{p}}$ is one, so must the inertia degree of $\mathfrak{p}$. This proves the statement. □

Note that m_α can be a fifth power modulo ℓ in all three cases and this will always yield a singular del Pezzo surface of degree 5 with one singular point of type A_4, and one -1-curve. We will look more closely at this surface.

4.5.4 Fibres with an A_4-singularity

Consider a fibre of $\mathcal{X}$ over $\mathbb{Z}$ with a singularity of type A_4. We can encounter such a fibre over any prime ℓ, but we have seen in Lemma 4.5.11 that the fibre over any ramified prime p will be of this type. Since we will mainly discuss this fibre over ramified primes we will write p for the prime in this section, although theses results are true for any fibre with a singularity of type A_4.

PROPOSITION 4.5.12. *Let $\mathcal{X}_p$ be a fibre of $\mathcal{X}$ over $\mathbb{Z}$ with a singularity of type A_4. The surface $\mathcal{X}_p$ is the unique singular del Pezzo surface of degree* 5 *with a single* -1-*curve E_4 and one singular point which is of type A_4. Furthermore, the complement of this -1-curve E_4 in $\mathcal{X}_p$ is isomorphic to $\mathbb{A}^2_{\mathbb{F}_p}$.*

Let Z' be a curvilinear subscheme of degree 4 *supported in the inflection point p_0 of a cubic plane curve $C \subseteq \mathbb{P}^2_{\mathbb{F}_p}$. The surface $\mathcal{X}_p$ is the singular del Pezzo surface over $\mathbb{F}_p$ associated to Z'.*

The choice for notation of this unique -1-curve will become clear during the proof.

Proof of Proposition 4.5.12. Let us prove the first statement. It follows from Proposition 4.5.8 that $\mathcal{Z}_p$ is a degree 5 subscheme of $\Gamma_{0,p}$ supported in a single point Q. The procedure described in Proposition 4.5.1 shows that we can find $\tilde{\mathcal{B}}_p$ by first blowing up $\mathbb{P}^2_{\mathbb{F}_p}$ five times to get a configuration of three -1-curves and four -2-curves as shown in Figure III.

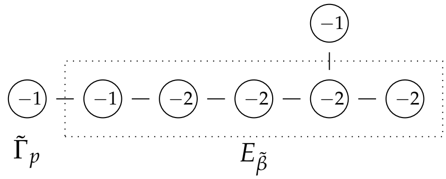

Figure III: Curves of negative self-intersection on $\tilde{\mathcal{B}}_p$.

The -1-curve on the left is $\tilde{\Gamma}_p \subseteq \tilde{\mathcal{B}}_p$. Consider the tangent line $L_{0,p} \subseteq \mathbb{P}^2_{\mathbb{F}_p}$ to $\Gamma_{0,p}$ in Q. The strict transform L of $L_{0,p}$ on $\tilde{\mathcal{B}}_p$ is a -1-curve by Lemma 2.7.9. The position of L in Figure III is determined by Lemma 2.7.10. This accounts for the -1-curve on top. The remaining four -2-curves and the -1-curve are the components of the exceptional divisor $E_{\tilde{\beta}}$. Then we contract $\tilde{\Gamma}_p$, which becomes a smooth point and makes the unique -1-curve on $E_{\tilde{\beta}}$ into a curve of self-intersection 0. Finally we contract all the -2-curves which gives an A_4 singularity lying on the remaining curve of negative self-intersection.

We see that all s-curves on $\tilde{\mathcal{X}}_p$ are defined over $\mathbb{F}_p$. This proves that there is an $\mathbb{F}_p$-morphism $\tilde{\pi}\colon \tilde{\mathcal{X}}_p \to \mathbb{P}^2_{\mathbb{F}_p}$ which is the blowup of the projective plane in 4 points in almost general position. Let $Z' \subseteq \mathbb{P}^2_{\mathbb{F}_p}$ be the associated zero-dimensional subscheme of this composition of blowups. Since we have only one -1-curve on $\tilde{\mathcal{X}}_p$ we conclude from Proposition 2.4.4 that Z' is supported in only one point p_0. This accounts for the -1-curve and three -2-curves, because they occur in the exceptional divisor $E_{\tilde{\pi}}$. Let us rename these divisors as in Proposition 2.4.4; the -2-curves are E_1, E_2 and E_3, and the -1-curve is E_4. Let us call the remaining -2-curve R. The intersection graph on s-classes on $\tilde{\mathcal{X}}_p$ is now shown in Figure IV.

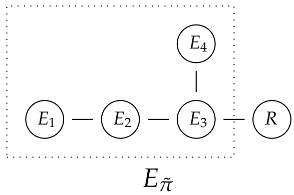

Figure IV: Curves of negative self-intersection on $\tilde{\mathcal{X}}_p$.

Let L be the image of R in $\mathbb{P}^2_{\mathbb{F}_p}$. We will now prove that L is a line. We know that

$$-2 = R^2 = L^2 - \deg(Z' \cap L) \geq L^2 - 3$$

since Z' is supported on a cubic curve C which is smooth at p_0. This proves that $L^2 \leq 1$ and hence $\deg L = 1$ and $\deg(Z' \cap L) = 3$. This proves that L is the tangent line at an inflection point of C. In the diagram in (4.5) of birational morphisms we get isomorphisms after removing the -1-curve on $\mathcal{X}_p$, which by abuse of notation will also be denoted by E_4, in the middle all the E_i and R, and on the right the line L.

$$\mathcal{X}_p \longleftarrow \tilde{\mathcal{X}}_p \longrightarrow \mathbb{P}^2_{\mathbb{F}_p} \tag{4.5}$$

This proves that the complement of the -1-curve E_4 in $\mathcal{X}_p$ is isomorphic to $\mathbb{A}^2_{\mathbb{F}_p}$. $\square$

COROLLARY 4.5.13. *The surface $\tilde{\mathcal{X}}_p$ is the generalized del Pezzo surface associated to Z'. Write $\tilde{\pi}\colon \tilde{\mathcal{X}}_p \to \mathbb{P}^2_{\mathbb{F}_p}$ for the associated blowup of the projective plane in 4 points in almost general position.*

The generalized del Pezzo surface $\tilde{\mathcal{X}}_p$ has five s-curves. Three -2-curves and a -1-curve form the support of the exceptional divisor $E_{\tilde{\pi}}$, and a -2-curve R is the strict transform of the tangent line L in p_0 to C along $\tilde{\pi}$.

We will fix coordinates for p_0 and the equation for the line L. This does not determine the equation for C uniquely. It does however uniquely determine the zero-dimensional ideal Z' up to an automorphism of $\mathbb{P}^2_{\mathbb{F}_p}$ which fixes p_0 and L.

LEMMA 4.5.14. *Assume without loss of generality that p_0 is the point $(0\colon 1\colon 0)$ and that L is given by $z = 0$. Let C be a cubic curve which passes through x, is smooth there, has L as the tangent line to C at x, and has an inflection point at x. Let Z' be the curvilinear subscheme associated to $\mathcal{I}_{C,p_0,4}$.*

There is a unique $\lambda \in \mathbb{F}_p^\times$ such that the cubic curve $x^3 - \lambda y^2 z = 0$ passes through Z'.

Proof. Consider the homogeneous cubic $f_{\text{hom}} \subseteq \mathbb{F}_p[x,y,z]$ defining C. We will consider the corresponding affine curve defined by $f = f_{\text{hom}}(x,1,z)$. Since this polynomial $f(x,z)$ defines a inflection point at $(0,0)$ it must contain the monomial x^3 and no other monomials which only contain x. Since L is the unique tangent line at $(0,0)$ the linear term of f is given by a multiple of z. So we can rescale f to $f = x^3 + z\kappa(x,z) - \lambda z$ where the degree of every monomial of κ is at least 1. Now note that xz and z^2 pass through Z' so this means that $f - z\kappa(x,z) = x^3 - \lambda z$ defines a cubic curve which passes through Z'.

Now if we had two such curves given by $x^3 = \lambda y^2 z$ and $x^3 = \lambda' y^2 z$ for different λ and λ', then we would find that the line L defined by $(\lambda - \lambda')z = 0$ passes through Z'. This would mean that $\deg(Z' \cap L) = \deg Z' = 4$, which is impossible since Z' lies in the intersection of L and C. □

We can assume without loss of generality that $\lambda = 1$ by rescaling the coordinate z. The curve defined by $x^3 = y^2 z$ has a inflection point at the smooth point $(0\colon 1\colon 0)$ so we can take this curve to be C.

COROLLARY 4.5.15. *The subscheme Z' is defined by the homogeneous ideal*

$$(x^3 - y^2 z, xz, z^2) \subseteq \mathbb{F}_p[x,y,z].$$

The birational map $\psi\colon \mathbb{P}^2_{\mathbb{F}_p} \dashrightarrow \tilde{\mathcal{X}}_p \to \mathcal{X}_p \subseteq \mathbb{P}^5_{\mathbb{F}_p}$ is defined by a basis of the vector space over $\mathbb{F}_p$ of cubic polynomials in the ideal $(x^3 - y^2 z, xz, z^2)$.

Proof. It is clear that the subscheme defined by $(x^3 - y^2 z, xz, z^2)$ lies on C. Also, any point on this scheme would have to satisfy $z^2 = 0$ and $x^3 = yz^2$. This shows that the subscheme defined by $(x^3 - y^2 z, xz, z^2)$ is only supported in p_0. Let us compute the degree of this subscheme on the local chart $y = 1$. We can rewrite the ideal as $(x^3 - z, xz, z^2) = (x^3 - z, x^4, x^6) = (x^3 - z, x^4)$, which clearly defines a degree 4 subscheme.

The last statement follows from Lemma 2.7.20. □

COROLLARY 4.5.16. *We have the following equality of effective divisors*

$$\operatorname{div}_{\mathcal{X}_p} l_1 = \operatorname{div}_{\mathcal{X}_p} l_2 = 5E_4.$$

Proof. We know that the divisor of zeroes of l_1 is of degree 5 and supported in -1-curves. By Proposition 4.5.12 we know that there is a unique -1-curve E_4 on $\mathcal{X}_\ell$ and this implies the result. □

Since the map $\psi\colon \mathbb{P}^2_{\mathbb{F}_p} \dashrightarrow \mathcal{X}_p \subseteq \mathbb{P}^5_{\mathbb{F}_p}$ is given by a basis of the cubics in the ideal $(x^3 - y^2z, xz, z^2)$ we see that there is a correspondence between the cubics in the ideal $(x^3 - y^2z, xz, z^2) \subseteq \mathbb{F}_p[x, y, z]$ and the sections in $\mathrm{H}^0(\mathcal{X}_p, \omega^\vee)$.

