On the quasi group of a cubic surface
over a finite field

Andreas-Stephan Elsenhans* and Jörg Jahnel†

Abstract

We construct nontrivial homomorphisms from the quasi group of some cubic surfaces over $\mathbb{F}_p$ into a group. We show experimentally that the homomorphisms constructed are the only possible ones and that there are no nontrivial homomorphisms in the other cases. Thereby, we follow the classification of cubic surfaces, initially due to A. Cayley.

1 The quasi group of a cubic surface

1.1. Following Manin [Ma], a cubic surface $V$ carries a structure of a quasi group. For us, this shall simply mean the ternary relation

$$[x_1, x_2, x_3] \iff x_1, x_2, x_3 \text{ non-singular, intersection of } V \text{ with a line}.$$ 

If $V$ is defined over a field $K$ then, on $V^{\text{reg}}(K)$, there is a structure of a quasi group.

1.2. Remark. Here, the precise definition is that the lines lying entirely on the surface shall not cause any relation. On the other hand, it is allowed that two or all three points coincide. Then, the line shall simply be tangent to the surface of order two or three.

1.3. Definition. Let $(\Gamma, [\ ])$ be a quasi group and $(G, +)$ be an abelian group. By a homomorphism $p: \Gamma \to G$, we mean a mapping such that, for a suitable $g \in G$,

$$p(x_1) + p(x_2) + p(x_3) = g$$

whenever $[x_1, x_2, x_3]$.

*Mathematisches Institut, Universität Bayreuth, Universitätsstraße 30, D-95440 Bayreuth, Germany, Stephan.Elsenhans@uni-bayreuth.de, Website: http://www.staff.uni-bayreuth.de/~btm216

†Fachbereich 6 Mathematik, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany, jahnel@mathematik.uni-siegen.de, Website: http://www.uni-math.gwdg.de/jahnel
1.4. Fact. The category of all homomorphisms from a quasi group $\Gamma$ to abelian groups has an initial object. The corresponding abelian group is $\Gamma := \mathbb{Z}\Gamma/N$, for $N$ the subgroup generated by $1 \cdot x_1 + 1 \cdot x_2 + 1 \cdot x_3 - 1 \cdot x'_1 - 1 \cdot x'_2 - 1 \cdot x'_3$ for all $[x_1, x_2, x_3]$ and $[x'_1, x'_2, x'_3]$. $\Gamma$ carries a surjective augmentation homomorphism $s: \Gamma \to \mathbb{Z}$. We will call ker$s$ the group associated to $\Gamma$.

1.5. Definitions. Let $V$ be a cubic surface over a field $K$.

i) We will call the group associated to the quasi group $V^{\text{reg}}(K)$ the Mordell-Weil group of $V$. It will be denoted by $\text{MW}(V)$.

ii) We call two points $x_1, x_2 \in V^{\text{reg}}(K)$ equivalent if $[x_1] - [x_2] = 0 \in \text{MW}(V)$.

1.6. Remark. It is very well possible that there are non-equivalent points on a geometrically irreducible cubic surface. For example, as observed in [El], on the standard Cayley cubic $xyz + xyw + xzw + yzw = 0$, two points $(x_1 : y_1 : z_1 : w_1)$ and $(x_2 : y_2 : z_2 : w_2)$ with all coordinates different from zero may be equivalent only if $x_1y_1z_1w_1x_2y_2z_2w_2$ is a square in $K$. The purpose of this article is to investigate this phenomenon more systematically.

1.7. Remarks. i) Here, we are mainly interested in the case that $K = \mathbb{F}_q$ is a finite field. Then, for every concrete cubic surface $V$ over $\mathbb{F}_q$, the group $\text{MW}(V)$ is, in principle, computable. The point is that only the finite set $V(\mathbb{F}_q)$ is used. We will discuss efficient algorithms for the computation of $\text{MW}(V)$ in section 8.

ii) Although $\text{MW}(V)$ is, in principle, computable in every single case, it seems difficult to make general statements on $\text{MW}(V)$. We will therefore compare $\text{MW}(V)$ with a group more tractable from the theoretical point of view. This will be $A_0(V^{\text{reg}})$, the degree-0 part of Suslin’s homology group $h_0(V^{\text{reg}})$. We will establish a canonical homomorphism $\pi_V: \text{MW}(V) \to A_0(V^{\text{reg}})$ for $V$ a geometrically irreducible cubic surface over a finite field. Under minimal assumptions, $\pi_V$ will be surjective.

