Piotr Blass

Picard groups of Zariski surfaces

Compositio Mathematica, tome 54, n° 1 (1985), p. 3-36

<http://www.numdam.org/item?id=CM_1985__54_1_3_0>
PICARD GROUPS OF ZARISKI SURFACES

Piotr Blass

To Kirsten

Acknowledgements

In addition to P. Deligne to whom the main idea of this paper is due I wish to thank Bill Fulton for his patient illumination of Deligne’s outline and for listening to my several early versions. With such two guides I could hardly go astray.

In addition I would like to acknowledge with pleasure conversations with J.S. Milne, A. Fauntleroy, R. Donagi, R. Lazarsfeld, L. Tu, L. Ein, L. Illusie, M. Raynaud, J. Denef, John Milnor, S. Mori and Steve Yau.

I was also greatly encouraged by frequent conversations with my former student and present collaborator Jeffrey Lang. He had solved several questions related to this paper.

I am deeply grateful to the Institute for Advanced Study in Princeton for providing the perfect environment for this effort during the Algebraic Geometry Year 1981-82.

In particular I wish to thank C. Underwood, I. Gaskill, D. Phares, K. Lunetta, P. Murray and Rene Baril for typing various parts of this manuscript.

Introduction

This paper originated in the following philosophical framework. Inspired by M. Noether’s theorem [4] and facts about generic double planes over C, [10], as well as by Rudakov’s and Šafarevič’s computations in characteristic two [8] we were led to suspect that the ring \( k[x, y, z]/(z^p - f(x, y)) \) is a UFD provided \( f \) is a sufficiently general polynomial of degree \( m \). Here \( k = \overline{k} \), characteristic \( k = p \geq 5 \), \( m \geq 5 \), say. The above conjecture still remains open but here we offer a result that in our opinion renders it extremely probable, to say the least, in the case when \( p \) divides \( m \).

We consider in the paper a generic polynomial with indeterminate coefficients. \( F = \sum T_{ij} X^i Y^j \), where \( 0 \leq i + j \leq p \), and the ring \( R = L[X, Y, Z]/(Z^p - F) \), \( L = k(T_{ij}) \), where \( T_{ij} \) are algebraically independent transcendentals over \( k \), \( \deg F = p \). We show that \( R \) is a UFD. This is our main theorem (MTH) in its algebraic form. In a subsequent paper
we hope to prove our original conjecture and also to generalize the result
of this paper to degrees of $f \neq p$.

The proof given here follows very closely an outline shown to the
author by Deligne. It is conceptually akin to SGA VII exp XIX. A new
feature is, for example, $\text{DRL} \rightarrow \text{MTH}$ (see Chapter V).

Let us outline the main idea of the proof, which is simple, if somewhat
lengthy in detail. Let $\overline{S} = \text{Proj}[X, Y, Z, Z_0]/(Z^p - F(X, Y, Z_0))$. $\overline{S}$ has
$N = p^2 - 3p + 3$ rational double points of type $A_{p-1}$, $(\text{Sing } \overline{S})$. The galois
group $G = \text{Gal}(k(T_{ij}) : k(T_{ij}))$ acts on $\overline{S}$ and it permutes the $N$
elements of $\text{Sing } \overline{S}$.

Step I is to show that $G$ induces the full symmetric group on $\text{Sing } \overline{S}$.

Step II is to refine the above and to analyze more closely the action of
$G$ on $\text{Pic } \tilde{S}$ ($\tilde{S}$ is the minimal desingularization of $\overline{S}$). It turns out that
there are elements of $G$ which induce the identity on $\text{Sing } \overline{S}$ but
nevertheless act non-trivially on certain exceptional curves contained in
$\tilde{S}$. See Double Reversal Lemma (DRL) and $\text{Gal } B$ below.

Step III is to deduce from DRL the fact that $\text{Pic } \tilde{S}$ is generated by the
obvious curves, namely the exceptional curves for $\tilde{S} \rightarrow S$ and a very
ample curve on $\overline{S}$ pulled back to $\tilde{S}$.

Step III provides us already with the proof of our main theorem in its
geometric form (MTHG). The equivalence of the geometric form with the
algebraic from ($R$ is a UFD) follows from a simple exact sequence which
we had introduced in a previous paper [1], see (0.5.1) below.

Finally, let us remark that Jeff Lang has proven a number of related
results in his Ph.D. thesis [6]. His method was to use differential
equations in characteristic $p > 0$.

At a crucial point in our proof we use the fact that $\text{Pic}(\tilde{S})$ has no
$p$-torsion. We had conjectured it, but the first proof is due to W.E. Lang
whose result we quote from [7].

It is not hard to extend our main theorem to the case where $F$ is
replaced by the polynomial not of degree $p$ but rather of degree $pe$, $e = 1,$
$2, \ldots$. We leave this extension as an exercise to the reader. In a subse-
quent paper we hope, among other things, to examine the transition from
"generic" to "general" and to prove our original conjecture at least in the
case when $p|m$. *

Chapter I. Notation; statement of the main theorem and of the principal
theorems and lemmas used in its proof

0. Notation

(0.1) $k = \overline{k}$ is an algebraically closed field of characteristic $p \geq 5$. $T_{ij}$ are

* See appendix to this paper, Comp. Math. 54 (1985) 37–40.
indeterminates algebraically independent over $k$, $0 \leq i + j \leq p$.

$$F(X, Y) = \sum_{0 \leq i + j \leq p} T_{ij} X^i Y^j$$

$\sum$ stands for $\sum_{0 \leq i + j \leq p}$ unless stated to the contrary.

$F_x, F_y$ means $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$, etc.

$$H(F) = \text{"hessian of } F\text{"} = \det \begin{vmatrix} F_{xx} & F_{xy} \\ F_{yx} & F_{yy} \end{vmatrix}$$

$L = \overline{k(T_{ij})}$, the algebraic closure of $k(T_{ij})$.

$G = \text{Gal}(\overline{k(T_{ij})} : k(T_{ij}))$.

$A = \text{Spec} k[T_{ij}]$

$E = \text{Spec}(k[T_{ij}][X,Y]/(F_x,F_y))$

$D = \text{Spec}(k[T_{ij}][X,Y,W]/(F_x,F_y,W^2 - H(F)))$.

We have the natural morphisms

$$D \xrightarrow{\phi} E \xrightarrow{\pi} A.$$

If $X \to A$ is a morphism we denote by $E_X$ the scheme $E_A \times X$ and by $\pi_X$ the projection $\pi_X: E_X \to X$.

If $U \subset A$ is open or closed $\pi_U: E_U \to U$ has the above meaning with respect to the inclusion map $U \to A$. We apply the same convention to maps $D \to E$, $D \to A$, $X \to E$, $X \to A$.

(0.2) We will identify closed points of $A$ with polynomials of degree $p$ in $k[X,Y]$. The following subset of $A$ will be important to us, $V \subset A$ corresponding to polynomials $g \in k[X,Y]$ of degree $p$ such that the surface $Z^p = g$ has no singularities at infinity. It is not hard to prove that $V$ is open and dense in $A$. This follows from the following fact:

Let us write out $g(X, Y)$ in terms of homogeneous parts:

$$g = g_p + g_{p-1} + \ldots + g_1 + g_0.$$
$U \subset V$ as follows $g \in U$ if and only if $g \in V$ and $g$ has only non-degenerate singularities (i.e., $g_x = g_y = 0$ implies hessian of $g \neq 0$). We will show below that $U$ is open and dense in $V$, see (3.1.3).

(0.3) In this paper we will constantly discuss an algebraic surface over $L$. Let us fix once and for all some notation relative to that surface. $R = L[X,Y,Z]/(Z^p - F(X,Y))$. $\mathcal{S}^{\text{aff}}$ or $\mathcal{S}^{\text{aff}} = \text{Spec}(L[X,Y,Z]/(Z^p - F(X,Y)))$ where $F$ is as above. $\mathcal{S}^{\text{aff}} = \text{Spec } R$. $\mathcal{S} = \text{Proj}(L[X,Y,Z,Z_0]/(Z^p - F(X,Y,Z_0)))$ where $F(X,Y,Z_0)$ is $F$ homogenized (sometimes we will write $F(X,Y,X_0)$). $\eta: \mathcal{S} \rightarrow \mathcal{S}$ a minimal desingularization of $\mathcal{S}$ over $L$. $P_L^n$ denotes the projective $n$-space over $L$.

The following facts can be shown about $\mathcal{S}^{\text{aff}}$ and $\mathcal{S}$. There is a natural projection, a finite map:

$$\mu: \mathcal{S} \rightarrow P_L^2 \quad \text{(see [1] Section 1)}.$$

We will denote by $l$ the element of $\text{Pic } \mathcal{S}$ given by:

$$\eta^*\mu^*(O_{P_L^2}(1)).$$

$\mathcal{S}$ has a set of isolated singularities denoted $\text{Sing } (\mathcal{S})$. One can show that:

$$\text{Sing } (\mathcal{S}) \subset \mathcal{S}^{\text{aff}} \quad \text{(see lemma (2.4.1) below)}.$$

Thus

$$\text{Sing } (\mathcal{S}) = \text{Sing } (\mathcal{S}).$$

Also, all the singularities are rational double points of type $A_{\mu-1}$, see (3.1.14). Further, the number of singularities is $p^2 - 3p + 3$, see (3.1.12).