LEMMA 4.5.17. *The hyperplane section on $\mathcal{X}_p$ cut out by l_1 corresponds to the cubic z^3 up to a factor of $\mathbb{F}_p^\times$.*

Proof. Note that l_1 does not vanish on $\mathcal{X}_p \backslash E_4$. This proves that the associated cubic curve on $\mathbb{P}^2_{\mathbb{F}_p}$ does not meet $\mathbb{A}^2_{\mathbb{F}_p} = \mathbb{P}^2_{\mathbb{F}_p} \backslash L$. We see that this cubic curve must be given by a multiple of z^3. □

After fixing a multiple of z^3 which corresponds to l_1 we get an actual correspondence between the elements of $\mathrm{H}^0(\mathcal{X}_p, \omega^\vee)$ and the homogeneous cubic polynomials in $(x^3 - y^2z, xz, z^2)$.

DEFINITION 4.5.18. Let h be a linear form on $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ with coprime coefficients and let p be a prime for which $\mathcal{X}_p$ has a singular point of type A_4. The birational map $\pi\colon \mathcal{X}_p \dashrightarrow \tilde{\mathcal{X}}_p \to \mathbb{P}^2_{\mathbb{F}_p}$ induces an isomorphism $\kappa(\mathbb{P}^2_{\mathbb{F}_p}) \cong \kappa(\mathcal{X}_p)$. Let f_{hom} be the homogeneous polynomial over $\mathbb{F}_p$ such that $\frac{h}{l_1}$ corresponds to $\frac{f_{\mathrm{hom}}}{z^3}$ under this isomorphism. We will call f_{hom} and $f = f_{\mathrm{hom}}(x, y, 1)$ the *associated homogeneous and inhomogeneous polynomials* of h at p.

We will study hyperplane sections on $\mathcal{X}_p \subseteq \mathbb{P}^5_{\mathbb{F}_p}$ by looking at the corresponding cubic polynomial in three variables.

The following lemma is the first example and identifies the effective anticanonical divisors of $\mathcal{X}_p$ as cubic plane curves.

LEMMA 4.5.19. *The hyperplane sections of $\mathcal{X}_p \subseteq \mathbb{P}^5_{\mathbb{F}_p}$ which contain E_4 are those for which the associated homogeneous polynomial lies in the ideal*

$$(zx^2, z^2).$$

Proof. Let us work on the affine part given by $y = 1$. We see from Lemma 2.7.19 that the cubic forms for which the associated anticanonical divisor is supported on E_4 lie in the ideal

$$(x, z)(x^3 - z, xz, z^2) = (x^4 - xz, z^2, x^2z).$$

The homogeneous part of this ideal of degree 3 is clearly generated by zx^2 and z^2. □

4.6 Setup for the following sections

We have introduced a lot of notation over the last few sections. For convenience of the reader we will group the notation we will fix for the remainder of this chapter.

SETUP 4.6.1. We start by fixing one, hence both, of the following equivalent objects

» N, a subgroup of $\widehat{\mathbb{Z}}$ of index 5;

» K, a degree 5 Galois extension of $\mathbb{Q}$.

The correspondence between these objects is described in Definition 4.4.1.
Then we fix

» σ, a generator of $\mathrm{Gal}(K/\mathbb{Q})$;

» α, an element of $\mathcal{O}_K$ generating K.

This produces the following intermediate objects, which we will refer to

» m_α and m_{α^2}, the minimal polynomials of α and α^2;

» $\mathcal{Z}$, the subscheme of $\mathbb{P}^2_{\mathbb{Z}}$ defined by

$$(x^2 - yz, z^5 m_\alpha(x/z), z^5 m_{\alpha^2}(y/z)) \subseteq \mathbb{Z}[x, y, z];$$

» Γ_0, the subscheme of $\mathbb{P}^2_{\mathbb{Z}}$ defined by $x^2 = yz$;

» $\mathcal{B}$, the blowup of $\mathbb{P}^2_{\mathbb{Z}}$ in $\mathcal{Z}$;

» β, the blowup morphism $\mathcal{B} \to \mathbb{P}^2_{\mathbb{Z}}$;

» Γ, the strict transform of Γ_0 along $\beta\colon \mathcal{B} \to \mathbb{P}^2_{\mathbb{Z}}$.

These objects were used in the process of defining

» $\mathcal{X}_\alpha$ or $\mathcal{X}$, which is a subscheme of $\mathbb{P}^5_{\mathbb{Z}}$;

» ϑ, the birational map $\vartheta\colon \mathbb{P}^2_{\mathbb{Z}} \dashrightarrow \mathcal{X}$;

» δ, the morphism $\delta\colon \mathcal{B} \to \mathcal{X}$ which contracts Γ.

We also fix the following notation for schemes and morphisms defined over either $\mathbb{Q}$ or $\mathbb{F}_\ell$.

» X_α or X, the generic fibre of $\mathcal{X}$;

» Z and B, the generic fibres of $\mathcal{Z}$ and $\mathcal{B}$;

» $\tilde{\mathcal{B}}_\ell$, the minimal desingularization of $\mathcal{B}_\ell$;

» $\tilde{\mathcal{X}}_\ell$, the minimal desingularization of $\mathcal{X}_\ell$;

» $\tilde{\Gamma}_\ell$, the strict transform of $\tilde{\beta}_\ell\colon \tilde{\mathcal{B}} \to \mathbb{P}^2_{\mathbb{F}_\ell}$;

» $\tilde{\delta}_\ell$, the morphism $\tilde{\mathcal{B}}_\ell \to \tilde{\mathcal{X}}_\ell$ which contracts the -1-curve $\tilde{\Gamma}_\ell$;

- ρ_ℓ, the contraction of -2-curves $\tilde{\mathcal{B}}_\ell \to \mathcal{B}_\ell$;
- γ_ℓ, the contraction of -2-curves $\tilde{\mathcal{X}}_\ell \to \mathcal{X}_\ell$.

It is even possible to define schemes $\tilde{\mathcal{B}}$ and $\tilde{\mathcal{X}}$ over $\mathbb{Z}$, such that their fibres over $\mathbb{Z}$ are the minimal desingularizations of the corresponding fibres of $\mathcal{X}$ and $\mathcal{B}$. Also the morphisms ρ_ℓ, γ_ℓ have $\tilde{\delta}_\ell$ relative versions over $\mathbb{Z}$. We will not define these objects and one should keep in mind that part of the diagram in (4.6) is only defined on the fibres over $\mathbb{Z}$.

$$\begin{tikzcd}
& \tilde{\mathcal{X}} \arrow[dl, "\gamma"] & & \tilde{\mathcal{B}} \arrow[ll, "\tilde{\delta}"] \arrow[dl, "\rho"] \arrow[dd, "\tilde{\beta}"] \\
\mathcal{X} & & \mathcal{B} \arrow[ll, "\delta"] \arrow[dr, "\beta"] & \\
& & & \mathbb{P}^2_{\mathbb{Z}}. \arrow[lllu, dashed, "\vartheta"]
\end{tikzcd} \tag{4.6}$$

Other notation which will reappear in this chapter:

- n, the conductor of N and K;
- α_i, the conjugates of α in K;
- $P_i = (\alpha_i : \alpha_i^2 : 1)$, the K-points on $\mathbb{P}^2_{\mathbb{Q}}$ in the support of Z;
- $\mathrm{dP}_5(N)$, $\mathrm{dP}_5(K)$ or when it makes sense $\mathrm{dP}_5(n)$, for the isomorphism class of X;
- l_1 and l_2, linear forms over $\mathbb{Z}$ with coprime coefficients considered as elements of $\mathcal{O}_{\mathbb{P}^5_{\mathbb{Z}}}(1)$.

We will want to consider integral points on an affine open of $\mathcal{X}$ by choosing

- h, a linear form over $\mathbb{Z}$ with coprime coefficients considered as an element of $\mathcal{O}_{\mathbb{P}^5_{\mathbb{Z}}}(1)$;
- $\mathcal{C}$, the hyperplane section on $\mathcal{X}$ defined by $h = 0$;
- $\mathcal{U}$, the complement of $\mathcal{C}$ in $\mathcal{U}$;
- C and U, the generic fibres of $\mathcal{C}$ and $\mathcal{U}$.

This allows us to consider

- $\mathcal{A}$, the class of the Azumaya algebra $\left(\frac{l_1}{h}, K/k, \sigma\right)$ in $\operatorname{Br} U$.

We will also write

» ℓ, for a general prime number;

» p, for a prime number which is totally ramified in K;

» $\mathfrak{l}$, a prime of K lying above ℓ;

» $\mathfrak{p}$, the prime of K lying above p.

Let $\mathcal{X}_p$ be a fibre with a singular point of type A_4. When dealing with such a fibre we use the following notation introduced in Section 4.5.4

» C, the cubic curve on $\mathbb{P}^2_{\mathbb{F}_p}$ given by $x^3 = y^2 z$;

» p_0, the $\mathbb{F}_p$-point $(0\colon 1\colon 0)$ on C;

» L, the line $z = 0$ tangent to C in p_0;

» Z', the curvilinear subscheme associated to the ideal sheaf $\mathcal{I}_{C,p_0,4}$;

» π, the birational map $\mathcal{X}_p \dashrightarrow \mathbb{P}^2_{\mathbb{F}_p}$ associated to Z';

» ψ, the birational inverse of π;

» E_i and R, the -2-curves E_1, E_2, E_3 and R, and the -1-curve E_4 on $\tilde{\mathcal{X}}_p$;

» E_4, the image of $E_4 \subseteq \tilde{\mathcal{X}}_p$ along $\delta_p\colon \tilde{\mathcal{X}}_p \to \mathcal{X}_p$;

» f and f_{hom}, the associated inhomogeneous and homogeneous polynomial of h at p.

4.7 Arithmetic of $\mathcal{U}$

Using the projective model $\mathcal{X}$ we can construct a model for affine surfaces with non-trivial algebraic Brauer group as described in Lemma 4.1.4.

Definition 4.7.1. Let h be a primitive linear form defining a hyperplane in $\mathbb{P}^5_{\mathbb{Z}}$. Denote by $\mathcal{C}$ the curve on $\mathcal{X}$ defined by this hyperplane and write $\mathcal{U}$ for the complement of $\mathcal{C}$ in $\mathcal{X}$. We will denote the generic fibres of these objects by C and U. If we want to stress the dependence on h we might add it as a subscript.

Note that if C is geometrically irreducible then $\mathrm{Br}_1 U / \mathrm{Br}\, k$ is a cyclic group of order 5 by Proposition 4.1.3. To determine whether this might give an obstruction to the Hasse principle for integral points we are first interested in points on $\mathcal{U}$ over all completions of $\mathbb{Z}$.

Lemma 4.7.2. *We have that $U(\mathbb{Q})$ is not empty and the same holds for $\mathcal{U}(\mathbb{Z}_\ell)$ if ℓ is a prime which is at least 7. The same is true for all odd ℓ for which the fibre $\mathcal{X}_\ell$ is smooth.*

Proof. Rational points on an ordinary del Pezzo surface of degree 5 are Zariski dense by Proposition 2.8.2. We conclude that the set of rational points on X cannot be contained in C. This proves the first statement.