1.8. Plan of the article. First, in section 2, we will recall Cayley’s classification of singular cubic surfaces. Then, in section 3, under a mild assumption, we will prove that $\text{MW}(V)$ is a finite abelian group. For this, we will compare $\text{MW}(V)$ with the Mordell-Weil groups of the plane sections of $V$.

Then, in section 4, we will treat the reducible case. It will turn out that there is a nontrivial surjection from $\text{MW}(V)$ to a nontrivial abelian group which is given in an elementary manner. Finally, we will compute $A_0(V^{\text{reg}})$ systematically for every case of the classification of irreducible cubic surfaces. In section 8, we will report on the comparison between $\text{MW}(V)$ and $A_0(V^{\text{reg}})$ in a large sample of examples.
1.9. Remarks. a) The Mordell-Weil group is related to the famous Mordell-Weil problem which may be formulated as to find a minimal system of generators for $\text{MW}(V)$.
b) We are particularly interested in the cases when, for $V$ a cubic surface over a finite field, $\text{MW}(V) \neq 0$. The point is that there is the following application.
Let $\mathcal{V}$ be a cubic surface over $\mathbb{Q}$ such that there are a nontrivial group $G$ and primes $p_1, \ldots, p_t$ satisfying the following conditions.
i) The singularities of $\mathcal{V}_{p_i}$ do not lift to points on $\mathcal{V}$.
ii) There are surjections $\text{MW}(\mathcal{V}_{p_i}) \rightarrow G$.
Then, at least $(t-1)\mathbb{Q}$-rational points are necessary in order to generate $\mathcal{V}(\mathbb{Q})$ [El].

2 Cayley’s classification of cubic surfaces

2.1. Singular cubic surfaces are classified since the days of A. Cayley. We will use this theory as it is presented in [Do, sec. 9.2] and ignore about possible changes in small characteristics.

2.2. According to this, there are the following types.
I) A normal cubic surface is either
i) in one of the 21 classes of surfaces with finitely many double points, listed in [Do, Table 9.2.5]. This includes the case of a smooth cubic surface.
ii) Or the cone over a smooth cubic curve $C$.
II) A non-normal, geometrically irreducible cubic surface is either
i) a cubic ruled surface. There are two types of those [Do, Theorem 9.2.1], ordinary and Cayley’s cubic ruled surfaces.
ii) Or the cone over a singular cubic curve. This might be a cubic with a self-intersection or a cusp.

2.3. The desingularizations are as follows.
I.i) $\mathbb{P}^2$ blown-up in six points. Thereby, the $A_1, D_2, \text{ or } E$-configurations of $(-2)$-curves, given in the table, do occur.
I.ii) a ruled surface over the cubic curve. On this surface, there is exactly one curve with a negative self-intersection number, a $(−3)$-curve.
II.i) $\mathbb{P}^2$ blown-up in one point,
II.ii) the Hirzebruch surface $F_3$.

2.4. Remarks. a) In the situation of a finite base field, the classification of cubic surfaces is actually a little finer.
I.i) Among these types, $2A_1$, $3A_1$, $2A_2$, $A_2 + 2A_1$, $4A_1$, $2A_2 + A_1$, $A_3 + 2A_1$, and $3A_2$ have symmetries. This leads to 13 further types where the singularities are defined over extensions of the ground field.

II.i) An ordinary cubic ruled surface may have its normal form $xz^2 + yw^2 = 0$ only over a quadratic extension. This causes a third type of cubic ruled surfaces over a finite field.