The elements of $\text{Sing } \mathcal{S}$ will be denoted by Greek letters $\alpha, \beta, \gamma, \text{etc.}$ If we need to write out their coordinates in $A_L^1$ we will write $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, etc. In particular, we define

$$H_{\alpha} = (F_{xx}F_{yy} - F_{xy}^2)(\alpha_1, \alpha_2).$$

(0.4) The following facts about the minimal resolution map $\eta: \mathcal{S} \rightarrow \mathcal{S}$ are well known, see [1] Section 1.

Let $\alpha \in \text{Sing } \mathcal{S}$, then $\eta^{-1}(\alpha)$ consists of a tree of $(p - 1)$ rational curves over $L$ with intersection matrix (in $\text{Pic } \mathcal{S}$)

$$\begin{bmatrix}
-2 & 1 & & & & & 0 \\
1 & -2 & & & & & \\
& 1 & & & & & \\
& & & \ddots & & & \\
& & & & & \ddots & & \\
& & & & & & \ddots & 1 \\
& & & & & & & 1 -2
\end{bmatrix} \quad \text{(0.4.1)}$$
The tree can be pictured as follows:

We wish to emphasize the following subtle point which is of key importance in this paper. There are two possible natural choices of ordering the curves of the tree (from left to right or from right to left). We choose from the outset one orientation for each singularity \( \alpha \in \text{Sing} \overline{S} \) and we number the curves accordingly. Thus the tree will now be labelled

\[(0.4.2)\]
$T_\alpha$ stands for the ordered (tree) sequence $C_1^\alpha, C_2^\alpha, \ldots, C_{p-1}^\alpha$. $T^{\text{opp}}$ stands for $C_{p-1}^\alpha, C_{p-2}^\alpha, \ldots, C_1^\alpha$.

For each $\alpha \in \text{Sing} \hat{S}$ we now define a special element of $\text{Pic} \hat{S}$

$$D_\alpha = C_1^\alpha + 2C_2^\alpha + \ldots + (p-1)C_{p-1}^\alpha$$

(0.4.3)

and

$$D^{\text{opp}}_\alpha = C_{p-1}^\alpha + 2C_{p-2}^\alpha + 3C_{p-3}^\alpha + \ldots + (p-1)C_1^\alpha$$

(0.4.4)

$D_\alpha$ has the following properties. First of all, $D_\alpha \cdot C_j^\alpha \equiv O(p)$ for all $j$, $1 \leq j \leq p - 1$. Also

$$D_\alpha^2 = -p(p-1)$$

(0.4.5)

$$D_\alpha + D^{\text{opp}}_\alpha = pC_\alpha = p\left(C_1^\alpha + C_2^\alpha + \ldots + C_{p-1}^\alpha\right)$$

(0.4.6)

$$D_\alpha - D^{\text{opp}}_\alpha = 2D_\alpha - pC_\alpha.$$

(0.5) We will denote by

$$\text{Pic}^{\text{obvious}}(\hat{S}) \text{ or } \text{Pic}^{\text{ob}}(\hat{S})$$

the subgroup generated by $l$ and the $C_j^\alpha$, $\alpha \in \text{Sing} (\hat{S})$, $1 \leq j \leq p - 1$. There is an intersection form on $\text{Pic} \hat{S}$, we denote it by $A \cdot B, A, B \in \text{Pic} \hat{S}$. It can be shown that $l \cdot l = l^2 = p$. Also, we have the exact sequence

$$0 \to \text{Pic}^{\text{ob}}\hat{S} \to \text{Pic} \hat{S} \to C_1 R \to 0.$$  

(0.5.1)

And $C_1 R$ is a finite elementary $p$ group, see [6] or [9]. It was shown by W.E. Lang that $\text{Pic}(\hat{S})$ has no torsion [7].

(0.6) Let $X$ be a scheme (noetherian), $\text{Et}(X)$ the category of finite étale coverings of $X$.

Let $\Omega$ be an algebraically closed field $b: \text{Spec} \Omega \to X$, a geometric point of $X$. Let $Y \in \text{Et}(X)$.

$$F^X_b(Y)$$

is the set of liftings $Y$ of $b: \text{Spec} \Omega \to X$.

If $W \to X$ is a morphism, we get the base change functor $\text{Et} X \to \text{Et} W$ denoted $R_W$ or just $R$.

If $X$, $Y$ are schemes we denote by $X \sqcup Y$ the disjoint union of $X$ and $Y$. 
(0.7) In the following definition the ground field is assumed algebraically closed of characteristics $\neq 2$.

$A, B$ are smooth curves, $B$ irreducible, $\pi$ finite.

**Definition:** $A \rightarrow B$ is called *very simple* if there exists a point $\bar{q} \in A$ with $\pi(\bar{q}) = q$ and such that $e(\bar{q}) = 2$ (ramification is two); further if $B^0 = B - \{ q \}, A^0 = \pi^{-1}(B^0)$, then $A^0 \rightarrow B^0$ is finite and étale; also $\pi$ is étale on $A - \{ q \}$.

(0.8) **Definition:** $S, T$ two finite sets. $m: S \rightarrow T$ a two-to-one and onto mapping. We call the following commutative diagram a *double flip*:

\[
\begin{array}{ccc}
S & \xrightarrow{m} & T \\
\sigma_S \downarrow & & \downarrow id_T \\
S & \xrightarrow{m} & T
\end{array}
\]

where $\sigma_S$ is an automorphism of $S$ such that there are two elements $A, B \in T$ with preimages $\{ A_1, A_2 \}, \{ B_1, B_2 \}$ in $S$ and such that:

$\sigma_S(A_1) = A_2, \quad \sigma_S(A_2) = A_1,$

$\sigma_S(B_1) = B_2, \quad \sigma_S(B_2) = B_1.$

Also $\sigma_S|S - \{ A_1, A_2, B_1, B_2 \}$ is the identity. (Intuitively we think of $T$ as the set of position of a certain number of coins; each coin has "heads" and "tails", hence the two-to-one map $m: S \rightarrow T$. A "double flip" corresponds to turning over exactly two coins without altering the order of the coins.)

### 1. Statement of principal results

Our Main Theorem (MTH) is this:

**Main Theorem (MTH) (1.1):** $R$ is a unique factorization domain.

We will restate the theorem and in fact prove it in its geometric form.

**Main Theorem (Geometric Form) (MTHG) (1.2):** $\text{Pic}(\mathcal{S}) = \text{Pic}^{\text{ab}}(\mathcal{S})$.

**Remark:** Since there is no torsion we will, in fact, prove $p \text{Pic}(\mathcal{S}) = p \text{Pic}^{\text{ab}}(\mathcal{S})$. 

The equivalence of MTH and MTHG is an immediate consequence of the exact sequence (0.5.1). We will deduce MTHG from the following theorems to which we give descriptive names G1, G2, G2’, DRL (double reversal lemma).

Here are the statements:

**Theorem G1** (1.3): $G = \text{Gal}(k(T_i): k(T_{ij}))$ acts on $\text{Sing}(\overline{S})$ as the full symmetric group.

**Theorem G2** (1.4): There exists a $\sigma \in G$ such that $\sigma$ induces the identity on $\text{Sing} \ S$ but for some pair of singularities $\alpha, \beta \in \text{Sing} \ S$ $\sigma(\sqrt{H_\alpha}) = -\sqrt{H_\alpha}$ and for all $\beta \neq \gamma \neq \alpha, \gamma \in \text{Sing} \ S$ $\sigma(\sqrt{H_\gamma}) = \sqrt{H_\gamma}$.

**Theorem G2’** (1.5): For every pair of singularities $\alpha, \beta \in \text{Sing} \ S$ there exists $\alpha_0 \in G$ such that $\sigma$ induces the identity on $\text{Sing} \ S$ but $\sigma(\sqrt{H_\alpha}) = -\sqrt{H_\alpha}$ and $\sigma(\sqrt{H_\gamma}) = \sqrt{H_\gamma}$ for $\beta \neq \gamma \neq \alpha, \gamma \in \text{Sing} \ S$.

**DRL (Double Reversal Lemma)** (1.6): For every pair of singularities $\alpha, \beta, \gamma \in \text{Sing} \ S$ there is an element $\sigma \in G$ such that the induced isometry $i(\sigma)$ of $\text{Pic}(\overline{S})$ preserves $\text{Pic}^{\text{ab}}(\overline{S})$ and satisfies: $i(\sigma)(D_\alpha) = D_\alpha^{op}$, $i(\sigma)(D_\beta) = D_\beta^{op}$, $i(\sigma)(l) = 1$ and for all $\gamma \in \text{Sing} \ S$ with $\alpha \neq \gamma \neq \beta$ we have $i(\sigma)(D_\gamma) = D_\gamma$. The logical structure of the proof will be as follows:

\[
\begin{align*}
\text{easy exercise} \\
G1, G2 \Rightarrow G2' \Rightarrow DRL \Rightarrow MTHG \Rightarrow MTH
\end{align*}
\]

The implication $G1, G2 \Rightarrow G2'$ is a simple exercise and will not be described. The implication $MTHG \Rightarrow MTH$ has been indicated above. Thus, our paper consists in proving $G1, G2$, see Chapter IV. Further, in showing $G2' \Rightarrow DRL$, this will be sketched at the end of Chapter IV below, and finally we will prove the implication $DRL \Rightarrow MTHG$, in Chapter V.