Now let $\ell \geq 7$ be a prime. Since h is primitive we find that $\mathcal{C}_\ell$ is a degree 5 curve of arithmetic genus 1 in $\mathbb{P}^5_{\mathbb{F}_\ell}$. From the degree we see that $\mathcal{C}_\ell$ consists of at most 5 geometrically irreducible components. From the genus we deduce that at most one of these components is of arithmetic genus 1. The number of $\mathbb{F}_\ell$-points on an irreducible genus 0 curve is bounded by $\ell + 1$ and for a genus 1 curve it is at most $\ell + 1 + 2\sqrt{\ell}$. It now follows using the result in Lemma 4.5.2 that

$$\#\mathcal{U}(\mathbb{F}_\ell) = \#\mathcal{X}(\mathbb{F}_\ell) - \#\mathcal{C}(\mathbb{F}_\ell) \geq (\ell^2 + 1) - (5\ell + 5 + 2\sqrt{\ell}). \tag{4.7}$$

It is easily checked that the right hand side is at least 4 for $\ell \geq 7$. As there are at most two singular points on each fibre by Proposition 4.5.8 we find a smooth $\mathbb{F}_\ell$-point on $\mathcal{U}_\ell$ which lifts using Hensel's lemma to a $\mathbb{Z}_\ell$-point.

Now assume that $\mathcal{X}_\ell$ is smooth. That implies that m_α modulo ℓ is separable and either all roots are defined over $\mathbb{F}_\ell$ or over $\mathbb{F}_{\ell^5}$. In the first case the approach in (4.7), using the exact count $\#\mathcal{X}(\mathbb{F}_\ell) = \ell^2 + 5\ell + 1$, yields $\#\mathcal{U}(\mathbb{F}_\ell) \geq 1$. In the second case the fibre $\mathcal{X}_\ell$ is an interesting del Pezzo surface of degree 5 over $\mathbb{F}_\ell$. It follows from Lemma 4.1.6 that the geometrically irreducible components of a hyperplane section are all of degree 1 or 5. In the first case we find that $\mathcal{C}_\ell$ is the orbit of a geometric -1-curve which is defined over $\mathbb{F}_{\ell^5}$ and there are obviously no $\mathbb{F}_\ell$-points on $\mathcal{C}$. In the latter case we find that the hyperplane section is a geometrically irreducible curve of arithmetic genus 1. So we find

$$\#\mathcal{U}(\mathbb{F}_\ell) = \#\mathcal{X}(\mathbb{F}_\ell) - \#\mathcal{C}(\mathbb{F}_\ell) \geq (\ell^2 + 1) - (\ell + 1 + 2\sqrt{\ell})$$

which is positive for $\ell \geq 3$. □

For primes over which the fibre $\mathcal{X}_\ell$ is singular there might be better bounds if one fixes the multiplicities of the factors of m_α modulo ℓ. We will only need the following result.

LEMMA 4.7.3. *Let p be an odd prime such that $\mathcal{X}_p$ has a singularity of type A_4. The set $\mathcal{U}(\mathbb{Z}_p)$ is non-empty.*

In particular using Corollary 4.4.3 we see that if p is ramified in K, then $\mathcal{U}_p$ admits a $\mathbb{Z}_p$-point

Proof. Recall that $\mathcal{X}_p \subseteq \mathbb{P}^5_{\mathbb{F}_p}$ is a singular del Pezzo surface and $\mathcal{U}_p$ is the intersection of $\mathcal{X}_p$ with a fixed affine chart $\mathbb{A}^5_{\mathbb{F}_p}$ defined by $h \neq 0$. Furthermore, E_4 is a line in $\mathbb{P}^5_{\mathbb{F}_p}$ which lies on $\mathcal{X}_p$.

From the isomorphism between $\mathcal{X}_p \backslash E_4$ and $\mathbb{A}^2_{\mathbb{F}_p}$ we see that any $\mathbb{F}_p$-point of $\mathcal{U}_p \backslash E_4$ is smooth. So we can lift such a point to a $\mathbb{Z}_p$-point. So let us prove that $(\mathcal{U}_p \backslash E_4)(\mathbb{F}_p) \cong (\mathbb{A}^2_{\mathbb{F}_p} \backslash V(f))(\mathbb{F}_p)$ is non-empty, where f is the associated inhomogeneous polynomial associated to h. So it is enough to prove that this associated polynomial f of h is non-zero at some point of the affine plane. We know that f is non-zero and of degree at most 3. A geometrically irreducible affine plane cubic, conic or line with a rational point at infinity contains at most $p+2\sqrt{p}$, p or p points respectively. So we see that f vanishes in at most $2p$ points which happens when f cuts out two parallel lines. Since $\#\mathbb{A}^2(\mathbb{F}_p) = p^2$ there is an $\mathbb{F}_p$-point on the affine plane which is not a zero of f. □

On the other hand, the bound for the smooth fibres cannot be sharpened in general; we will see examples where $\mathcal{X}_2$ is smooth but $\mathcal{U}(\mathbb{Z}_2)$ is empty.

4.8 Computation of the invariant maps

The following section is about computing the invariant maps for the element $\mathcal{A}$ of the Brauer group of U. At the infinite prime of $\mathbb{Q}$ we see that the map

$$\operatorname{inv}_\infty \mathcal{A}\colon U(\mathbb{R}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

is zero because $\mathcal{A}$ is of odd order. So from now on we will only consider the finite primes. At points in $\mathcal{U}(\mathbb{Z}_\ell)$ for a finite prime ℓ we have the following result.

LEMMA 4.8.1. *Fix a prime ℓ and let P be a point in $\mathcal{U}(\mathbb{Z}_\ell)$ such that $\frac{l_1}{h}(P)$ is defined and invertible modulo ℓ. Then*

$$\operatorname{inv}_\ell \mathcal{A}(P)$$

is $0 \in \mathbb{Q}/\mathbb{Z}$ precisely if the image of $\frac{l_1}{h}(P) \in \mathbb{Z}_\ell^\times$ under the homomorphism $\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times$ lies in N.

Proof. Let P be such a point. Then $\mathcal{A}(P) \in \operatorname{Br}(\mathbb{Q}_\ell)$ is simply the class of the cyclic algebra $\left(\frac{l_1}{h}(P), \sigma\right)$. Proposition 1.3.2 tells us that the cyclic algebra $\left(\frac{l_1}{h}(P), \sigma\right)$ over $\mathbb{Q}_\ell$ is trivial in the Brauer group precisely when $\frac{l_1}{h}(P)$ is a norm in the extension $K_{\mathfrak{l}}/\mathbb{Q}_\ell$ for a prime $\mathfrak{l}$ lying above l. The group $N_{K_{\mathfrak{l}}/\mathbb{Q}_\ell}(K_{\mathfrak{l}}^\times)$ is the kernel of the top map in (4.4) in the proof of Proposition 4.4.2. This group is exactly the kernel of $\mathbb{Q}_\ell^\times \to \operatorname{Gal}(K/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times/N$ since the map $\operatorname{Gal}(K_{\mathfrak{l}}/\mathbb{Q}_\ell) \to \operatorname{Gal}(K/\mathbb{Q})$ is an inclusion. □

Since the image of $\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times$ is a subset of N for all but finitely primes we have the following result.

COROLLARY 4.8.2. *Consider a model $\mathcal{U}/\mathbb{Z}$ as before of conductor n. Let ℓ be a prime which does not ramify in K and $P \in \mathcal{U}(\mathbb{Z}_\ell)$ be a point where l_1 or l_2 is invertible modulo ℓ. Then we have $\operatorname{inv}_\ell \mathcal{A}(P) = 0$.*

Proof. We saw in the proof of Proposition 4.4.2 that ℓ is unramified in K precisely when the image of $\mathbb{Z}_\ell^\times \to \widehat{\mathbb{Z}}^\times$ lies in N. This proves the claim. □

For primes $p \equiv 1 \mod 5$ which divide the conductor of such a subgroup N, i.e. the tamely ramified primes of K, we have the following result.

COROLLARY 4.8.3. *Let p a prime which is tamely ramified in K. This implies that $p \equiv 1 \mod 5$. Write W for the set of $\mathbb{Z}_p$-points P on $\mathcal{U}$ where $\frac{l_1}{h}(P)$ is invertible in $\mathbb{Z}_p$ and let $q\colon W \to (\mathcal{U}_p \backslash E_4)(\mathbb{F}_p)$ be the reduction map. This map is surjective and the invariant map $\mathrm{inv}_p \mathcal{A}$ on W can be computed as*

$$W \stackrel{q}{\twoheadrightarrow} (\mathcal{U}_p \backslash E_4)(\mathbb{F}_p) \stackrel{\frac{l_1}{h}}{\to} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^5 \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

where the second map sends a point P to the class of $\frac{l_1}{h}(P)$ modulo fifth powers and the last map is a group isomorphism onto the unique subgroup of $\mathbb{Q}/\mathbb{Z}$ of order 5.

In particular we see that for a point $P \in \mathcal{U}(\mathbb{Z}_p)$ which does not reduce modulo p to a point on E_4 that $\mathrm{inv}_p \mathcal{A}(P) = 0$ precisely if $\frac{l_1}{h}(P)$ is a fifth power modulo p.

Proof. Consider an $\mathbb{F}_p$-point $\bar{P}$ in $\mathcal{U}_p \backslash E_4$. As $\frac{l_1}{h}(\bar{P})$ is invertible the point $\bar{P}$ cannot lie in the zero locus of l_1. By Lemma 4.5.5 all singular points lie on the intersection of the zero loci of l_1 and l_2. So by assumption $\bar{P}$ must be a smooth point. This implies that $\bar{P}$ lifts using Hensel's lemma to a point P in W. This shows that q is surjective.

The last statement follows from Lemma 4.4.4. □

These last two results are a restatement of the fact that in unramified extensions of local fields every norm is a unit, and agrees with the fact that in a totally but tamely ramified extension every principal unit is a norm.

For the wildly ramified prime 5 the situation is a little different.

COROLLARY 4.8.4. *Suppose that 5 is ramified in K and let $P \in \mathcal{U}(\mathbb{Z}_5)$ be a point which does not lie in the zero locus of both l_1 and l_2 modulo 5. Then P lies in the kernel of $\mathrm{inv}_5 \mathcal{A}$ precisely if for one i, or equivalently both, we have $\frac{l_i}{h}(P) \in \{\pm 1, \pm 7\}$ modulo 5^2.*

Proof. This proof is similar to the proof of the previous corollary and again relies on Lemma 4.4.4. □

We see that in a point P over $\mathbb{Z}_\ell$ not reducing to the zero locus of both l_1 and l_2 modulo ℓ the value of $\mathrm{inv}_\ell \mathcal{A}(P)$ follows from these three corollaries. We will now show how to compute the invariant map on the remaining points or why we should not bother to do so.

4.8.1 The invariant map for unramified primes

The invariant map is often best understood at unramified primes. This is also the case here.