II.ii) In the case of the cone over a cubic curve with self-intersection, there are two variants as to whether the two tangent directions at the point of intersection are defined over the ground field or not.

b) We will restrict ourselves to cubic surfaces which are reduced. In other words, the following types of reducible surfaces are allowed.

i) A reducible cubic surface might consist of a quadric and a plane. There are four cases where the quadric is nondegenerate. In fact, the quadric may split over the ground field or not and the plane may be tangent or not. There are four more cases when the quadric is a cone. The intersection with the plane might be a conic, two lines, a double line, or a point.

ii) Finally, the surface might be reducible into three planes. There are two cases as to whether their intersection is a point or a line. Observe, it is possible that the decomposition into three planes is defined only after a finite field extension.

3 Comparison with cubic curves

3.1. Let $C \subset \mathbb{P}^2$ be a reduced cubic curve over a field $K$. Then, in a manner analogous to the surface case, there are a quasi group structure on $C$ and the Mordell-Weil group $\text{MW}(C)$. This group is known in every case.

i) It may happen that all $K$-rational smooth points are contained in a line. Then, the quasi group structure is empty and $\text{MW}(C) = \ker(\text{sum}: \mathbb{Z}[L(K)] \to \mathbb{Z})$.

We have this degenerate case whenever $C$ contains a line defined over a proper extension of $K$. The same may happen even for a smooth cubic curve when $\#K \leq 5$.

Otherwise,

ii) $\text{MW}(C) = J(C)(K)$ for $C$ smooth, and

iii) $\text{MW}(C) = K^+ \text{ if } C \text{ is a cubic curve with a cusp.}$

iv) If $C$ is a cubic curve with a node then $\text{MW}(C) = K^*$ in case that the two tangent directions at the node are defined over $K$. If the tangent directions are defined over the quadratic extension $F/K$ then $\text{MW}(C) = \ker(\text{N}: F^* \to K^*)$.

v) When $C$ is reducible into a line and a conic then $\text{MW}(C) = \ker(\text{N}: F^* \to K^*) \oplus \mathbb{Z}$, $\text{MW}(C) = K^+ \oplus \mathbb{Z}$ or $\text{MW}(C) = K^* \oplus \mathbb{Z}$ depending on whether, over $K$, there are no, one, or two points of intersection.
vi) When \( C \) is reducible into three components then \( \text{MW}(C) = K^+ \oplus \mathbb{Z}^2 \) or \( \text{MW}(C) = K^* \oplus \mathbb{Z}^2 \) depending on whether the three points of intersection coincide or not. In the case of three points of intersection, this is actually Menelaos' Theorem.

3.2. **Example (Cones).** —— For \( V \) a cone over a cubic curve \( C \), we have a canonical surjection \( \text{MW}(V) \to \text{MW}(C) \).

3.3. **Fact.** —— Let \( V \) be a cubic surface over a field \( K \). Take a plane section which yields a reduced curve \( C \).

a) Then, the canonical injection \( C^\text{reg}(K) \hookrightarrow V^\text{reg}(K) \) is compatible with the quasi group structures.

b) There is an induced group homomorphism \( \text{MW}(C) \twoheadrightarrow \text{MW}(V) \). \( \square \)

3.4. **Corollary (Criterion for torsion).** —— Let \( V \) be a cubic surface over the finite field \( \mathbb{F}_q \) and \( x_0, x \in V^\text{reg}(\mathbb{F}_q) \). Further, let \( E \) be a plane through \( x_0 \) and \( x \) intersecting \( V \) in an irreducible cubic curve \( C \).

Then, \([x] - [x_0] \in \text{MW}(V)\) is torsion. It is annihilated by multiplication with \( \#C^\text{reg}(\mathbb{F}_q) \).