**Chapter II. Preliminaries**

1. **Fundamental group facts** (see SGA I, Reference [3])

Let $i: Y \rightarrow X$ be a morphism of locally noetherian connected (regular) schemes. Let $b: \text{Spec} \ \Omega \rightarrow Y$ be a geometric point of $Y$. Let us abuse notation and denote by $b$ also the corresponding geometric point of $X$. 
(2.1.0) We recall the definition of the induced homomorphism:

\[ i^*: \pi_1(Y, b) \to \pi_1(X, b) \]

\[
\begin{array}{cccc}
\text{Et}(Y) & \xrightarrow{R} & \text{Et}(X) \\
\downarrow F_b^Y & & \downarrow F_b^Y \\
\text{ENS} & & \text{ENS}
\end{array}
\]

Now

\[ \pi_1(Y, b) = \text{Aut}(F_b^Y), \]

\[ \pi_1(X, b) = \text{Aut}(F_b^X). \]

By SGA I, p. 142 we have the isomorphism of functors:

\[ F_b^Y \circ R \cong F_b^X \]

where \( \mu \tau = \text{id} F_b^X, \tau \mu = \text{id}(F_b^Y \circ R) \)

If \( \sigma \in \pi_1(Y, b) = \text{Aut} (F_b^Y) \) we define \( \bar{\sigma} = i^*(\sigma) \) by the diagram:

\[
\begin{array}{ccc}
F_b^X(W) & \xrightarrow{\tau} & F_b^Y(W_Y) \\
\downarrow \bar{\sigma}_W & & \downarrow \sigma_{W_Y} \\
F_b^X(W) & \xleftarrow{\mu} & F_b^Y(W_Y).
\end{array}
\]

**PROPOSITION (2.1.1)** If \( W \in \text{Et}(X) \) is irreducible then \( \pi_1(X, b) \) acts transitively on \( F_b^X(W) \) for any base point \( b \) in \( X \).

**PROOF:** \( W \) is connected, so Proposition 1 follows from SGA I, [3], p. 140.

**PROPOSITION (2.1.2):** Assume \( W \in \text{Et}(X) \) irreducible and that \( R(W) = W_Y \) decomposes \( W_Y = s(Y) \sqcup T \) where \( s: Y \to W_Y \) is a section and \( T \) irreducible. Then for any base point \( b \in X \) the action of \( \pi_1(X, b) \) on \( F_b(W) \) is transitive and twice transitive.

**PROOF:** Transitivity was shown above. Also the statement is independent of base point (by SGA I). So choose the base point to be in \( Y \).
We have $F_b^Y \circ R \approx F_b^X$, see [3], p. 142.

$$(F_b^Y \circ R)(W) = F_b^Y(W_Y) =$$

$$= F_b^Y(s(Y)) \sqcup F_b^Y(T)$$

$$= \{ A \} \sqcup F_b^Y(T)$$

where $F_b^Y(s(Y))$ is the one element set $\{ A \}$.

Now $\pi_1(Y, b)$ acts on $F_b^Y(W_Y)$, it fixes $A$ and acts transitively on $F_b^Y(T)$ since $T$ is irreducible, see [3], p. 140. Now the identification $F_b^Y(W) = F_b^Y(W_Y)$ shows that for some element $A_1$ of $F_b^Y(X)$, $\pi_1(X, b)$ acts on $F_b^Y(W)$ so that the stabilizer of $A_1$ acts transitively on the complement of $A_1$ in $F_b^Y(W)$. This, together with transitivity, establishes twice transitivity. Q.E.D.

**PROPOSITION (2.1.3):** Let $W \in \text{Et}(X)$, $R(W) = W_Y \in \text{Et}(Y)$, let $b$ be a base point in $Y$. Suppose that the action of $\pi_1(Y, b)$ on $F_b^Y(W_Y)$ includes a transposition, then so does the action of $\pi_1(X, b)$ on $F_b^Y(W)$. Also, if $\tilde{b}$ is any other base point in $X$ not necessarily in $Y$, the action of $\pi_1(X, \tilde{b})$ on $F_b^X(W)$ also includes a transposition.

**PROOF:** Follows immediately from the definition of the induced homomorphism $\pi_1(Y, b) \to \pi_1(X, b)$ and the fact that the functors $F_b^Y$, $F_b^X$ are isomorphic.

**PROPOSITION (2.1.4):** Let $V, W \in \text{Et}(X)$, $m: V \to W$ étale covering of degree two,

Set $V_Y = R(V), W_Y = R(W), m_Y: V_Y \to W_Y$ the induced covering.

Suppose that there is a $\sigma \in \pi_1(Y, b)$ such that the diagram

$$F_b(V_Y) \to F_b(W_Y)$$

$$\sigma_{V_Y} \quad \sigma_{W_Y}$$

$$F_b(V_Y) \to F_b(W_Y)$$

is a double flip. Then also the diagram

$$F_b(V) \to F_b(W)$$

$$\sigma_V \quad \sigma_W$$

$$F_b(V) \to F_b(W)$$

is a double flip.
PROOF: Follows from the definition of \( \sigma \) and a diagram chase.

REMARK (2.1.4.1): Under the above assumptions for any base point \( \tilde{b} \) in \( X \) the action of \( \pi_1(X, \tilde{b}) \) on \( F_{\tilde{b}}(V) \to F_{\tilde{b}}(W) \) includes a double flip.

PROOF: Diagram chase using the fact that \( F_b \) and \( F_{\tilde{b}} \) are isomorphic functors.

2. Preliminaries on curves

**Theorem C1 (2.2.1):** Let \( A \to B \) be a very simple covering, then the action of \( \pi_1(B^\circ, b) \) on \( F_b(A^\circ) \) contains a transposition.

**Theorem C2 (2.2.2):** Let \( D \to A \to B \) be two very simple coverings. Assume that \( \tilde{q} \in D, \tilde{q} \in A, q \in B \) are such that \( e_\phi(\tilde{q}) = 2, e_\pi(\tilde{q}) = 2, e_\pi(\tilde{q}) = 2, \phi(\tilde{q}) = \tilde{q}, \pi(\tilde{q}) = q \). Let \( D^\circ \to A^\circ \to B^\circ \) be the induced étale coverings where \( B^\circ = B - \{ q \}, A^\circ = \pi^{-1}(B^\circ), D^\circ = \phi^{-1}(B^\circ) \). Then for any base point \( b \) in \( B^\circ \) the action of \( \pi_1(B^\circ, b) \) on the diagram \( F_b(D^\circ) \to F_b(A^\circ) \) includes a double flip.

**Proof of Theorem C1:** We denote \( f: A \to B, \tilde{q} \in A, f(\tilde{q}) = q, e_f(\tilde{q}) = 2 \).

\[
\begin{align*}
B^\circ &= B - \{ q \} \\
A^\circ &= f^{-1}(B^\circ)
\end{align*}
\]

\( f^\circ: A^\circ \to B^\circ \) the induced étale cover.

Let \( \mathcal{O}_q \) be the local ring of \( q \) in \( B \).

Let \( \hat{\mathcal{O}}_q \) be the henselization of \( \mathcal{O}_q \). We may take \( \hat{\mathcal{O}}_q \subset k(B^\circ)_{\text{sep}} \).

Consider the cartesian diagram

\[
\begin{array}{ccc}
\text{Spec } \mathcal{O}_q & \to & A \\
\downarrow \downarrow & & \downarrow \\
\text{Spec } \mathcal{O}_q & \to & B
\end{array}
\]

If \( \tilde{K} \) is the field of fractions of \( \hat{\mathcal{O}}_q \) we get the induced diagram

\[
\begin{array}{ccc}
\text{Spec } \tilde{K} & \to & A^\circ \\
\downarrow \downarrow & & \downarrow \\
\text{Spec } \tilde{K} & \to & B^\circ
\end{array}
\]
Now Spec $\mathcal{O}_q X B_{\text{over}} q \cong S \sqcup \text{Spec } \mathcal{O}_q(\sqrt{t})$ where $S$ is a union of sections over $\text{Spec } \mathcal{O}_q$, thus a trivial covering and $t$ is a uniformizing parameter in $\mathcal{O}_q$. This follows from elementary theory of henselian rings. Correspondingly, we can write the second diagram as:

$$\tilde{S} \sqcup \text{Spec } \tilde{K}(\sqrt{r}) \to A^0$$
$$\text{Spec } \tilde{K} \to B^0$$

where again $\tilde{S}$ is a union of several copies of $\text{Spec } \tilde{K}$.

Now we have $\text{Spec } k(B^0) \to \text{Spec } \tilde{K} \to \text{Spec } k(B^0) \to B^0$. Thus we get a geometric point $b$ of $\text{Spec } \tilde{K}$ and the corresponding geometric point $b_1$ of $B^0$. $\pi_1(\text{Spec } \tilde{K}, b) \cong \text{Gal}(k(A^0) : K)$ acts on $F^{\text{Spec } \tilde{K}}_b(\tilde{S} \sqcup \text{Spec } \tilde{K}(\sqrt{r}))$ and it is clear that it induced a transposition. Consequently, $\pi_1(B^0, b_1)$ induces a transposition in $F^{B^0}_{b_1} (A^0)$ by our discussion of the fundamental group (2.1.3).

**PROOF OF THEOREM C2:** Choose a henselization

$$\mathcal{O}_q \subset \mathfrak{o}_q \subset k(B^0)$$

and consider the base change.

$$S_1 \sqcup S_2 \sqcup \text{Spec } \mathcal{O}_q(\sqrt{t}) \cong \text{Spec } \mathfrak{o}_q XD \to D$$
$$S \sqcup \text{Spec } \mathfrak{o}_q(\sqrt{t}) \cong \text{Spec } \mathfrak{o}_q YA \to A$$
$$\text{Spec } \mathfrak{o}_q \cong \text{Spec } \mathfrak{o}_q \to B$$

We get the leftmost column from elementary properties of henselian rings. $S$ is a union of several copies of Spec $\mathfrak{o}_q$, thus a trivial covering. Similarly, $S_1$ and $S_2$ are trivial coverings of $S$.