LEMMA 4.8.5. *Suppose a prime ℓ splits completely in K. The map*

$$\operatorname{inv}_\ell \mathcal{A}\colon \mathcal{U}(\mathbb{Z}_\ell) \to \mathbb{Q}/\mathbb{Z}$$

is identically equal to zero.

Proof. Let P be a $\mathbb{Z}_\ell$-point of $\mathcal{U}$. The evaluation map $\operatorname{Br} U \to \operatorname{Br} \mathbb{Q}_\ell, \mathcal{A} \mapsto \mathcal{A}(P)$ factors through $\operatorname{Br} U_{\mathbb{Q}_\ell}$. For a prime $\tilde{\mathfrak{l}}$ above a completely split prime ℓ we find that $K_{\tilde{\mathfrak{l}}} = \mathbb{Q}_\ell$. Since $\mathcal{A}_{\mathbb{Q}_\ell} \in \operatorname{Br} U_{\mathbb{Q}_\ell}$ is split by $K_{\tilde{\mathfrak{l}}}$ we see that it is trivial and so is the image $\mathcal{A}(P)$ in $\operatorname{Br} \mathbb{Q}_\ell$. □

For inert primes we have similar, but slightly weaker, result.

LEMMA 4.8.6. *Suppose that ℓ is an inert prime. The map* inv_ℓ *is identically equal to zero if $\mathcal{U}_\ell$ is smooth over $\mathbb{F}_\ell$. If $\mathcal{U}_\ell$ is singular, then* inv_ℓ *is zero on the points in $\mathcal{U}(\mathbb{Z}_\ell)$ which do not reduce to the singular point of $\mathcal{U}_\ell$.*

Note that by Lemma 4.5.9 that $\mathcal{X}_\ell$ has at most one singular point. So the same is true for $\mathcal{U}_\ell$.

Proof. Note that inv_ℓ being constant on the indicated point sets follows from [6, Theorem 1]. We will however need to prove a stronger result.

There is a correspondence between the factors of m_α over $\mathbb{Q}_\ell$ and primes of K dividing ℓ. Since ℓ is inert in K there is a unique prime $\mathfrak{l}$ in K lying above ℓ. This shows that m_α is irreducible over $\mathbb{Q}_\ell$ and hence $U_{\mathbb{Q}_\ell}$ is an interesting del Pezzo surface. In particular, there are no $\mathbb{Q}_\ell$-points on U in the zero locus of both l_1 and l_2.

Consider a point $P \in \mathcal{U}(\mathbb{Z}_\ell)$. By the above discussion we see that $\frac{l_i}{h}(P) \neq 0 \in \mathbb{Z}_\ell$ for at least one i. Assume without loss of generality that $i = 1$. We will use the representation $\left(\frac{l_1}{h}, \sigma\right)$ of $\mathcal{A}$ to prove that $\operatorname{inv}_\ell \mathcal{A}(P)$ is equal to zero if P does not reduce to a singular point on $\mathcal{U}_\ell$. We will have to show that $\frac{l_1}{h}(P)$ is the of an element in $\mathcal{O}_{K_\mathfrak{l}}$. We have seen in Corollary 4.8.2 that only the valuation of $\frac{l_1}{h}(P)$ matters. We will show that this valuation is always a multiple of 5.

If $\frac{l_1}{h}(P)$ is a unit in $\mathbb{Z}_\ell$ then this is clear. So suppose ℓ divides $\frac{l_1}{h}(P)$ and let $\bar{P} \in \mathcal{U}(\mathbb{F}_\ell)$ be the reduction of P modulo ℓ. This means that $\bar{P}$ lies on the zero locus of l_1 on $\mathcal{U}_\ell \subseteq \mathcal{X}_\ell$. By Lemma 4.5.9 there are two possibilities for this zero locus.

If m_α is irreducible in $\mathbb{F}_\ell$ then $\mathcal{X}_\ell$ is an interesting del Pezzo surface. So the zero locus of l_1 consists of five conjugate lines. In particular there are no $\mathbb{F}_\ell$-points in the zero divisor of l_1.

If m_α reduces to the fifth power of a linear function modulo ℓ then $\mathcal{X}_\ell$ contains one line E_4 and one singular point which lies on this line. Locally around $\bar{P}$ the closed subscheme E_4 is Cartier since $\bar{P}$ is assumed to be smooth. This proves that in the local ring at $\bar{P}$ the function $\frac{l_1}{h}$ is the fifth power of the function defining E_4, since $\operatorname{div}_{\mathcal{X}_\ell} l_1 = 5E_4$. This proves that the valuation of $\frac{l_1}{h}(P)$ is a multiple of 5.

We conclude that $\operatorname{inv}_\ell \mathcal{A}(P) = 0$ for all indicated points $P \in \mathcal{U}(\mathbb{Z}_\ell)$. □

4.8.2 The invariant map for tamely ramified primes

Let us consider the case of a prime p which is ramified in K. By construction of the field K, the only primes which can be ramified are the primes 5 and the ones which are $1 \mod 10$. The prime 5 is wildly ramified, but we will first consider the tamely ramified primes. By Corollary 4.8.3 we see that the invariant map on $\mathbb{Z}_p$-points is largely determined by the $\mathbb{F}_p$-points of $\mathcal{U}_p$ (see also [6, Theorem 1]).

Unlike for the unramified primes we will see that $\operatorname{inv}_p \mathcal{A}$ is only constant in an obvious situation and in all other cases it takes many values. To prove these results we will first look at the following lemmas on affine curves over $\mathbb{F}_p$ which we will translate back to $\mathcal{X}_p$ using the isomorphism in Proposition 4.5.12.

LEMMA 4.8.7. *Fix a prime $p \geq 5$ and let $f \in \mathbb{F}_p[x, y]$ be a non-constant irreducible polynomial of degree $d \leq 3$. Also assume that*

» *if $d = 3$ the projective closure of the corresponding affine curve is geometrically integral and intersects the line at infinity in a single point with multiplicity 3;*

» *if $d = 2$ the corresponding curve either has two distinct rational points at infinity, or it has a single point at infinity and is geometrically integral.*

Then the map $f \colon \mathbb{F}_p^2 \to \mathbb{F}_p$ is surjective.

Proof. Let us write $f_{\mathrm{hom}} \in \mathbb{F}_p[x, y, z]$ for the homogenization of f. We can now consider the following cases depending on the degree of f.

Case 1: f is a linear polynomial. In this case f is a non-constant linear map, and it is clear that it takes all values in $\mathbb{F}_p$ on $\mathbb{F}_p^2$.

Case 2: f is a quadratic polynomial. There are two cases to consider. First assume f_{hom} has two distinct rational solutions at $z = 0$. Without loss of generality these points are $(1\colon 0\colon 0)$ and $(0\colon 1\colon 0)$ and then f must be of the form $\kappa xy + \lambda x + \mu y + \nu$, where $\kappa \neq 0$. Now fix y_0 such that $\kappa y_0 + \lambda$ is non-zero. Then we see that $f(x, y_0) = x(\kappa y_0 + \lambda) + \mu y_0 + \nu$ assumes all values in $\mathbb{F}_p$.

Now consider the case where f_{hom} is geometrically integral and has a single solution with $z = 0$. Assume without loss of generality that this point is $(0\colon 1\colon 0)$. This implies that f can be written as $f = \kappa x^2 + \lambda x + \mu y + \nu$. Since the curve defined by f_{hom} is geometrically integral we find $\mu \neq 0$ which directly implies that f is surjective.

Case 3: f is a cubic polynomial. We know that f has a single point at infinity of multiplicity 3. Assume that this point is $(0\colon 1\colon 0)$. We will show that f is surjective by proving that the projective cubic plane curve C_λ defined by the cubic form $f_{\mathrm{hom}} - \lambda z^3$ has an $\mathbb{F}_p$-point satisfying $z \neq 0$ for all $\lambda \in \mathbb{F}_p$.

We will first show that each of these p plane curves C_λ does not split into three lines over $\bar{\mathbb{F}}_p$. Note that a cubic plane curve defined by a cubic homogeneous polynomial F passes through $(0\colon 1\colon 0)$ with multiplicity three and splits into three lines precisely when F is independent of y. Since C_0 is geometrically integral by assumption we see that f_{hom} does depend on y. So the same holds for all $f_{\text{hom}} - \lambda z^3$ and none of the curves C_λ splits into three lines over $\bar{\mathbb{F}}_p$.

So each plane curve C_λ is either geometrically integral or factors into a linear and quadratic factor. We will prove in each case that the curve C_λ has at least two $\mathbb{F}_p$-points, and since it has single point $(0\colon 1\colon 0)$ at infinity it will have an $\mathbb{F}_p$-points satisfying $z \neq 0$.

A geometrically integral cubic curve has at least $p + 1 - 2\sqrt{p}$ points and as $p \geq 5$ there must be a point away from infinity. In the second case we have a projective curve consisting of line and a conic defined over $\mathbb{F}_p$, both with the given point $(0\colon 1\colon 0)$ at infinity. Either component will have rational points on the affine part defined by $z \neq 0$.

We see that for all $\lambda \in \mathbb{F}_p$ the curve C_λ has a point satisfying $z \neq 0$ and we conclude that f is surjective on the affine plane. □

If f defines a non-reduced conic we have the following weaker statement.

LEMMA 4.8.8. *Let $f \in \mathbb{F}_p[x]$ be the square of a non-constant linear function over $\mathbb{F}_p$ with root ρ. The map $f\colon \mathbb{F}_p \backslash \{\rho\} \to \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5$ is surjective.*

LEMMA 4.8.9. *Fix a prime p and let f_{hom} be a homogeneous cubic polynomial in the ideal $(x^3 - y^2 z, xz, z^2)$ over $\mathbb{F}_p$. The polynomial $f = f_{hom}(x, y, 1)$ either*

- *is constant;*
- *vanishes on two distinct parallel lines on $\mathbb{A}^2_{\mathbb{F}_p}$;*
- *satisfies the conditions in Lemma 4.8.7, or*
- *is independent of y and satisfies the conditions in Lemma 4.8.8.*

In the second case we allow the lines to be conjugated over $\mathbb{F}_p$.

Proof. Let us write $f_{\text{hom}} = \kappa x^3 + z(\mu(x, y)x + \nu(x, y, z)z - \kappa y^2)$ where μ and ν are homogeneous linear polynomials in the indicated variables. In the case that $\kappa = 0$ the polynomial f is of degree at most 2 and all points with $z = 0$ are rational points. All these polynomials are covered among the four cases.

If $\kappa \neq 0$ we have a cubic polynomial $f = \kappa x^3 + (\mu(x, y)x + \nu(x, y, 1) - \kappa y^2)$, which has an inflection point at $(0\colon 1\colon 0)$ and the result of Lemma 4.8.7 holds for such f. □

We have seen a surjectivity statement for the last two of these four cases. In the first case we will not find such a result and in the second we have the following proposition, which applies since f is going to be the product of two distinct lines precisely when it is independent of y.