**Proof.** The assertion is true already for \([x] - [x_0] \in \text{MW}(C)\). \( \square \)

3.5. **Fact.** —— Let \( V \) be a cubic surface over \( \mathbb{F}_q \).

a) Then, for \( x_0 \in V^\text{reg}(\mathbb{F}_q) \) arbitrary, \( \text{MW}(V) \) is generated by all differences \([x] - [x_0]\) for \( x \in V^\text{reg}(\mathbb{F}_q) \).

b) In particular, \( \text{MW}(V) \) is a finitely generated abelian group. \( \square \)

4 **Reducible cubic surfaces**

4.1. —— Let \( V \) be a reducible cubic surface over a field \( K \). Then, there are two essentially different cases.

i) There are two irreducible components, a plane \( E \) and a quadric, but the quadric consists of two planes defined over a quadratic extension. Then, only the plane \( E \) contains \( K \)-rational smooth points. We have an empty quasi group structure and \( \text{MW}(V) = \ker(\text{sum} : \mathbb{Z}[E(K)] \to \mathbb{Z}) \).

ii) Otherwise, when \( V \) decomposes into \( k = 2, 3 \) components, there is a canonical surjection \( \text{MW}(V) \to \ker(\text{sum} : \mathbb{Z}^k \to \mathbb{Z}) \cong \mathbb{Z}^{k-1} \).

4.2. **Example.** —— Over a finite field \( \mathbb{F}_q \) of characteristic \( \neq 2 \), let \( V \) be a reducible cubic surface consisting of a nondegenerate quadratic cone \( Q \) and a plane \( E \). Suppose that \( E \) does not meet the cusp of \( Q \). Then, there is a canonical surjection

\[ \text{MW}(V) \to \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} . \]
Proof. The homomorphism to $\mathbb{Z}$ is that from 4.1.ii). It remains to construct the homomorphism to $\mathbb{Z}/2\mathbb{Z}$.

For this, we fix coordinates such that the cusp is in $(1 : 0 : 0 : 0)$ and the plane $E$ is given by $x = 0$. Further, we assume without restriction that the plane “$y = 0$” is tangent to the cone $Q$. Then, the cone is given by, say, $yz + Kw^2 = 0$ for $K \neq 0$. The whole cubic surface has the equation

$$x(yz + Kw^2) = 0.$$ 

On the plane “$x = 0$”, we define the homomorphism $\text{MW}(V) \to \mathbb{Z}/2\mathbb{Z}$ simply as \(\chi_2(K(yz + Kw^2))\) for $\chi_2$ the quadratic character on $\mathbb{F}_q^*$. On the cone “$yz + Kw^2 = 0$”, we take $\chi_2(xy)$, respectively $\chi_2(-Kxz)$ when $y = 0$.

We have to show that this definition is indeed compatible with the quasi group structure. For this, let $(x : y : z : w) \in Q(\mathbb{F}_q)$, $(x' : y' : z' : w') \in Q(\mathbb{F}_q)$, and $(0 : y'' : z'' : w'') \in E(\mathbb{F}_q)$ be three collinear points. Then, we clearly have $(0 : y'' : z'' : w'') = (0 : (x' y - xy') : (x' z - xz') : (x' w - xw'))$. Furthermore,

$$(xy)(x' y')(y'' z'' + Kw'^2) = Kx' z' y' y'' [(x' y - xy')(x' z - xz') + K(x' w - xw')]$$

$$= -Kx' z' y' y'' [x' (yz' + y' z + 2Kw'')]$$

$$= -Kx^2 x'^2 (-Ky^2 w^2 - Ky'^2 w^2 + 2Kyy' w')$$

$$= K^2 x^2 x'^2 (yw' - y' w)^2$$

is a perfect square. \(\square\)

5 Irreducible cubic surfaces not being cones

5.0.1. --- Reducible cubic surfaces were dealt with in section 4. If a cubic surface $V$ is irreducible, but geometrically reducible, then it consists of three planes acted upon transitively by the Galois group. In this case, $V_{\text{reg}}(K) = \emptyset$ and, therefore, $\text{MW}(V) = 0$. From now on, we may restrict ourselves to the geometrically irreducible case. There is another restriction which can and should be made. Cones have been treated in Example 3.2. Thus, let us exclude from now on cubic surfaces being cones. We may therefore limit our considerations to cubic surfaces of the types I.i) and II.i).