We get the induced diagram, where $\tilde{K}$ is the field of fractions of $\mathfrak{o}_q$.

$$\tilde{S}_1 \sqcup \tilde{S}_1 \sqcup \text{Spec } \tilde{K}(\sqrt{r}) \to D^0$$
$$S \sqcup \text{Spec } \tilde{K}(\sqrt{r}) \to A^0$$
$$\text{Spec } \tilde{K} \to B^0$$

Choose an embedding $K \subset K(B^0)$. This defines a geometric point $b$ of Spec $K$ (and $b_1$ of $B^0$). By [3], prop. 8.1, p. 143, we have $\pi_1(\text{Spec } \tilde{K},$
b) \( \text{Gal}(k(\mathcal{B}^\circ): \tilde{K}) \) and this group acts on

\[
\begin{align*}
F_b\left( \tilde{S}_1 \sqcup \tilde{S}_2 \sqcup \text{Spec } \tilde{K}(\sqrt{t}) \right) \\
F_b\left( \tilde{S} \sqcup \text{Spec } \tilde{K}(\sqrt{t}) \right)
\end{align*}
\]

and we get a double flip by simple Galois theory (just send \( \sqrt{t} \) to \( -\sqrt{t} \)). If \( b_1 \) is the corresponding base point of \( \mathcal{B}^\circ \) we conclude that the \( \pi_1(\mathcal{B}^\circ, b_1) \) action on \( F_b(D^\circ) \rightarrow F_b(A^\circ) \) includes a double flip (from our discussion of the fundamental group (2.1.4)).

### 3. Irreducibility of the hessian

We will need the following proposition in order to prove that \( D \) is irreducible and normal and \( \phi: D \rightarrow E \) is finite. A related question is discussed in Coolidge's book about curves [Treatise on Algebraic Plane Curves, Dover], p. 153.

**Proposition (2.3.1):** \( F_{xx}F_{yy} - (F_{xy})^2 = H(F) \) is irreducible in \( R_1 = k[T_{ij}, X, Y] \).

**Lemma (2.3.2):** \( F_{xx} \) is irreducible and so is \( F_{yy} \).

**Proof:** \( F_{xx} = 2T_{20} + S_{xx} \) where \( S_{xx} \) does not involve \( T_{20} \). \( R_1/(F_{xx}) \approx R_2; R_2 = R_1/(T_{20}), a \) domain. Q.E.D.

**Lemma (2.3.3):** \( F_{yy} \) does not divide \( H(F) \).

**Proof:** \( F_{yy} \) contains the term \( 2T_{02} \) and \( (F_{xy})^2 \) does not contain \( T_{02} \).

**Corollary (2.3.4):** Let \( V: H(F) = 0 \) so that \( k[V] = R_1/H(F) \) then \( F_{yy} \) is not a zero divisor in \( k[V] \).

**Proof:** Obvious.

**Corollary (2.3.5):** \( k[V] \) injects into the localization \( k[V][1/F_{yy}] \).

**Lemma 2.3.6:** \( k[V][1/F_{yy}] \) is a domain.

**Proof:** Define a homomorphism \( h \) of \( R_1 \) into \( R_1 \) by \( h(X) = X, h(Y) = Y, h(T_{ij}) = T_{ij} \) for \( (i, j) \neq (2, 0) \) and \( h(T_{20}) = H(F) = T_{20}, F_{yy} + S_{xx}F_{xy} - (F_{xy})^2 \). Note that \( F_{yy}, S_{xx}, F_{xy} \) do not involve \( T_{20} \). Also \( h(F_{yy}) = F_{yy} \). \( h \) induces an injective map \( h: R_1/(T_{20}) \rightarrow R_1/(H(F)) \) which takes the class
of $F_{yy}$ to the class of $F_{yy}$. We therefore get the induced map:

$$h_1: R_1(T_{20})[1/F_{yy}] \to k[V][1/F_{yy}]$$

which is still injective. But now the image of $h_1$ includes not only $T_{ij}, X, Y$ for $(i,j) \neq (2,0)$ and $S_{xx}F_{yy} - (F_{xy})^2$ hence also $T_{20}F_{yy}$ but also $T_{20}$ since we have inverted $F_{yy}$ in the image. Thus $h_1$ is an isomorphism. This proves Proposition (2.31).

Q.E.D.

4. Non-singularity of $\bar{S}$ at infinity

For the sake of completeness we also include a simple lemma about the singularities of $\bar{S}$.

**Lemma (2.4.1):** There are no singularities of $\bar{S}$ in $\bar{S} - S$.

**Proof:** At such a singular point we would have:

$$\sum_{i+j=p-1} T_{ij} X^i Y^j = 0$$

$$\sum_{i+j=p, i,j \geq 0} iT_{ij} X^{i-1} Y^j = 0$$

$$\sum_{i+j=p, i,j \geq 0} jT_{ij} X^i Y^{j-1} = 0$$

but it is clear that the only common solution in $L$ is $X = Y = 0$ but then also $Z = 0$ and that does not define a point of the projective space over $L$.

Q.E.D.

Chapter III. Geometry of the mappings

$$E \to A, E_V \to V,$$

$$E_U \to U, D \to E$$

(3.1) Generalities

The main results of this chapter are theorem (3.2.12) (existence of a special pencil) and twice transitivity result (3.3.1). In order to prove these
results, we have to established certain basic facts about the maps $\pi$: $E \to A$ and $\phi$: $D \to E$. These facts should also be of some independent interest in the theory of Zariski Surfaces. Theorem (3.2.12) will be combined with basic facts about the fundamental group to prove the crucial Theorem G2 (1.4). The twice transitivity result will be essential in proving the two-transitivity in Theorem G1 (1.3).

PROPOSITION (3.1.1): $E$ is smooth, irreducible; in fact $E$ is isomorphic to an affine space over $k$ of dimension equal to the dimension of $A$.

PROOF: If we write out $F_x$ and $F_y$ we easily see that:

$$E = \text{Spec} \frac{k[T_{00}, T_{10}, T_{01}, \ldots]}{(F_x, F_y)}$$

is isomorphic to

$$E = \text{Spec} k[T_{00}, T_{20}, T_{11}, T_{02}, \ldots][X, Y].$$

Q.E.D.

REMARK (3.1.1.1): the above observation is due to S. Mori. We will use his idea again in (3.2.10) below.

REMARK (3.1.1.2): $\pi$ has at least one finite fiber.

PROOF: This follows from example (3.1.6) below.

COROLLARY (3.1.1.3): $\pi$ is dominating and generically finite. The field extension $k(A) \subset k(E)$ is a finite algebraic extension.

PROOF: This follows from the above remark and [5].

PROPOSITION (3.1.2): $\tau: \nu\to V$ is a finite map.

PROOF: It is enough to show that $\tau$ is quasi-finite and projective ([5], exercise 11.2, p. 280).

(i) $\tau$ is quasi-finite. If $g \in V$ then the surface $Z^\nu = g$ can only have finitely many singularities. Otherwise, there would be a singularity at infinity which contradicts the definition of $V$.

(ii) $\tau$ is projective. We have the commutative diagram:

$$\begin{array}{ccc}
\text{Sing}(\bar{S}_\nu)_{\text{red}} & \to & \bar{S}_\nu \\
\downarrow & & \downarrow
\\
E_{\nu} & \to & P^2_{\nu} \to V
\end{array}$$
where $\overline{S}_v$ is defined in $P^3_v$ by $Z^p - F(X, Y, Z_0)$ and $\text{Sing}(\overline{S}_v)$ is defined by the above homogeneous polynomial and its partials with respect to $X$, $Y$, $Z$, $Z_0$. The middle vertical arrow corresponds to projecting from the point at infinity on the $Z$ axis in each fiber. The map $E_v \to P^2_v$ is projective because $\text{Sing}(\overline{S}_v) \subseteq \overline{S}_v$ is closed and $E_v$ is the reduced image of $\text{Sing}(\overline{S}_v)$, thus closed in $P^2_v$. Therefore $E_v \to V$ is projective. Q.E.D.

**Corollary (3.1.3):** $U \subset V$ is open and dense. $\pi_U: E_U \to U$ is étale.

**Proof:** $E_v$ is open and dense in $E$. The polynomial $H(F)$ is not identically zero on $E$. Thus, it defines a proper closed subscheme $\sigma_v \subset E_v$. Since $\pi_v$ is finite, $\pi_v(\sigma_v)$ is a proper and closed subset of $V$. Now $U = V - \pi_v(\sigma_v)$. This shows that $U$ is open and dense in $V$. The fact that $\pi_U$ is étale follows from the Jacobian criterion.

**Corollary (3.1.4):** For any base point $b$ in $U$ the action of $\pi_1(U, b)$ on $F_b(E_U)$ is transitive.

**Proof:** $E_U$ is open and dense in $E$ and thus it is irreducible and therefore connected. The corollary follows now from SGA 1, [3], p. 140.

**Proposition (3.1.5):** $D$ is irreducible and normal. $\phi: D \to E$ is finite of degree two.

**Proof:** This follows from the irreducibility of the polynomial $H(F)$ in the ring $k[E] = k[T_{00}, T_{20}, T_{11}, T_{01}, \ldots, X, Y]$, see (2.3.1) and [5], p. 147, exercise 6.4.

Next we given an example of a point $T \in U$. By counting the points in $\pi^{-1}(T)$ we will find the degree of $\pi$ to be $p^2 - 3p + 3$. This result was originally proven by J. Sturnfield, see [1].