LEMMA 4.8.10. *Let p be a prime and $f \in \mathbb{F}_p[x]$ a quadratic polynomial with distinct roots ρ_1 and ρ_2 in $\bar{\mathbb{F}}_p$. The homomorphism $f\colon \mathbb{F}_p \backslash \{\rho_1, \rho_2\} \to \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5$ is surjective when $p \geq 31$.*

Proof. Write $f = ax^2 + bx + c$ with $a \neq 0$ and fix a $\lambda \in \mathbb{F}_p^\times$. We will prove that if $p \geq 31$ there exist $u, v \in \mathbb{F}_p$ with v invertible, such that $f(u) = \lambda v^5$. Consider the affine hyperelliptic curve $f(x) = \lambda y^5$, which is smooth because f has distinct roots. The smooth birational model for this curve is of genus 2 and has at least $p + 1 - 4\sqrt{p}$ points, one of which does not lie on the affine part given by $f(x) = \lambda y^5$ and at most two points satisfy $y = 0$. So the number of $u, v \in \mathbb{F}_p$ with v invertible satisfying $f(u) = \lambda v^5$ is at least $p + 1 - 4\sqrt{p} - 3$. This is positive if $p \geq 31$, which proves the statement. □

Remark. One can check that if $p = 11$ the map $f \colon \mathbb{F}_p \backslash \{\rho_1, \rho_2\} \to \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5$ is never surjective; the image of $f \colon \mathbb{F}_{11} \backslash \{\rho_1, \rho_2\} \to \mathbb{F}_{11}^\times / (\mathbb{F}_{11}^\times)^5$ for any separable quadratic polynomial f is of size 4.

We have seen that the cubics in $(x^3 - y^2 z, xz, z^2)$ correspond to the effective divisors of degree 3 on $\mathbb{P}^2_{\mathbb{F}_p}$ which pull back to effective anticanonical divisors on $\mathcal{X}_p$. Considering the different bounds in Lemma 4.8.7, Lemma 4.8.8 and Lemma 4.8.10 we get a trichotomy of effective anticanonical divisors on $\mathcal{X}$.

DEFINITION 4.8.11. Let p be a prime which is ramified in K, h an irreducible linear form on $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ and f the associated inhomogeneous polynomial of h at p. We say that h at the prime p is of

» *class I* if f is constant;

» *class II* if f vanishes on two distinct parallel lines in $\mathbb{A}^2_{\mathbb{F}_p}$;

» *class III* in all other cases.

We have seen that these three classes partition the five-dimensional projective space of linear forms on $\mathcal{X}_p$ over $\mathbb{F}_p$. As the invariant map for tamely ramified primes is determined by the reduction of a point modulo p we get the following result.

THEOREM 4.8.12. *Let h be a linear form on the surface $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ constructed using a degree 5 number field K. Let p be a prime which is tamely ramified in K.*

The invariant map $\mathrm{inv}_p\, \mathcal{A} \colon \mathcal{U}_h(\mathbb{Z}_p) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$

» *is constant if h is of class I;*

» *misses exactly one value in $\frac{1}{5}\mathbb{Z}/\mathbb{Z}$ if h is of class II and $p = 11$;*

» *is surjective if h is of class II and $p \geq 31$;*

» *is surjective if h is of class III.*

Since p is congruent to 1 modulo 10 this covers all possible cases.

Proof. We have a birational map $\pi \colon \mathcal{X}_p \dashrightarrow \mathbb{P}^2_{\mathbb{F}_p}$ such that the isomorphism on function fields identifies $\frac{l_1}{h}$ on $\mathcal{X}_p$ with $\frac{z^3}{f_{\mathrm{hom}}}$ on $\mathbb{P}^2_{\mathbb{F}_p}$. On the projective plane we have the line L given by $z = 0$ and on $\mathcal{X}_p$ the -1-curve E_4 given by $l_1 = 0$, such that the birational map π restricts to an isomorphism $\mathcal{X}_p \backslash E_4 \cong \mathbb{P}^2_{\mathbb{F}_p} \backslash L \cong \mathbb{A}^2_{\mathbb{F}_p}$ as we saw in Proposition 4.5.12.

This proves the following chain of isomorphisms

$$\mathcal{U}_p \backslash E_4 \cong \mathcal{X}_p \backslash (V(h) \cup E_4) \cong \mathbb{P}^2_{\mathbb{F}_p} \backslash (V(f_{\mathrm{hom}}) \cup L) \cong \mathbb{A}^2_{\mathbb{F}_p} \backslash V(f).$$

Define the set W of $\mathbb{Z}_p$-points P on $\mathcal{U}$ where $\frac{l_1}{h}(P)$ is invertible in $\mathbb{Z}_p$. The reduction map $q\colon W \to (\mathcal{U}_p \backslash E_4)(\mathbb{F}_p)$ is surjective by Corollary 4.8.3.

We dehomogenize the function fields on the affine schemes $\mathcal{U}_p$ and $\mathbb{A}^2_{\mathbb{F}_p}$ using $l_1 = 1$ and $z = 1$ to find the commutative diagram in (4.8) which can be used to compute the invariant map for points in W.

$$\begin{tikzcd}
W \arrow[r, "q"] & (\mathcal{U}_p \backslash E_4)(\mathbb{F}_p) \arrow[r, "\frac{l_1}{h} = \frac{1}{h}"] \arrow[d, "\cong"] & \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5 \arrow[r] \arrow[d, equal] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\
 & \left(\mathbb{A}^2_{\mathbb{F}_p} \backslash V(f)\right)(\mathbb{F}_p) \arrow[r, "\frac{1}{f}"] & \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5 \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd} \tag{4.8}$$

Now if h is of class I or II we get from Lemma 4.5.19 that h vanishes along E_4 and so $W = \mathcal{U}_p(\mathbb{Z}_p)$. By the surjectivity of $q\colon \mathcal{U}_p(\mathbb{Z}_p) \to (\mathcal{U}_p \backslash E_4)(\mathbb{F}_p)$ and the injectivity of $\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5 \to \mathbb{Q}/\mathbb{Z}$ we see that $\mathrm{inv}_p\, \mathcal{A}\colon \mathcal{U}_p(\mathbb{Z}_p) \to \mathbb{Q}/\mathbb{Z}$ has the same image as the map $\frac{1}{f}\colon \left(\mathbb{A}^2_{\mathbb{F}_p} \backslash V(f)\right)(\mathbb{F}_p) \to \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^5$. If h is of class I at p, then f is constant by definition. The statements for h of class II follow from Lemma 4.8.10 and the remark following this lemma.

Now assume that h is of class III. The surjectivity of q, Lemma 4.8.7 and Lemma 4.8.8 combine to show that $\mathrm{inv}_p\, \mathcal{A}$ is surjective on the set W of $\mathbb{Z}_p$-points of $\mathcal{U}$ not reducing to E_4 so it is definitely surjective on $\mathcal{U}(\mathbb{Z}_p)$. □

In the cases where $\mathrm{inv}_p\, \mathcal{A}\colon \mathcal{U}(\mathbb{Z}_p) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ is surjective we cannot get a Brauer–Manin obstruction to the integral Hasse principle. In particular we have the following result coming from Lemma 4.5.19.

COROLLARY 4.8.13. *Let p be a prime which is tamely ramified in K and let h define a hyperplane section on $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ such that the -1-curve $E_4 \subseteq \mathcal{X}_p$ does not lie in the zero locus of the reduction of h modulo p. The invariant map $\mathrm{inv}_p\, \mathcal{A}\colon \mathcal{U}_h(\mathbb{Z}) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ is surjective.*

This shows that a Brauer–Manin obstruction to the integral Hasse principle will not exist if h does not cut out the unique -1-curve over each tamely ramified prime. If it does then by the isomorphism in Proposition 4.5.12 we see that $\mathcal{U}_p$ is isomorphic to an open subscheme of $\mathbb{A}^2_{\mathbb{F}_p}$ which generally simplifies the situation.

4.8.3 The invariant map for the wildly ramified prime 5

We have looked at the invariant maps at unramified and tamely ramified primes. The last case is that of wildly ramified primes. The only prime which can be wildly ramified in our number fields K of degree 5 is the prime 5 which happens precisely if 5 divides the conductor n.

We have already seen a useful result in Corollary 4.8.4. We will also make frequent use of the following easy lemma.

LEMMA 4.8.14. *Two different lifts to $(\mathbb{Z}/25\mathbb{Z})^\times$ of an element $(\mathbb{Z}/5\mathbb{Z})^\times$ lie in different cosets of the subgroup $\{\pm 1, \pm 7\} \subseteq (\mathbb{Z}/25\mathbb{Z})^\times$.*

Now let us show that in many cases the invariant map is surjective.

LEMMA 4.8.15. *Suppose that 5 is ramified in K. Then*

$$\mathrm{inv}_5\, \mathcal{A} \colon \mathcal{U}_h(\mathbb{Z}_5) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$$

is surjective if h is not of class I.

Proof. Pick coordinates u_i on $\mathbb{P}^5_{\mathbb{F}_5}$ and x, y and z on $\mathbb{P}^2_{\mathbb{F}_5}$ such that the birational map

$$\psi \colon \mathbb{P}^2_{\mathbb{F}_5} \dashrightarrow \mathcal{X}_5$$

is given by $(x, y, z) \mapsto (z^3, xz^2, yz^2, x^2z, xyz, y^2z - x^3)$ and we find an isomorphism after restricting to the affine opens $\mathbb{A}^2_{\mathbb{F}_5}$ and $\mathcal{X}_5 \backslash E_4$ respectively given by $z = 1$ and $u_0 = 1$. The size of the image of $\mathrm{inv}_5\, \mathcal{A} \colon \mathcal{U}_h(\mathbb{Z}_5) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ only depends on $\mathcal{A}$ up to constants. Since we also know that $l_1 \mod 5$ is a multiple of u_0, we can assume without loss of generality that $u_0 \equiv l_1 \mod 5$.

Pick an $\mathbb{F}_5$-point $\bar{P}$ on $\mathcal{V} := \mathcal{U}_5 \backslash E_4$. Recall that the map ψ restricts to an isomorphism on $\mathcal{V}$ to an open subscheme of $\mathbb{A}^5_{\mathbb{F}_5}$. Then $\bar{P}$ is an $\mathbb{F}_5$-point of $\mathcal{X}$ which does not lie in the zero locus of h and l_1. This guarantees that $\bar{P}$ is a smooth point and $\lambda := \frac{l_1}{h}(\bar{P})$ is defined and invertible modulo 5. We will show that at the $\mathbb{Z}_5$-points P reducing to $\bar{P}$ the function $\frac{l_1}{h}$ assumes either one or five values modulo 25.