5.1 Suslin’s singular homology group $h_0$

5.1.1. --- For a scheme of finite type over a field $K$, the singular homology groups $h_n(S)$ were introduced by A. Suslin [SV]. They are the homology groups of the chain complex $C_*(S)$ where the $n$-chains are given by

$$C_n(S) = \{ \text{finite correspondences } \Delta^n_K \to S \}.$$
Here, $\Delta^n_K := \text{Spec } K[t_0, \ldots, t_n]/(t_0 + \ldots + t_n - 1)$ is the $n$-dimensional standard simplex over $K$. A finite correspondence is a finite linear combination $\sum n_i Z_i$, where every $Z_i$ is an integral closed subscheme of $S \times \Delta^n_K$ such that the projection to $\Delta^n_K$ is finite and surjective. The differential $d: C_n(S) \rightarrow C_{n-1}(S)$ is defined as the alternating sum of the homomorphisms induced by the cycle-theoretic intersections with the codimension-1 boundaries $S \times \Delta^{n-1}_K \subset S \times \Delta^n_K$. This definition is motivated by the Dold-Thom Theorem in Algebraic Topology.

5.1.2. Remarks. 

i) For $S$ an integral scheme of finite type over $\mathbb{C}$, A. Suslin and V. Voevodsky show that there is a natural isomorphism

$$h_*(S, \mathbb{Z}/n\mathbb{Z}) \cong H^*_{\text{sing}}(S(\mathbb{C}), \mathbb{Z}/n\mathbb{Z})$$

to the ordinary singular homology as soon as finite coefficient groups are considered. There are several other comparison theorems to theories of interest. In fact, these methods led V. Voevodsky to his theory of motives.

ii) For our purposes, however, a small part of this powerful theory will suffice. We will entirely work with $h_0(S)$. There is a concrete description for $h_0(S)$ which we will recall in Theorem 5.1.3 below. Observe that this shows $h_0(S) \cong \text{CH}^0(S)$ in the case that $S$ is proper.

5.1.3. Theorem. Let $S$ be an integral scheme of finite type over a field $K$. Then,

$$h_0(S) = Z_0(S)/\text{Rat}'_0(S).$$

Here, $Z_0(S)$ is the group of 0-cycles, i.e., the free abelian group over all closed points of $S$. $\text{Rat}'_0(S)$ is generated by all 0-cycles of the following kind.

Let $C \subset S$ be an irreducible curve, $C'$ its normalization, and $\overline{C}$ the corresponding smooth, proper model. Then, take all the cycles $\text{div}(f)$ where $f \not\equiv 0$ is a rational function on $C$ which, after pull-back to $\overline{C}$, is constantly 1 on $\overline{C}\setminus C'$.

Proof. See [Sch, Theorem 5.1].

5.1.4. Remarks. 

a) $h_0(S)$ is equipped with a natural degree map $\text{deg}: h_0(S) \rightarrow \mathbb{Z}$. We will denote its kernel by $A_0(S)$.

b) Let $i: S_1 \rightarrow S_2$ be an arbitrary morphism of quasi-projective varieties over $K$. Then, there is the induced homomorphism $i_*: h_0(S_1) \rightarrow h_0(S_2), [x] \mapsto [i(x)]$. This immediately yields a map $i_*: A_0(S_1) \rightarrow A_0(S_2)$.

5.1.5. Lemma. Let $V$ be a geometrically irreducible cubic surface over $\mathbb{F}_q$. Then, there is a canonical homomorphism

$$\pi_V: \text{MW}(V) \rightarrow A_0(V^{\text{reg}}).$$
Proof. To each combination $a_1[p_1] + \ldots + a_k[p_k]$ for $p_1, \ldots, p_k \in V^{\text{reg}}(K)$ and $a_1 + \ldots + a_k = 0$, the homomorphism $i_*$ assigns the corresponding cycle. We take this as a definition for $\pi_V$. To show that $\pi_V$ is well-defined, we have to verify the following.