**Example (3.1.6):** For almost every choice of $A \in k$ the polynomial $h(x, y) = xy + Ax^{p-1} + y^{p-1} + xy^{p-1} + yx^{p-1}$ defines a point $T \in U$. Further we have that the cardinality of $\pi^{-1}(T)$ is $p^2 - 3p + 3$. The proof will follow from the following computational lemmas:

**Proof of Example (3.1.6)**

**Lemma (3.1.7):**

$$ g = xy + Ax^{p-1} + y^{p-1} + xy^{p-1} + yx^{p-1}. $$
For all but finitely many choices of $A \in k$ the system of equations
\[ g_x = 0 \]
\[ g_y = 0 \]
\[ \det \begin{vmatrix} g_{xx} & g_{xy} \\ g_{yx} & g_{yy} \end{vmatrix} = 0 \]
has no solution.

**Lemma (3.1.8):** For all but finitely many $A \in K$ the intersection number of $g_x = 0$ and $g_y = 0$ at infinity is $p - 2$.

**Proof of Lemma (3.1.7):** Consider the system:
\[ y - Ax^{p-2} + y^{p-1} - yx^{p-2} = 0 \]
\[ x - y^{p-2} - xy^{p-2} + x^{p-1} = 0 \]
\[ (2Ax^{p-3} + 2yx^{p-3})(2y^{p-3} + 2xy^{p-3}) + \]
\[ -(1 - y^{p-2} - x^{p-2})^2 = 0 \]
$x = 0$ implies $y = 0$ but $(x, y) = (0, 0)$ is not a solution. Assume $x \neq 0$, and rewrite the last equation,
\[ 4(Ax^{p-2} + yx^{p-2})(y^{p-3} + xy^{p-3}) + \]
\[ -(1 - y^{p-2} - x^{p-2})^2 x = 0 \]
eliminate $Ax^{p-2}$
\[ 4(y + y^{p-1} - yx^{p-2} + yx^{p-2})(y^{p-3} + x^{p-3}) + \]
\[ -(1 - y^{p-2} - x^{p-2})^2 x = 0. \]
It is enough to show that
\[ 4(y + y^{p-1})(y^{p-3} + x^{p-3}) + \]
\[ -(1 - y^{p-2} - x^{p-2})^2 = 0 \]
and
\[ x - y^{p-2} - xy^{p-2} + x^{p-1} = 0 \]
have no common component. \((x = 0\) is excluded again). We get finitely many values from \(A\) from the first equation once this is established.

At common points at infinity of the two curves

\[-xy^{p-2} + x^{p-1} = 0\]

\[4y^{p-1}(y^{p-3} + x^{p-3}) - (y^{p-2} + x^{p-2})^2 = 0\]

If \(x = 0\) then

\[4y^{p-1}(y^{p-3}) - (y^{p-2})^2 = 0\]

\[4y^{2p-4} - y^{2p-4} = 0\]

since \(p \neq 3\). This gives

\[y^{2p-4} = 0.\]

Thus no point with \(x = 0\). If \(x \neq 0\) then

\[\frac{y^{p-2}}{x^{p-2}} = 1.\]

Set \(T = y/x\) so that \(T^{p-2} = 1\). The second equation gives

\[4T^{p-1}(T^{p-2} + 1) - (T^{p-2} + 1)^2 = 0\]

so that

\[8T - 4 = 0 \quad \text{or} \quad T = \frac{1}{2}\]

so that

\[2^{p-2} = 1\]

which gives \(2 = 1\). Contradiction.

Therefore the two curves have no common point at infinity and they cannot have a common component. Q.E.D. (for lemma 5.1.).

PROOF OF (3.1.8): This proof is based on an idea of Jim Sturnfield. At a common point at infinity we must have:

\[y(y^{p-2} - x^{p-2}) = 0\]

\[x(-y^{p-2} + x^{p-2}) = 0\]  \hspace{1cm} (3.1.8.1)

Thus there are \(p - 2\) common points.

\[
\frac{y}{x} = \lambda \quad \text{where} \quad \lambda^{p-2} = 1.
\]
Homogenize
\[ g_x, y W^{p-2} + Ax^{p-2} W + y^{p-1} - y x^{p-2} \]
Set
\[ y = 1 \]
Set
\[ \tau = \frac{1}{\lambda} \]
Rewrite
\[ W^{p-2} - Ax^{p-2} W + 1 - x^{p-2} = 0 \]
as
\[ W^{p-2} - A[(x - \tau) + \tau]^{p-2} W + 1 + -[(x - \tau) + \tau]^{p-2} = 0. \]
The tangent line at \( W = 0, x = \tau \) is
\[ -A \tau^{p-2} W - (p - 2) \tau^{p-3} (x - \tau) \]
or
\[ -A \tau^{p-2} W + 2 \tau^{p-3} (x - \tau) \]
or
\[ -A \tau W + 2 (x - \tau) = 0. \]
Similarly for the second curve
\[ x W^{p-2} - W - x + x^{p-1} = 0 \]
and we consider \( W = 0 \). We obtain:
\[ x^{p-1} - x = 0 \]
\[ x^{p-2} = 1 \]
\[ x = \tau \]
and we have:
\[ \tau^{p-1} - \tau = 0. \]
We compute the tangent line at \( W = 0, x = \tau \). From
\[ -W - [(x - \tau) + \tau] + [(x - \tau) + \tau]^{p-1} + \ldots \]
we obtain:

$$-W - (x - \tau) + (p - 1) \tau^{p-2}(x - \tau) = 0$$

or

$$-W + (x - \tau)(-2) = 0.$$ 

Finally

$$-W + (x - \tau)(-2) = 0$$

defines the tangent line. We compare the two obtained tangent lines: Suppose

$$\det \begin{vmatrix} -1, & (x - \tau) \\ -A\tau, & 2 \end{vmatrix} = 0.$$ 

So that $2 + 2TA = 0$. But choose $A$ so that $A \neq -\frac{1}{\tau}$ for every $\tau$ such that $\tau^{p-2} = 1$. Then we get a contradiction. Thus for all but finitely many $A \in k$ we get no common tangent, Q.E.D.

**Lemma (3.1.9):** For all but finitely many choices of $A \in k$ we have $g \in V$.

**Proof** is by computation. By (0.2) we must consider the system,

$$\begin{align*}
Ax^{p-1} + y^{p-1} &= 0 \\
y^{p-1} - yx^{p-2} &= 0 \\
x^{p-1} - xy^{p-2} &= 0.
\end{align*}$$

(3.1.9.1)

Suppose that there is a solution with $x \neq 0$, then

$$Ax^{p-1} + y^{p-1} = 0$$

and

$$y^{p-2} - x^{p-2} = 0.$$ 

Set $T = y/x$ so that

$$T^{p-2} = 1.$$
But \( A T^{p-1} = -1 \) and we obtain

\[
AT = -1 \\
-\frac{1}{A} = T \\
\left(-\frac{1}{A}\right)^{p-2} = 1
\]

Contradiction for almost every choice of \( A \). Q.E.D.

**Corollary (3.1.10):** There exists a point \( g \in V \) such that \( \pi^{-1}(g) \) consists of \( p^2 - 3p + 3 \) unramified points (at which \( \pi \) is étale) \( \deg \pi = p^2 - 3p + 3 \).

**Corollary (3.1.10.1):** \( \pi \) is generically étale.

**Corollary (3.1.10.2):** \( U \) is open and dense in \( A \) (and in \( V \)).

**Corollary (3.1.11):** The degree of the field extension \( k(A) \subset k(E) \) is \( p^2 - 3p + 3 \).

**Corollary (3.1.12):** The surface \( S^{\text{aff}} \) has \( p^2 - 3p + 3 \) singularities at finite distance.

**Proof:** \( \text{Sing } S \cong F_b(U)(E_U) \) where \( b: \text{spec } k(U) \to \text{Spec } k(U) \to \text{Spec } U \). Now the cardinality of \( F_b(U)(E_U) \) is equal to the degree of \( \pi_U: E_U \to U \) and that is \( p^2 - 3p + 3 \). Q.E.D.

**Corollary (3.1.13):** The map \( D_U \to E_U \) is finite and étale of degree two. The degree of the field extension

\[
k(A) \subset k(D) \quad \text{is} \quad 2p^2 - 6p + 6.
\]

**Proof:** Follows from definition of \( D \), and (3.1.11) above.

**Corollary (3.1.14):** All the singularities of \( S \) are non-degenerate.

**Proof:** The maps \( D_U \to E_U \to U \) are étale coverings. Let \( b: \text{Spec } k(U) \to U \) be as above (3.1.12). Now we have \( m: F_b(D_U) \to F_b(E_U) \) and this map is two-to-one and onto. But \( F_b(D_U) \cong \text{set of pairs} \)

\[
\langle \alpha, t \rangle, \quad \alpha \in \text{Sing } S, \\
t \in L, \quad t^2 = H_\alpha
\]

Furthermore, \( F_b(E_U) \cong \text{Sing } S \), and \( m \) corresponds to projecting \( \langle \alpha, t \rangle \) to \( \alpha \). By a counting argument we must have all \( t \neq 0 \) so all \( H_\alpha \neq 0 \). Q.E.D.
**Example (3.2.1): Construction of the Special Polynomial (point of \( V \)) \( q \).**

The point \( q \) will be constructed as follows:

\[
q \leftrightarrow y^2 + x^3 + Ax^p - 1 + By^p - 1 + xy^p - 1 + yx^p - 1 = g(x, y)
\]

where \( B = +1 \) if \( p \neq 13 \) and \( B = -1 \) if \( p = 13 \). \( A \in k \) can be chosen so that the cardinality of \( \pi^{-1}(q) = (\deg \pi) - 1 \), \( q \in V \). Also the surface \( Z_p = g \) has \( (\deg \pi) - 1 \) non degenerate singularities and one degenerate singularity (in other words \( H(F) \) is equal to zero at exactly one point of \( \pi^{-1}(q) \)).