Let us work with $\frac{h}{l_1}$ which on $\mathcal{V}$ becomes

$$h_{\mathrm{aff}} = a_0 + a_1u_1 + a_2u_2 + a_3u_3 + a_4u_4 + a_4u_5.$$

Now let $\vec{x} = (x_1, x_2, x_3, x_4, x_5)$ be a 5-tuple of integers reducing to $\bar{P} \in \mathcal{V}$. We will first show that the lifts of $\bar{P}$ to points in $\mathcal{X}(\mathbb{Z}/25\mathbb{Z})$ are $\vec{x} + 5\vec{w}$ where $\vec{w}$ is any vector in a translation of the tangent space of $\mathcal{V}$ at $\bar{P}$.

Suppose that $\mathcal{X}$ is given by polynomials g_j in the variables u_i. The tangent space at $\bar{P}$ is by definition

$$T_{\bar{P}}\mathcal{V} = \left\{ \vec{v} \in \mathbb{F}_5^5 : \sum_{i=1}^{5} \frac{dg_j}{du_i}(\bar{P})v_i \equiv 0 \mod 5 \right\}$$

and if $\vec{x} + 5\vec{w} \in \mathcal{X}(\mathbb{Z}/25\mathbb{Z})$ then for all j

$$0 \equiv g_j(\vec{x} + 5\vec{w}) \equiv g_j(\vec{x}) + 5\sum_{i=1}^{5} \frac{dg_j}{du_i}(\vec{x})w_i \mod 25$$

which proves the claim.

To compute h_{aff} at these lifts, let us write $\vec{a} = (a_1, a_2, a_3, a_4, a_5) \in \mathbb{Z}^5$. Then we find

$$h_{\text{aff}}(\vec{x} + 5\vec{w}) \equiv h_{\text{aff}}(\vec{x}) + 5\vec{a} \cdot \vec{w} \mod 25.$$

So we find all possible lifts modulo 25 of $h_{\text{aff}}(\vec{x}) \mod 5$ when $\vec{a} \cdot \vec{w}$ is not constant modulo 5 or equivalently that there exists a $\vec{v} \in T_P\mathcal{V}$ such that $5 \nmid \vec{a} \cdot \vec{v}$. This clearly does not happen when $\vec{a} \equiv 0 \mod 5$, so let us assume that one of the components of $\vec{a}$ is not divisible by 5.

We will prove that under this assumption we can find a point $\bar{P} \in \mathcal{V}(\mathbb{F}_p)$ and a tangent vector $\vec{v} \in T_{\bar{P}}\mathcal{V}$ such that $5 \nmid \vec{a} \cdot \vec{v}$. Using ψ we can translate this problem to $\mathbb{A}^2_{\mathbb{F}_5} \backslash \{f = 0\}$. Using the equations of ψ we see that the tangent space at $\psi(x, y)$ is generated by the vectors $\vec{v}_1 = (1, 0, 2x, y, -3x^2)$ and $\vec{v}_2 = (0, 1, 0, x, 2y)$. We are looking for a point (x, y) such that $f(x, y) = h_{\text{aff}} \circ \psi(x, y) \neq 0$ and $\vec{a} \cdot \vec{v}_1$ or $\vec{a} \cdot \vec{v}_2$ is non-zero.

Note that the degrees of $\vec{a} \cdot \vec{v}_1$ and $\vec{a} \cdot \vec{v}_2$ as polynomials in x and y are at most 2 and 1 and that at least one is non-zero since we assumed that $\vec{a} \neq 0 \mod 5$. If the linear equation $\vec{a} \cdot \vec{v}_2$ is non-zero it vanishes in at most five points of $\mathbb{A}^2(\mathbb{F}_5)$. If it is the zero polynomial then $\vec{a} \cdot \vec{v}_1$ is a non-zero linear polynomial. We see that $\vec{a} \cdot \vec{v}_1$ and $\vec{a} \cdot \vec{v}_2$ vanish simultaneously in at most 5 points. We have seen in the proof of Lemma 4.7.3 that f vanishes in at most $2p = 10$ points on $\mathbb{A}^2_{\mathbb{F}_p}$. So if $\vec{a} \not\equiv 0 \mod 5$ then there exists a point $\bar{P} \in \mathcal{V}(\mathbb{F}_5)$ and a vector $\vec{v}$ in its tangent space such that $\vec{a} \cdot \vec{v} \not\equiv 0 \mod 5$.

In particular if $\vec{a} \not\equiv 0 \mod 5$ we see that there exists a point $\bar{P} \in \mathcal{V}(\mathbb{F}_5)$ such that $\vec{a} \cdot \vec{v} \mod 5$ is surjective on the tangent space of $\bar{P}$, proving that h_{aff} assumes five values modulo 25 on $\mathbb{Z}_5$-points P reducing to $\bar{P}$. We see from Lemma 4.8.14 that h_{aff} assumes all values in $(\mathbb{Z}/25\mathbb{Z})^\times$ modulo fifth powers and so do $\frac{h}{l_1}$ on $\mathcal{U}_5$ and $\frac{l_1}{h}$ on $\mathcal{U}$. This proves the surjectivity of $\text{inv}_5\, \mathcal{A}$ in this case.

If on the other hand $\vec{a} \equiv 0 \mod 5$ we find that h_{aff} assumes only one value modulo 25 on $\mathbb{Z}_p$-points reducing to a fixed point $\bar{P} \in \mathcal{V}(\mathbb{F}_5)$. We also see that 5 cannot divide the coefficient of u_0 in h since it already divides all the other coefficients and so h is of class I. □

In particular we have proved the following result similar to Lemma 4.8.13.

COROLLARY 4.8.16. *Suppose that* 5 *divides the conductor n and consider a hyperplane section given by $h = 0$ on $\mathcal{X} \subseteq \mathbb{P}^5_{\mathbb{Z}}$ such that the -1-curve $E_4 \subseteq \mathcal{X}_5$ does not lie on the zero locus of the reduction of h modulo* 5*. The invariant map* $\text{inv}_5\, \mathcal{A} \colon \mathcal{U}_h(\mathbb{Z}) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ *is surjective.*

We can even classify all of the remaining hyperplane sections for which the evaluation map is not surjective.

THEOREM 4.8.17. *Suppose that* 5 *is ramified in K. Then* $\mathrm{inv}_5 \mathcal{A}\colon \mathcal{U}(\mathbb{Z}_5) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ *is not surjective precisely when there exist integers* λ, c_1 *and* c_3 *satisfying* $5 \nmid \lambda$, *and* $5 \mid c_1, c_3$ *or* $5 \nmid c_1$ *such that*

$$h \equiv \lambda l_1 + 5(c_1 u_1 + c_3 u_3) \mod 25$$

for specific hyperplane sections $u_1, u_3 \in \mathcal{O}_{\mathbb{P}^5_{\mathbb{Z}}}(1)$. *The invariant map is constant when* $5 \mid c_1, c_3$ *and otherwise the size of its image is* 3.

Proof. Let us again fix coordinates u_i for $1 \leq i \leq 5$ on $\mathcal{X}_5 \subseteq \mathbb{P}^5_{\mathbb{F}_5}$ such that their reduction modulo 5 corresponds to $(z^3, xz^2, yz^2, x^2z, xyz, y^2z - x^3)$ under the isomorphism of function fields described in Proposition 4.5.12.

Since l_1 and h are both of class I at 5 we see that there exist an integer λ such that $5 \nmid \lambda$ and $h \equiv \lambda l_1 \mod 5$. This implies the existence of a polynomial k over $\mathbb{Z}$ such that $h - \lambda l_1 = 5k$.

It follows for any point $P \in \mathcal{U}(\mathbb{Z}_5)$ that $\frac{h}{l_1}(P) \equiv \lambda \mod 5$ and that $\frac{h}{l_1}(P) \mod 25$ only depends on the image of P in $\mathcal{U}(\mathbb{F}_5)$.

Let us compute $\frac{h}{l_1}$ at P modulo 25:

$$\begin{aligned}\frac{h}{l_1}(P) &= \frac{\lambda l_1 + 5k}{l_1}(P) \\ &= \lambda + 5\frac{k}{l_1}(P).\end{aligned}$$

We know that $z^3\frac{k}{l_1}$ corresponds to a homogeneous cubic polynomial f_{hom} in the ideal $(x^3 - y^2z, xz, z^2)$ of $\mathbb{F}_5[x, y, z]$. Now write

$$k = c_0u_0 + c_1u_1 + c_2u_2 + c_3u_3 + c_4u_4 + c_5u_5$$

such that the cubic polynomial becomes

$$f_{\mathrm{hom}} = c_0z^3 + c_1xz^2 + c_2yz^2 + c_3x^2z + c_4xyz + c_5(y^2z - x^3).$$

Now consider $f = f_{\mathrm{hom}}(x, y, 1)$. We have seen in Lemma 4.8.7 that f is surjective to $\mathbb{F}_5^\times$ if it describes a line, a conic with two distinct rational points at infinity, a geometrically integral conic with a single point at infinity, or a cubic curve. The remaining cases are the constant functions and the quadratics which are independent of y. This shows that $k \equiv c_0u_0 + c_1u_1 + c_3u_3 \mod 5$. Let us show that we can assume that $c_0 = 0$. First note that l_1 reduces to a multiple of u_0 modulo 5. Let us write $\lambda' l_1 \equiv u_0 \mod 5$ where $\lambda' \in \mathbb{F}_5^\times$. This gives

$$(\lambda + 5c_0\lambda')l_1 \equiv \lambda l_1 + 5c_0\lambda' l_1 \equiv \lambda l_1 + 5c_0u_0 \mod 25.$$

So we can indeed assume that $c_0 = 0$.

The hyperplane section of $\mathbb{P}^5_{\mathbb{F}_5}$ defined by $k \equiv c_1u_1 + c_3u_3 \mod 5$ corresponds to the polynomial $c_1x + c_3x^2$ on $\mathbb{A}^2_{\mathbb{F}_5}$ which is quadratic if $c_3 \neq 0$ and constant if $c_1 = c_3 = 0$. By symmetry we see that a quadratic in one variable over $\mathbb{F}_5$ assumes exactly 3 values. And obviously if $h \equiv \lambda l_1 \mod 25$ then $c_1u_1 + c_3u_3$ is constant modulo 5.

So we see that $\frac{h}{l_1}(P)$ is constant modulo 5, and assumes either one, three or five values modulo 25. By Lemma 4.8.14 we see that $\frac{h}{l_1}(P)$ and hence $\frac{l_1}{h}(P)$ also assumes one, three or five values in $(\mathbb{Z}/25\mathbb{Z})^\times$ modulo fifth powers and so the same holds for $\operatorname{inv}_5 \mathcal{A}$ by Lemma 4.4.4.

This proves that precisely in the specified cases the invariant map is not surjective. □

4.9 Actual examples of obstructions

We will now combine the results on the invariant maps to produce some explicit examples of Brauer–Manin obstructions of order 5 and discuss some cases in which no algebraic obstruction can exist.

4.9.1 Obstructions for $\mathcal{U}$ of large conductor

Let us first show that in most cases there does not exist an algebraic obstruction to integral points if the conductor has a large prime divisor.