**Lemma (3.2.2): \( q \in V \) for almost every choice of \( A \in k \).**

**Proof:** Identical to the proof of 5.3.

**Lemma (3.2.3): For almost every \( A \in k \) the system of equations \((**\) below only has the solutions \((0, 0, t)\), \( t \in k \)**

\[
(\star\star) \quad g_{xx} g_{yy} - (g_{xy})^2 = 0
\]

\[
g_x = 0
\]

\[
g_y = 0.
\]

**Proof:** Consists of the following computation:

\[
g = y^2 + x^3 + Ax^p - 1 + By^p - 1 + xy^p - 1 + yx^p - 1
\]

\[
g_x = 3x^2 - Ax^{p-2} + y^{p-1} - yx^{p-2}
\]

\[
g_y = 2y - By^{p-2} - xy^{p-2} + x^{p-1}
\]

\[
g_{xx} = 6x - 2Ax^{p-3} + 2yx^{p-3}
\]

\[
g_{yy} = 2 + 2By^{p-3} + 2yx^{p-3}
\]

\[
g_{xy} = -y^{p-2} - x^{p-2}
\]

\[
g_{xx} g_{yy} - (g_{xy})^2 = 0
\]

\[
(\star\star) \quad g_x = 0
\]

\[
g_y = 0
\]
\((0, 0, t)\) is always a root. Also \(x = 0 \Rightarrow y = 0\).

Let us find all solutions with \(x \neq 0\). We eliminate \(A\) from the first two equations as follows:

\[
Ax^{p-2} = 3x^2 + y^{p-1} - yx^{p-1}
\]

or

\[
xg_{xx}g_{yy} - x\left( g_{xy} \right)^2 = 0
\]

And we obtain:

\[
2(3x^2 + 3x^2 + y^{p-1} - yx^{p-2} + yx^{p-2})g_{yy} - x\left( g_{xy} \right)^2 = 0
\]

We wish to show that the curves

\[
2(6x^2 + y^{p-1})(2 + 2By^{p-3} + 2xy^{p-3}) + \]

\[
- x\left( y^{p-2} + x^{p-2} \right)^2 = 0 \quad (***)
\]

and

\[
g_y = 2y - By^{p-2} - xy^{p-2} + x^{p-1} = 0
\]

have only finitely many points in common. Again \(x = 0\) implies \(y = 0\) so enough to prove this for \(x \neq 0\).

**Lemma (3.2.4):** The curve \(g_y = 0\) is smooth and irreducible.

**Proof:** Consider the projective curve (closure of \(g_y = 0\))

\[
2yW^{p-2} - By^{p-2}W - xy^{p-2} + x^{p-1} = 0.
\]

At points at infinity, i.e., where \(W = 0\), we have:

\[
x\left( x^{p-2} - y^{p-2} \right) = 0
\]

\[
W = 0, \quad x = 0, \quad y = 1
\]
or if

\[ x \neq 0 \quad \left( \frac{y}{x} \right)^{p-2} = 1. \]

\[ \frac{\partial}{\partial W} = 0 \quad \text{at infinity implies} \quad y = 0. \]

Thus, there are no singularities at infinity. We dehomogenize:

\[ 2y - By^{p-2} - xy^{p-2} + x^{p-1} = 0 \]

and check for singularities at finite distance:

\[ 2y - By^{p-2} - xy^{p-2} + x^{p-1} = 0 \]

\[ 2 + 2By^{p-3} + 2xy^{p-3} = 0 \quad (3.2.4.1) \]

\[ -y^{p-2} - x^{p-2} = 0 \]

First of all \( x = 0 \) is impossible if \( y = 0 \) then \( x = 0 \), contradiction. Assume \( y \neq 0 \) and transform

\[ 2y - By^{p-2} - xy^{p-2} + x^{p-1} = 0 \]

\[ 2y + 2By^{p-2} + 2xy^{p-2} = 0 \quad (3.2.4.2) \]

\[ y^{p-2} = -x^{p-2} \]

\[ 2y + Bx^{p-2} + x^{p-1} + x^{p-1} = 0 \]

\[ 2y - 2Bx^{p-2} - 2x^{p-1} = 0 \quad (3.2.4.3) \]

\[ y^{p-2} = -x^{p-2} \]

\[ Bx^{p-2} + 2x^{p-1} = -2Bx^{p-2} - 2x^{p-1} \]

\[ y^{p-2} = -x^{p-2} \quad (3.2.4.4) \]

\[ 2y = 2Bx^{p-2} + 2x^{p-1} \]

\[ 3Bx^{p-2} + 4x^{p-1} = 0 \]

\[ y^{p-2} = -x^{p-2} \quad (3.2.4.5) \]

\[ y = Bx^{p-2} + x^{p-1} \]
$x = 0$ is excluded. We obtain

$$x = \frac{-3B}{4}, \quad x^{p-2} = \frac{-4}{3B}, \quad x^{p-1} = 1$$

$$y = -\frac{4}{3} + 1 = -\frac{1}{3}$$

$$y^{p-2} = -3.$$

Now we must have

$$-3 = + \frac{4}{3B} \quad \text{or} \quad 9B = -4.$$  

If $p \neq 13$ then $B = 1$ by our assumption and $13 = 0$ a contradiction. If $p = 13$ then $B = -1, -9 = -4$ or $5 = 0$, again a contradiction.

Q.E.D. (for lemma 3.2.4).

In order to complete the proof of (3.2.3) it is enough to find one point on the curve $g_x = 0$ which is not on the first one in the system (***)

(3.2.3.2).

Take a point with

$$x = 0, \quad 2y = By^{p-2}$$

and with

$$y \neq 0$$

so that

$$2 = By^{p-3}.$$  

The first curve gives

$$(2y^{p-1})(2 + 2By^{p-3}) = 0$$

or

$$4y^{p-1} + 4By^{2p-4} = 0$$

since

$$y \neq 0, \quad 1 + By^{p-3} = 0$$

$$By^{p-3} = -1.$$
Thus

\[ 2 = -1 \quad \text{or} \quad 3 = 0 \quad \text{contradiction since} \ p \geq 5. \]

Q.E.D. (for 3.2.3).

**Corollary (3.2.5):** For almost every \( A \in k \) (**3.2.3.1**) has only the \((0, 0)\) solution in \((x, y)\).

**Lemma (3.2.6):** For almost every choice of \( A \in k \) the intersection number of \( g_x = 0 \) and \( g_y = 0 \) at the points at infinity is \( p - 2 \).

**Proof:** Analogous to (3.1.8). We omit it.

**Lemma (3.2.7):** Assumptions as in (3.2.6). The intersection number at the origin is two.

**Proof:** Simple computation using \( p \neq 2 \) and \( p \neq 3 \) (omitted).

**Corollary (3.2.8):** The cardinality of \( \pi^{-1}(q) \) is \( p^2 - 3p + 2 = \deg \pi - 1 \). The hessian is non-zero at all but one point of \( \pi^{-1}(q) \). It is zero at one point which we call \( \bar{q}, \bar{q} \in \pi^{-1}(q) \).

**Proof:** The total intersection number of the curves \( g_x = 0, \ g_y = 0 \) is \((p - 1)^2\) by Bezout's theorem. The number of intersections at finite distance is \((p - 1)^2 - (p - 2) - 1\) by the above. Thus it is \( p^2 - 3p + 2 \). Also the local intersection number is equal to one at every point where the hessian is non-zero. Q.E.D.

**Proposition (3.2.9):** Let \( A \) be as in example (3.2.1). Let \( L \) be the line in \( A = \text{Spec}\ k[T_{ij}] \) corresponding to polynomials of the form:

\[
\begin{align*}
y^2 + x^3 + \lambda x + Ax^{p-1} + By^{p-1} + \\
yx^{p-1} + xy^{p-1}
\end{align*}
\]

then \( \pi_L: E_L \to L, E_L \) is an irreducible and smooth curve. There is exactly one ramified point lying over \( q \), let us call it \( \bar{q} \) with ramification index \( e(\bar{q}) = 2 \).

**Lemma (3.2.10):** \( E_L \) is smooth and irreducible.

**Proof:**

\[
E_L \approx (k[x, y, \lambda])(\lambda + 3x^2 - Ax^{p-2} - yx^{p-2} + y^{p-1}, \\
2y - By^{p-2} + x^{p-1} - y^{p-2}x)^{-1} \\
\approx (k[x, y])(2y - y^{p-2} + x^{p-1} - y^{p-2}x)^{-1}
\]
Now we have shown above that the last curve is smooth and irreducible, see (3.2.4). \( E_L \rightarrow L \) is isomorphic to the projection to the \( \text{Spec } k[\lambda] \) axis of the space curve defined in \( \text{Spec } k[x,y,\lambda] \) by the two equations:

\[
\begin{align*}
\lambda + 3x^2 - Ax^{p-2} + y^{p-1} - yx^{p-2} &= 0 \\
2y - By^{p-2} - xy^{p-2} + x^{p-1} &= 0
\end{align*}
\]

\( q \) corresponds to the point \( \lambda = 0 \). The matrix of partials with respect to \( x, y, \lambda \) is:

\[
\begin{bmatrix}
6x + 2Ax^{p-3} + 2yx^{p-2} & -y^{p-2} - x^{p-2} & 1 \\
-y^{p-2} - x^{p-2} & 2 + 2By^{p-3} - 2xy^{p-3} & 0
\end{bmatrix}
\]

or

\[
\begin{bmatrix}
g_{xx} & g_{xy} & 1 \\
g_{yx} & g_{yy} & 0
\end{bmatrix}
\]

We have shown above that if

\[
\lambda = 0 \quad \text{then} \quad \det \begin{bmatrix} g_{xx} & g_{xy} \\ g_{yx} & g_{yy} \end{bmatrix} \neq 0
\]

for every point of the space curve except \( \lambda = x = y = 0 \). Thus, all of those points are smooth. Also, \( \lambda = x = y = 0 \), the point \( \bar{q} \), is smooth and \( x \) is a uniformizing parameter at \( \bar{q} \). Finally, we see that the hessian has a simple zero at \( \bar{q} \) and \( e(\bar{q}) = 2 \). All this follows from the matrix.

Similarly, we consider the map

\( D_L \rightarrow E_L \rightarrow L \).

\( D_L \) is isomorphic to the curve in 4-space \( \text{Spec } k[x,y,\lambda,W] \)

\[
\begin{align*}
\lambda + 3x^2 - Ax^{p-1} + y^{p-1} + yx^{p-2} &= 0 \\
2y - By^{p-2} - xy^{p-2} + x^{p-1} &= 0 \\
W^2 &= g_{xx}g_{yy} - (g_{xy})^2
\end{align*}
\]

The Jacobian matrix is:

\[
\begin{bmatrix}
g_{xx} & g_{xy} & 1 & 0 \\
g_{yx} & g_{yy} & 0 & 0 \\
\alpha & \beta & 0 & 2W
\end{bmatrix} \tag{3.2.10.1}
\]

\[
\begin{align*}
\alpha &= g_{xxx}g_{yy} + g_{xx}g_{yy} - 2g_{xy}g_{xxy} \\
\beta &= g_{xxy}g_{yy} + g_{xx}g_{yyy} - 2g_{xy}g_{xyy}
\end{align*}
\]
all points with $W \neq 0$ are clearly smooth. If $\lambda = 0$ and $W = 0$ then we must be at the point $\bar{q}$ given by $x = y = \lambda = W = 0$ by (3.2.9). We compute matrix there:

$$
\begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 \\
12 & 0 & 0 & 0
\end{bmatrix}
$$

it has rank 3, thus the point is non-singular.

$W$ is a uniforming parameter at $\bar{q}$ and $g_{xx}g_{yy} - (g_{xy})^2 = W^2$ has a zero of order two at $\bar{q}$. From this we see that the projection $\pi_L \circ \phi_L: D_L \to L$ (L corresponds to the Spec $k[\lambda]$ axis) has ramification equal to four at $\bar{q}$. Also $\phi_L(\bar{q}) = \bar{q}$ and $e_{\pi_L}(\bar{q}) = 2$, therefore, $e_{\phi_L}(\bar{q}) = 2$.

**Lemma (3.2.11):** $D_L$ is Irreducible.

**Proof:** $\phi_L: D_L \to E_L$ is finite and generically two to one. Thus $D_L$ may have at most two components. Let $C_L$ be the component which contains $\bar{q}$. Now $\bar{q}$ is a smooth point of $C_L$ and $e(\bar{q}) = 2$. Also, $C_L \to E_L$ is a finite map (proper and quasi finite), thus $C_L \to E_L$ must have degree two. Therefore, $C_L = D_L$ (inclusion of a closed subscheme is proper – [5]. p. 102) 48 (a).

The following theorem summarizes what we have shown:

**Theorem (3.2.12) (Existence of a Special Pencil):** There exists a point $q \in V - U$ and a smooth rational curve $L$ closed in $V$ such that $q \in L$ and $L_U = L \cap U$ is open and dense in $L$ and closed in $U$. Further, let $L_1$ be the open subset of $L$ defined by $L_1 = L \cup \{q\}$. We have the induced coverings:

$$
D_L \to E_L \to L,
$$

$$
U \quad U \quad U,
$$

$$
D_{L_1} \to E_{L_1} \to L_1,
$$

$$
U \quad U \quad U,
$$

$$
D_{L_U} \to E_{L_U} \to L_U,
$$

$$
D_{L_1} \to E_{L_1} \quad \text{and} \quad E_{L_1} \to L_1,
$$

are very simple coverings

$q \in D_{L_1}, \quad \bar{q} \to q, \quad q \to q$

$e(\bar{q}) = 2 \quad e(\bar{q}) = 2$
Remark (3.2.12.1): $L_U \subset U$ is closed and the bottom line may be induced directly by the base change $L_U \to U$ from $E_U$. $D_{L_U} \to E_{L_U} \to L_U$ are étale maps.

Remark (3.2.12.2): $E_L$, $E_{L_1}$, $D_{L_1}$ are smooth irreducible curves.

Proof: To obtain $L_U = L \cap U$ remove from $L$ the finitely many points over which $\pi: E_L \to L$ is ramified ($\pi$ is not everywhere ramified, for example, it is not ramified at $N-2$ points of $\pi^{-1}(q)$). Now $q$ corresponds to $\lambda = 0$. The smoothness of $D_{L_U}$ can be seen from the matrix (3.2.10.1) above.

All the other assertions have been shown before.

Corollary (3.2.13): Let $b: \text{Spec } \Omega \to L_U$ be any geometric base point, then a) the action of $\pi_1(L_U, b)$ on $F^U_b(E_{L_U})$ includes a transposition; b) the action of $\pi_1(L_U, b)$ on $F^L_b(D_U) \to F^L_b(E_{L_U})$ includes a double flip.

Proof: a), see Theorem C1 (2.2.1) above; b), see Theorem C2 (2.2.2) above.

Corollary (3.2.14): For any geometric base point $b$ in $U$ we have

a) the action of $\pi_1(U, b)$ on $F^U_b(E_U)$ includes a transposition;

b) the action of $\pi_1(U, b)$ on $F^L_b(D_U)$ acts transitively on $F^L_b(E_U) - \{A\}$.

Proof: See propositions (2.1.3), (2.1.4), and (2.1.4.1).

(3.3) Twice transitivity of the action of $\pi_1(U, b)$ and $F^U_b(E_U)$

Theorem (3.3.1): For any base point $b$ in $Z_U \pi_1(Z_U, b)$ acts on $F^U_b(E_{Z_U})$ in such a way that there is an element $A \in F^U_b(E_{Z_U})$ whose stabilizer in $\pi_1(Z_U, b)$ acts transitively on $F^U_b(E_{Z_U}) - \{A\}$.

Corollary (3.3.2): $\pi_1(U, b)$ acts on $F^U_b(E_U)$ transitively and twice transitively for any base point $b$ in $U$.

Proof of the Corollary: Transitivity has been shown before. If $b$ is in $Z_V$ we have $F^Z_b(E_{Z_U}) \approx F^U_b(E_U)$ and we recall the induced homomorphism $\pi_1(Z_U, b) \to \pi_1(U, b)$ which is such that the actions of $\pi_1(U, b)$ on $F^U_b(E_U)$ and of $\pi_1(Z_U, b)$ on $F^Z_b(E_{Z_U})$ are compatible so that by the above theorem there is an element $A \in F^U_b(E_U)$ whose stabilizer in $\pi_1(U, b)$ acts transitively on $F^U_b(E_U) - \{A\}$. This shows transitivity and twice transitivity. If $b$ is not in $Z_U$ then the conclusion still holds since all the functors $F^U_b$ are isomorphic by [3].
PROOF OF THEOREM:

\[ Z = \text{Spec } k\left[T_{00}, T_{20}, T_{11}, T_{02}, \ldots \right][X, Y] \]

\[ E_Z = \text{Spec} \frac{k\left[T_{00}, T_{20}, T_{11}, T_{02}, \ldots \right][X, Y]}{(2T_{20}X + T_{11}Y + \ldots, 2T_{02}Y + T_{11}X + \ldots)} \]

We get a section from sending \( X \to 0, Y \to 0 \). Let \( S: Z_U \to E_{Z_U} \) be the section. By SGA I, Cor. 5.3, p. 7, we have

\[ E_{Z_U} = S(Z_U) \cup T \]

\( T \) is reduced, smooth by SGA I 9.2, p. 16. We only need to show that \( T \) is topologically connected. Now \( T \) is covered by two opens \( T_x \) where \( X \neq 0 \) and \( T_y \) where \( y \neq 0 \). \( T_x \) is homeomorphic to \( \text{Spec } k\left[T_{00}, T_{02}, \ldots \right][X, Y][\frac{1}{X}] \)

thus connected. \( T_y \) is homeomorphic to \( \text{Spec } k\left[T_{00}, T_{20}, \ldots \right][X, Y][\frac{1}{Y}] \)
again connected.

To see that \( T_x \cap T_y \neq 0 \) note that for the point \( \tau \) from example (3.1.6), at least one point in \( \pi^{-1}(\tau) \) has \( X \neq 0, Y \neq 0 \). Thus, \( T \) is connected and therefore irreducible by SGA I, Prop. 10.1, p. 21.

Now:

\[ F_b^{Z_U}(E_{Z_U}) = F_b^{Z_U}(S(Z_U)) \cup F_b^{Z_U}(T) \]

\[ = \{ A \} \cup F_b^{Z_U}(T) \]

Now \( \pi_1(Z_U, b) \) stabilizes \( A \) and acts transitively on \( F_b^{Z_U}(T) \) by SGA I, p. 140. Q.E.D.