PROPOSITION 4.9.1. *Let $\mathcal{U}_h/\mathbb{Z}$ be a model as before of an interesting log K3 surface $U = X\backslash C$ of conductor n. If h is not of class I at a prime divisor $p > 11$ of n, then the invariant map $\operatorname{inv}_p \mathcal{A}\colon \mathcal{U}_p(\mathbb{Z}_p) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ is surjective. This implies that in these cases there does not exist an algebraic Brauer–Manin obstruction to the Hasse principle for integral points on $\mathcal{U}_h$.*

Proof. It follows from Theorem 4.8.12 that $\operatorname{inv}_p \mathcal{A}\colon \mathcal{U}_h(\mathbb{Z}_p) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ is surjective. This also proves that $\sum_\ell \operatorname{inv}_\ell \mathcal{A}\colon \mathcal{U}(\mathbb{A}_\mathbb{Z}) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ is surjective so in particular $\mathcal{X}(\mathbb{A}_{\mathbb{Q},\infty})^{\mathcal{A}}$ is not empty. □

If h is of class I at a prime divisor $p \equiv 1 \mod 5$ of the conductor n, then it is possible to get an obstruction.

THEOREM 4.9.2. *Fix a prime $p \equiv 1 \mod 5$. There exists a scheme $\mathcal{U}_h/\mathbb{Z}$ such that h is of class I at p which divides the conductor such that the surface $\mathcal{U}_h$ is locally soluble, but there is a Brauer–Manin obstruction to the Hasse principle for integral points.*

Proof. We will describe how to produce such examples.

Start off with a model $\mathcal{X}$ for $\mathrm{dP}_5(p)$ for p by picking an $\alpha \in \mathbb{Z}[\zeta_p]$ such that $K = \mathbb{Q}(\alpha)$ is a number field of degree 5. Such an α is not unique and a different choice of α will yield a different model for $\mathrm{dP}_5(p)$ over $\mathbb{Z}$. We will use the relatively large degree of freedom in the choice of h.

For $\ell \in \{2,3,5\}$ pick a smooth point $P_\ell \in \mathcal{X}(\mathbb{Z}_\ell)$ and a linear form $h_\ell \in \mathbb{F}_\ell[u_0,u_1,u_2,u_3,u_4,u_5]$ such that $h_\ell(P_\ell) \not\equiv 0 \mod \ell$. For inert primes ℓ which divide the discriminant of m_α we have a unique singular point S_ℓ on $\mathcal{X}_\ell$. We also impose the conditions $h_\ell(S_\ell) \equiv 0 \mod \ell$, i.e. S_ℓ does not lie on $\mathcal{U}_\ell$. Note that these conditions can be satisfied simultaneously in the case that ℓ is a small inert prime for which $\mathcal{X}_\ell$ has an A_4-singularity.

Now fix an invertible quintic non-residue q modulo p and let h_p be a linear form over $\mathbb{F}_p$ which satisfies $h_p \equiv ql_1 \mod p$. Let h be a primitive linear form over $\mathbb{Z}$ which is a lift of these h_ℓ.

By the condition modulo p we see that h is different from $\pm l_1$ and $\pm l_2$ so by Lemma 4.1.6 the hyperplane section defined by h is geometrically irreducible. Furthermore, $\mathcal{U}_h$ is locally soluble as it is has $\mathbb{Z}_\ell$-points for $\ell \leq 5$ by choice of h and it has local points for the remaining primes by Lemma 4.7.2.

Let us prove the theorem by showing that $\sum \mathrm{inv}_\ell \mathcal{A}$ is constant and non-zero. For primes $\ell \neq p$ we see from Lemmas 4.8.5 and 4.8.6 that $\mathrm{inv}_\ell \mathcal{A}$ is identically zero. For the ramified prime p we use Lemma 4.8.3, and as $\frac{l_1}{h} \equiv \frac{1}{q} \mod p$ is constant and not a fifth power modulo p we see that $\mathrm{inv}_p \mathcal{A}$ is constant and non-zero. $\square$

For $p = 11$, there are examples of such obstructions of a different nature.

4.9.2 Obstructions for $\mathcal{U}$ of conductor 11

We will use the model of $\mathrm{dP}_5(11)$ constructed using the element

$$\alpha = \zeta_{11} + \zeta_{11}^{-1} - 2 \in \mathbb{Q}(\zeta_{11})$$

with minimal polynomial $m_\alpha = s^5 - 11s^4 + 44s^3 - 77s^2 + 55s - 11$. This model $\mathcal{X}$ over $\mathbb{Z}$ is given by the five equations

$$u_0^2 - 492u_0u_3 - 52838u_0u_5 - u_1u_3 - 22u_1u_4 - 121u_1u_5 \\ + 1952u_2u_4 + 412071u_2u_5 - 971038u_3u_5 - 1771110u_5^2,$$

$$u_0u_2 - 22u_0u_3 - 4u_0u_4 - 3267u_0u_5 - u_1u_4 - 11u_1u_5 \\ + 88u_2u_4 + 20504u_2u_5 + 16u_3u_4 - 39017u_3u_5 - 78089u_5^2,$$

$$u_0u_3 + 169u_0u_5 + u_1u_5 - u_2^2 - 4u_2u_4 - 451u_2u_5 - 500u_3u_5 + 220u_5^2,$$

$$u_0u_4 - 11u_0u_5 - u_2u_3 + 121u_2u_5 - 4u_3u_4 - 363u_3u_5 - 594u_5^2,$$

$$u_0u_5 - u_2u_4 + u_3^2 - 11u_2u_5 + 40u_3u_5 + 55u_5^2.$$

As $\mathrm{disc}(m_\alpha) = 11^4$ we see that all fibres $\mathcal{X}_\ell$ are smooth for $\ell \neq 11$, and since $m_\alpha \equiv s^5 \mod 11$ we see that $\mathcal{X}_{11}$ has one singular point.

One can check that each of the two hyperplane sections given by

$$l_1 = u_1 + 187u_0 - 759u_2 + 693u_3 - 979u_4 + 4114u_5,$$

$$l_2 = u_1 + 187u_0 - 770u_2 + 792u_3 - 1199u_4 + 4840u_5$$

consist of five conjugate exceptional curves defined over the degree 5 number field $K = \mathbb{Q}(\zeta_{11})^+ = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ and the only ramified prime is 11.

Let us group the results on local solubility and computing the invariant maps on this surface for a general h. Again we consider the affine surface $\mathcal{U}$ over $\mathbb{Z}$ given by the complement of a hyperplane section $\mathcal{C} = \{h = 0\}$. The generic fibres of these two schemes are denoted by X and U.

LEMMA 4.9.3. *The affine surface $\mathcal{U}_h$ is everywhere locally soluble precisely when*

$$h \not\equiv u_2 + u_3 \mod 2.$$

Proof. A quick computer check shows that $\mathcal{X}(\mathbb{F}_2)$ consists of five points which lie on a unique hyperplane given by $u_2 + u_3$. Local solubility at 11 is given in Lemma 4.7.3 and the existence of points over the other completions is precisely Lemma 4.7.2, since all the fibres over $\ell \neq 11$ are smooth. □

LEMMA 4.9.4. *Consider a geometrically irreducible hyperplane section given by a primitive h. Let ℓ be a prime and let $\mathcal{A}$ be a generator for $\operatorname{Br} U_h / \operatorname{Br} \mathbb{Q}$. We consider the invariant map*

$$\operatorname{inv}_\ell \mathcal{A} \colon \mathcal{U}_h(\mathbb{Z}_\ell) \to \mathbb{Q}/\mathbb{Z}.$$

(a) If $\ell \neq 11$, then the invariant map is identically zero.

(b) If $\ell = 11$, then h is of

- » *class I precisely when h is a multiple of u_1;*
- » *class II precisely when h is not of class I, but it is in the $\mathbb{F}_{11}$-span of u_0, u_1 and u_3;*
- » *class III in all other cases.*

The value $0 \in \mathbb{Q}/\mathbb{Z}$ does not lie in the image of $\operatorname{inv}_{11} \mathcal{A}$ precisely when h is class I or II and the associated polynomial

$$f = h(x + 4x^2, 1, y, x^2, xy, y^2 - x^3).$$

does not assume the values ± 1 modulo 11 for $x, y \in \mathbb{F}_{11}$.

Note that for h of class I the associated polynomial f is constant and whether or not ± 1 lies in the image of f is immediate. If h is of class II, then f is independent of y and one only needs to evaluate f at 11 points.

Proof. We treat the cases of unramified and the ramified prime separately.

(a) This follows directly from Lemmas 4.8.5 and 4.8.6 since $\mathcal{X}_{11}$ is the only singular fibre of $\mathcal{X}$ over $\mathbb{Z}$.

(b) One can check that the rational map $\psi\colon \mathbb{P}^2_{\mathbb{F}_{11}} \dashrightarrow \mathcal{X}_{11}$ is defined by

$$(x,y,z) \mapsto (xz^2 + 4x^2z, z^3, yz^2, x^2z, xyz, y^2z - x^3).$$

Its inverse π is given by

$$(u_0\colon u_1\colon u_2\colon u_3\colon u_4\colon u_5) \mapsto (u_0 + 7u_3\colon u_2\colon u_1).$$

This shows that the associated polynomial of h at 11 is given by $f(x,y) = h(x+4x^2, 1, y, x^2, xy, y^2 - x^3)$. It follows that h is of

» class I precisely when f is constant;

» class II precisely when f is independent of y, but not of x; and

» class III otherwise.

For an h of class III the map $\mathrm{inv}_{11}\,\mathcal{A}\colon \mathcal{U}(\mathbb{Z}_{11}) \to \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ is surjective, so there is a $\mathbb{Z}_{11}$-point P such that $\mathrm{inv}_{11}\,\mathcal{A}(P) = 0$.

We saw in Lemma 4.8.3 how to compute the invariant map on the set $W \subseteq \mathcal{U}(\mathbb{Z}_{11})$ of $\mathbb{Z}_{11}$-points P such that $\frac{l_1}{h}(P)$ is defined and invertible in $\mathbb{Z}_{11}$. In the proof of Theorem 4.8.12 we saw that for h of class I or II these are all $\mathbb{Z}_{11}$-points on $\mathcal{U}$, so we see that 0 does not lie in the image of $\mathrm{inv}_{11}\,\mathcal{A}$ precisely if f does not assume a fifth power modulo 11 on $\mathbb{A}^2_{\mathbb{F}_{11}} \backslash V(f)$, or equivalently f does not assume the values ± 1 on the whole of $\mathbb{A}^2_{\mathbb{F}_{11}}$. □

We can now apply the above results to compute the Brauer–Manin obstruction for a fixed h and find actual algebraic obstructions of order 5 to the integral Hasse principle.

THEOREM 4.9.5. *Let $\mathcal{H}$ be the hyperplane in $\mathbb{P}^5_{\mathbb{Z}}$ given by the vanishing of u_0. The complement $\mathcal{U} = \mathcal{X} \backslash \mathcal{H}$ has points over $\mathbb{Q}$ and every $\mathbb{Z}_\ell$, but there is an algebraic Brauer–Manin obstruction to the existence of integral points.*

Proof. The local solubility follows from Lemma 4.9.3 and the invariant map for $\ell \neq 11$ is identically zero by Lemma 4.9.4.

Let us consider the only remaining prime 11. We will follow the outline in Lemma 4.9.4 to check for a possible obstruction. The associated inhomogeneous polynomial of $h = u_0$ is found to be $f = 4x^2 + x$, which is easily checked to never assume the values ± 1. So the element $0 \in \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ does not lie in the image of $\mathrm{inv}_{11}\,\mathcal{A}$. This shows that for all $(P_\ell)_\ell \in \mathcal{U}(\mathbb{A}_{\mathbb{Q},\infty})$ we have $\sum_\ell \mathrm{inv}_\ell\,\mathcal{A}(P_\ell) = \mathrm{inv}_{11}\,\mathcal{A}(P_{11}) \neq 0$ and hence

$$\mathcal{U}(\mathbb{A}_{\mathbb{Q},\infty})^{\mathcal{A}} = \varnothing$$

and so $\mathcal{U}(\mathbb{Z}) = \varnothing$. □

A careful analysis of the above proof yields the following result.

THEOREM 4.9.6. *Let $\mathcal{U}_h$ be the complement in $\mathcal{X}$ of a geometrically irreducible hyperplane section given by a primitive linear form $h \in \mathbb{Z}[u_0, u_1, \ldots, u_5]$. The class of h modulo 2 determines whether the affine surface $\mathcal{U}_h$ is locally soluble. The existence of an algebraic obstruction to the Hasse principle for integral points depends only on the reduction of h modulo 11. Out of the $11^6 - 1 = 1771560$ possible reductions of h modulo 11 precisely 228 give an obstruction.*

Note that this does not mean that the reduction of h modulo 2 and 11 is the only condition; the proof still uses the assumption that h is primitive. It follows from Lemma 4.1.6 that the condition that the section is geometrically irreducible is immediately satisfied if h does not reduce to $\pm u_1$. For hyperplanes h reducing to either of these two form it is easily shown that $\operatorname{inv}_{11} \mathcal{A}$ is identically equal to 0 on $\mathcal{U}_h(\mathbb{Z}_{11})$.

Proof of Theorem 4.9.6. We already saw the statement about local solubility in Lemma 4.9.3 and in Lemma 4.9.4 we saw that the existence of an obstruction only depends on the associated polynomial f which only depends on the reduction of h modulo 11.

Let us count the non-zero linear forms h over $\mathbb{F}_{11}$ for which such an obstruction exists. In Theorem 4.8.12 we saw that we get no obstruction unless h is of class I or class II. Let $f \in \mathbb{F}_{11}[x, y]$ be the associated polynomial of h. We must consider the cases where f is constant or a separable quadratic polynomial.

If f is constant then we see that $\operatorname{inv}_{11} \mathcal{A}$ is constant and we get an obstruction if f is one of the 8 non-fifth powers modulo 11.

For h of class II we see that $f\colon \mathbb{F}_{11} \backslash \{\rho_1, \rho_2\} \to \mathbb{F}_{11}^\times / (F_{11}^\times)^5, x \mapsto f(x)$ misses exactly one value. If f misses the value $q \in \mathbb{F}_{11}^\times / (\mathbb{F}_{11}^\times)^5$ we see that λf for $\lambda \in \mathbb{F}_{11}^\times$ misses the class of λq.

There are $10 \cdot 11^2$ quadratic polynomials over $\mathbb{F}_{11}$ and $10 \cdot 11$ of these are inseparable. The group $\mathbb{F}_{11}^\times$ acts on the remaining $10^2 \cdot 11$ quadratic polynomials by multiplication. All orbits have size 10 and in such an orbit exactly 2 miss the unit element in $\mathbb{F}_{11}^\times / (\mathbb{F}_{11}^\times)^5$. This proves that for an h of class II at 11 there is an obstruction if h reduces to one of these $2 \cdot 10 \cdot 11 = 220$ separable quadratic polynomials. □

4.9.3 Obstructions for $\mathcal{U}$ of conductor 25

It is also possible to find obstructions of order 5 to the integral Hasse principle when $\mathcal{X}$ is a model of $\mathrm{dP}_5(25)$ so then K has 5 as a ramified prime. For example, define the field $K \subseteq \mathbb{Q}(\zeta_{25})$ as the splitting field of the polynomial

$$m_\alpha = s^5 - 20s^4 + 100s^3 - 125s^2 + 50s - 5.$$

This produces the projective surface $\mathcal{X}$ over the integers given by the five equations

$$\begin{aligned}
&u_1^2 - u_0u_3 - 1600u_1u_3 - 40u_0u_4 - 400u_0u_5 - 524950u_1u_5\\
&\qquad\qquad + 7251005u_2u_5 - 30039800u_3u_5 - 16150000u_5^2,\\
&u_1u_2 - 40u_1u_3 - u_0u_4 - 20u_0u_5 - 18125u_1u_5\\
&\qquad\qquad + 200050u_2u_5 - 750995u_3u_5 - 403750u_5^2,\\
&u_2^2 - u_1u_3 - u_0u_5 - 500u_1u_5 + 1875u_2u_5,\\
&u_2u_3 - u_1u_4 + 20u_1u_5 - 400u_2u_5 + 1875u_3u_5 + 995u_5^2,\\
&u_3^2 - u_2u_4 + u_1u_5 - 20u_2u_5 + 100u_3u_5 + 50u_5^2.
\end{aligned}$$

The two hyperplane sections over $\mathbb{Z}$ cutting out the two quintuples of -1-curves are

$$l_1 = u_0 + 575u_1 - 3550u_2 + 8650u_3 - 4285u_4 + 10475u_5,$$
$$l_2 = u_0 + 525u_1 - 2575u_2 + 4325u_3 - 2285u_4 + 11100u_5.$$

As in the previous case, local solubility is immediate at most primes.

LEMMA 4.9.7. *The surface $\mathcal{U}_h$ is everywhere locally soluble precisely when*

$$h \not\equiv u_2 + u_3 + u_5 \mod 2.$$

Proof. Since $\operatorname{disc}(m_\alpha) = 5^8 7^6$, there are only two singular fibres and the local solubility at primes $\ell \geq 3$ follows from Lemmas 4.7.2 and 4.7.3. For the prime 2 we find, just like in the proof of Lemma 4.9.3, that the five points on $\mathcal{X}_2$ lie on a unique hyperplane in $\mathbb{P}^5_{\mathbb{F}_2}$. This hyperplane is given by $u_2 + u_3 + u_5 \equiv 0$. □

THEOREM 4.9.8. *Consider the invariant map*

$$\operatorname{inv}_\ell \mathcal{A}\colon \mathcal{U}_h(\mathbb{Z}_\ell) \to \mathbb{Q}/\mathbb{Z}.$$

(a) *If $\ell \neq 5$, then the invariant map is identically zero.*

(b) *If $\ell = 5$ then either $\operatorname{Im}(\operatorname{inv}_5 \mathcal{A}) = \frac{1}{5}\mathbb{Z}/\mathbb{Z}$ or there are integers λ, c_1 and c_3 satisfying $5 \nmid \lambda$ and either $5 \mid c_1, c_3$ or $5 \nmid c_1$ such that $h \equiv \lambda(u_0 + 15u_4) + 5(c_1u_1 + c_3u_3) \mod 25$. In this case the value $0 \in \mathbb{Q}/\mathbb{Z}$ lies in the image of $\operatorname{inv}_{11} \mathcal{A}$ precisely when $\lambda 1 + 5(c_1x + c_3x^2)$ assumes one of values $\pm 1, \pm 7$ modulo 25 for $x \in \mathbb{Z}$.*

Proof. The first statement follows as before. For the second statement one checks that the birational map $\mathcal{X}_5 \dashrightarrow \mathbb{P}^2_{\mathbb{F}_5}$ which restricts to the isomorphism from Proposition 4.5.12 is given by $(u_0, u_1, u_2, u_3, u_4, u_5) \mapsto (u_1, u_2, u_0)$ and the inverse by $(x, y, z) \mapsto (z^3, xz^2, yz^2, x^2z, xyz, y^2z - x^3)$. We see that under this map the hyperplanes u_1 and u_3 reduce to x^2 and x on the affine plane over $\mathbb{F}_5$. The statement now follows from Lemma 4.8.17 since $l_1 \equiv u_0 + 15u_4 \mod 25$ and $\frac{h}{l_1}(P)$ reduces to one of $\pm 1, \pm 7$ modulo 25 precisely when $\frac{l_1}{h}(P)$ does. □

For completeness we will give an example of a hyperplane for which the associated affine scheme over the integers does not have integral solutions.

THEOREM 4.9.9. *Consider an h which cuts out a geometrically irreducible hyperplane section such that* 0 *does not lie in the image of* $\mathrm{inv}_5 \mathcal{A}$*. The reduction of h modulo* 25 *is one of* 176 *out of the* $(5^2)^6 - 5^6 = 244125000$ *possible hyperplanes over* $\mathbb{Z}/25\mathbb{Z}$*. For example, the surface $\mathcal{U}_h/\mathbb{Z}$ for $h = 2u_0 + 10u_3 + 5u_4$ admits a Brauer–Manin obstruction of order* 5 *to the existence of integral points.*

Proof. Let $(\mathbb{Z}/25\mathbb{Z})^\times$ act on the hyperplanes modulo 25 for which $\mathrm{inv}_5 \mathcal{A}$ is not surjective by multiplication. This translates the image of the invariant map by an element of $\frac{1}{5}\mathbb{Z}/\mathbb{Z}$ depending on the class of $(\mathbb{Z}/25\mathbb{Z})^\times$ modulo fifth powers. So if the size of the image of an invariant map corresponding to a hyperplane has one element, then $\frac{4}{5}$ of the scalar multiples of h do not have 0 in the image. For invariant maps whose image is of size 3 precisely $\frac{2}{5}$ of the scalar multiples have this property. This means that the number of hyperplanes modulo 25 for which 0 does not lie in the image of the invariant map is $\frac{4}{5} \cdot 20 + \frac{2}{5} \cdot 20 \cdot 4 \cdot 5 = 176$.

Now consider the hyperplane $h = 2u_0 + 10u_3 + 5u_4$. The affine surface $\mathcal{U}_h$ is locally soluble by Lemma 4.9.7. The result follows from the previous theorem; take $\lambda = 2$, $c_1 = 0$ and $c_3 = 2$ and note that $2(1 + 5x^2)$ only assumes the values $2, 12, 17 \mod 25$. So 0 does not lie in the image of the invariant map at 5 and the invariant maps at the other primes are all constant zero. □