Chapter IV

Proof of Theorems G1, G2 and G2’ and of DRL

THEOREM (4.1): For any geometric base point \( b: \text{Spec } \Omega \to U \) the action of \( \pi_1(U, b) \) on \( F_b(E_U) \) is the full symmetric group.

PROOF: It is transitive by (3.1.4). It is twice transitive by (3.3.2). It contains a transposition by (3.2.14). All the above properties do not depend on the choice of the base point. Q.E.D.
**Theorem (4.2):** In the notations of Theorem 1, the action of \( \pi_1(U, b) \) on \( F^U_b(\mathcal{D}_U) \rightarrow \mathcal{F}_b^U(\mathcal{E}_U) \) contains a double flip.

**Proof:** This is a restatement of (3.2.14) b).

**Proof of Theorem G1 (1.3):** Let \( b: \text{Spec } k(\mathcal{T}_1) \rightarrow k(\mathcal{E}_1) \) be the base point of \( U \). We have a surjective map \( G \rightarrow \pi_1(U, b) \rightarrow (e) \) by SGA I, p. 143. Also \( \text{Sing } S \leftrightarrow F_b(\mathcal{E}_U) \) and this identification is \( G \) equivariant where \( G \) acts on \( F_b(\mathcal{E}_U) \) via \( G \rightarrow \pi_1(U, b) \) this follows from the proof on page 143 of SGA I. This proves G1.

**Proof of Theorem G2 (1.4):** Choose \( b \) as in the proof of G1. Now \( F_b(\mathcal{D}_U) \leftrightarrow \text{set of pairs } \langle \alpha, t \rangle \) where \( \alpha \in \text{Sing } S, i^2 = H_\alpha, t \in L = k(\mathcal{T}_1) \) (see 0.3 for the definition of \( H_\alpha \)). Let us call this set of pairs \( P \). The map

\[
\begin{array}{c}
F_b(\mathcal{D}_U) \\
\downarrow \\
F_b(\mathcal{E}_U)
\end{array}
\]

corresponds to projection \( \langle \alpha, t \rangle \rightarrow \alpha \). The diagram

\[
P \approx F_b(\mathcal{D}_U) \\
\downarrow \\
\text{Sing } S \approx F_b(\mathcal{E}_U)
\]

is \( G \) equivariant, where \( G \) acts on \( F_b(\mathcal{D}_U), F_b(\mathcal{E}_U) \) via the map \( G \rightarrow \pi_1(U, b) \rightarrow (e) \). Theorem G2 follows immediately from Theorem (4.2).

**Proof of Theorem G2' (1.5):** Follows immediately from G1, G2.

**Proof of DRL (1.6):** Since we have already proven G2' it is enough to prove the implication G2' \( \rightarrow \) DRL. The proof is somewhat tedious thus we only sketch it here.

**Sketch of Proof that G2' \( \rightarrow \) DRL:** Let \( \sigma \) be as in G2' then \( \sigma \) induces an automorphism of \( \mathcal{S} \) and it can be shown that there exists a commutative diagram:

\[
\begin{array}{c}
\mathcal{S} \xrightarrow{\bar{\sigma}} \mathcal{S} \\
\downarrow \\
\mathcal{S} \xrightarrow{\sigma} \mathcal{S}
\end{array}
\]

with \( \bar{\sigma} \) an automorphism. It can be shown that \( \bar{\sigma} \) induces the desired
isometry as in DRL. We omit the details of the proof except to point out that $\tilde{S}$ is the result of $\frac{1}{2}(p - 1)$ blow ups.

$$S_{\frac{1}{2}(p - 1)} = \tilde{S} \xrightarrow{\sigma = \sigma_{\frac{1}{2}(p - 1)}} \tilde{S} = S_{\frac{1}{2}(p - 1)}$$

and in fact we can construct $\sigma_{\frac{1}{2}(p - 1)} = \tilde{\sigma}$ by induction. The influence of $\tilde{\sigma}$ on $T_\alpha$, $T_\beta$, $T_\gamma$ can then be seen if we write out the local equations for the resolution.

Chapter V

Proof of the main theorem

We only need to show the implication:

$$DRL \Rightarrow MTHG.$$  

We begin with an easy lemma:

Let $\alpha \in \text{Sing } S$. Let $P_\alpha$ be the subgroup of $\text{Pic}(\tilde{S})$ generated by the curves $C_\alpha$, $i = 1, 2, \ldots, p - 1$. $P_\alpha$ inherits the intersection form from $\text{Pic}(\tilde{S})$.

**Lemma (5.1):** Let $x_\alpha \in P_\alpha$ have the property that $x_\alpha \cdot w \equiv 0 \pmod{p}$ for every $w \in P_\alpha$. Then $x_\alpha = n_\alpha D_\alpha + pz$ where $0 \leq n_\alpha \leq p - 1$, $z \in P_\alpha$.

**Proof:** Let $\tilde{P}_\alpha = P_\alpha/pP_\alpha$. This is a $\mathbb{Z}/p\mathbb{Z}$ vector space. Let $u: P_\alpha \to \tilde{P}_\alpha = P_\alpha/pP_\alpha$ be the natural map. We have a commutative diagram:

$$
\begin{array}{ccc}
P_\alpha \times P_\alpha & \xrightarrow{i} & \mathbb{Z} \\
\downarrow{u \times u} & & \downarrow{v} \\
\tilde{P}_\alpha \times \tilde{P}_\alpha & \xrightarrow{i_1} & \mathbb{Z}/p\mathbb{Z}
\end{array}
$$

where $i$ is the intersection form and $i_1$ is the intersection form modulo $p$.  

Now $i_1$ has a one dimensional kernel over $\mathbb{Z}/p\mathbb{Z}$ because the intersection matrix of $i_1$ with respect to the basis $u(C_1^a), u(C_2^a), \ldots u(C_{p-1}^a)$ which is
\[
\begin{bmatrix}
-2 & 1 & 0 \\
1 & -2 & \ddots & \ddots \\
\vdots & \ddots & \ddots & 1 \\
0 & \ddots & \ddots & -2 \\
\end{bmatrix}
\]
of size $(p-1) \times (p-1)$, has rank $p-2$ over $\mathbb{Z}/p\mathbb{Z}$. $u(D_a)$ is in the kernel and is $\neq 0$ in $\overline{P_a}$. Thus we have $u(x_a) = n_a u(D_a)$ for some $0 \leq n_a \leq p-1$. Consequently, $x_a - n_a D_a = pz$ for some $z \in P_a$ as asserted. Q.E.D.

**Corollary (5.2):** Any element $x \in \text{Pic}^{\text{ob}}(\tilde{S})$ which satisfies the condition that $x \cdot C_j^a \equiv 0(p)$ for all $\alpha \in \text{Sing } S$ and $1 \leq j \leq p-1$ can be written in the form
\[
x = n_l + \sum m_\gamma D_\gamma + py
\]
where $y \in \text{Pic}^{\text{ob}}(\tilde{S})$ and $0 \leq n_l$, $m_\gamma \leq p-1$ and $\sum$ is taken over all the singularities of $S$.

**Proof of the Main Theorem (1.1), (1.2):** We only need to show that
\[
p \text{Pic}(\tilde{S}) \subset p \text{Pic}^{\text{ob}}(\tilde{S})
\]
since there is no torsion.

Let $x \in p \text{Pic}(\tilde{S})$, then $x \in \text{Pic}^{\text{ob}}(\tilde{S})$ because of (0.5.1). Write
\[
x = n_0 l + \sum n_\alpha D_\alpha + py
\]
where $0 \leq n_0$, $n_\alpha \leq p-1$, $y \in \text{Pic}^{\text{ob}}(\tilde{S})$. This representation is possible because of (5.2). We only need to show that $n_\alpha = 0$ for all $\alpha \in \text{Sing } S$ and that $n_0 = 0$.

Pick any pair of singularities $\alpha \neq \beta$ and apply the DRL, thus we get a $Q \in G$ and if $i(\sigma)$ is the induced isometry of Pic($\tilde{S}$) we have
\[
x - i(\sigma)(x) = n_\alpha (D_\alpha - D_\alpha^{op}) + n_\beta (D_\beta - D_\beta^{op}) + p(y - i(\sigma)(y))
\]
\[
= 2n_\alpha D_\alpha + 2n_\beta D_\beta - pn_\alpha \sum C_1^a
\]
\[
- pn_\beta \sum C_j^\beta + p(y - i(\sigma)(y))
\]
in any case since $p \neq 2$ we conclude that

$$n_\alpha D_\alpha + n_\beta D_\beta \equiv p \, \text{Pic}(\mathcal{S})$$

and then $p^2$ must divide

$$\left( n_\alpha D_\alpha + n_\beta D_\beta \right)^2 = \left( n_\alpha^2 + n_\beta^2 \right) p (1 - p)$$

by (0.4.5) so that $p$ must divide $n_\alpha^2 + n_\beta^2$, thus for any pair of singularities $\alpha, \beta \neq \beta$ we have shown that $n_\alpha^2 = -n_\beta^2$ modulo $p$. But there are at least 3 singularities and we conclude that in fact this is only possible if $n_\alpha = 0$ for all $\alpha \in \text{Sing} \, S$.

Thus $x - py = n_0 l$ belongs to $p \, \text{Pic}(\mathcal{S})$. Squaring again we get that $p^2$ divides $(n_0 l)^2 = pn_0^2$ so that $n_0 = 0$.

Q.E.D.

References


(Mathematics Division
Department of Mathematical Sciences
301 Science-Engineering Building
Fayetteville, AR 72701
USA)