Assume that $x_1, x_2, x_3$ are collinear and $x'_1, x'_2, x'_3$ are collinear, too. Suppose that the connecting lines are not contained in $V$. Then,

$$[x_1] + [x_2] + [x_3] - [x'_1] - [x'_2] - [x'_3] = 0 \in A_0(V^{\text{reg}}).$$

For this, consider the pencil of planes through $x_1, x_2, x_3$. Generically, the intersection with $V$ is a curve, smooth at $x_1, x_2$ and $x_3$. The only possible exceptions are the tangent planes. We claim that the generic intersection curve is irreducible, too. Indeed, the contrary would mean that all intersection curves contained a line. Suppose, this is a line through $x_1$. Then, $V$ contains a pencil of lines through $x_1$, which implies $V$ contains a plane through $x_1$. Hence, $V$ is reducible, a contradiction.

Thus, take a plane through $x_1, x_2, x_3$, generating an irreducible intersection curve $C$ which is smooth in $x_1, x_2$ and $x_3$. Further, take a plane through $x'_1, x'_2, x'_3$ generating an irreducible intersection curve $C'$ which is smooth in $x'_1, x'_2$ and $x'_3$ and meets $C$ only in smooth points $x''_1, x''_2, x''_3$. The sublemma below, applied to $C$ and $C'$, immediately yields the assertion. \hfill $\square$

5.1.6. Sublemma. –– Let $C$ be an irreducible cubic curve. Assume that $x_1, x_2, x_3 \in C^{\text{reg}}$ as well as $x'_1, x'_2, x'_3 \in C^{\text{reg}}$ are triples of collinear points such that $\{x_1, x_2, x_3\} \cap \{x'_1, x'_2, x'_3\} = \emptyset$.

Then, there is a rational function $f$ on $C$ having simple zeroes at $x_1, x_2, x_3$, simple poles at $x'_1, x'_2, x'_3$, no other zeroes or poles, and the value 1 at the possible singular point.

Proof. According to J. Plücker, an irreducible cubic curve may have at most one singular point. We may therefore put $f := K \cdot l_1/l_2$ for forms $l_1$ and $l_2$ defining the lines. By assumption, these do not meet the singular point. If necessary, we choose the constant $K$ such that the value at the singularity is normalized to 1. \hfill $\square$

5.2 $h_0$ and the tame fundamental group

5.2.1. –– Let $S$ be a smooth surface over the finite field $\mathbb{F}_q$ for $q = p^r$ and let $\overline{S} \supset S$ be a smooth compactification. Then, the tame fundamental group $\pi_1^t(S)$ of $S$ classifies all finite coverings of $S$ which are tamely ramified at $\overline{S} \setminus S$.

The group $\pi_1^t(S)$ is independent of the choice of the compactification $\overline{S}$. $\pi_1^t(S)$ is a quotient of $\pi_1^\text{ét}(S)$. By the purity of the branch locus [SGA1, Exp. X, Théorème 3.1], one has

$$\pi_1^t(S)_{\text{tors}} \cong (\pi_1^\text{ét}(S)_{\text{tors}}^{\text{ab}})_{\text{prime to } p} \oplus (\pi_1^\text{ét}(\overline{S})_{\text{ab}})_{p\text{-power}}.$$

Again, this decomposition is independent of the choice of $\overline{S}$. 

8
The structural morphism $S \to \text{Spec} \mathbb{F}_q$ induces a surjection $\pi^t_1(S) \to \pi_1(\text{Spec} \mathbb{F}_q)$ the kernel of which we will denote by $\pi^{l,\text{geo}}_1(S)$. Note that $\pi^{l,\text{geo}}_1(S)$ differs from $\pi^t_1(S_{\mathbb{F}_q})$. The point is that the analogue of the natural short exact sequence [SGA1, Exp. IX, Théorème 6.1] is only right exact for the tame fundamental group.

5.2.2. Theorem (Schmidt, Spieß). — Let $S$ be a surface over a finite field $\mathbb{F}_q$ which is smooth and geometrically irreducible, but not necessarily proper.

i) Then, $A_0(S)$ is a finite abelian group.

ii) There is a canonical isomorphism

$$\iota_S : A_0(S) \to \pi^{l,\text{geo}}_1(S)^{\text{ab}}.$$ 

Proof. See [SchS, Theorem 0.1]. \hfill \Box

5.2.3. Remarks. —— a) Concretely, $\iota_S$ is given as follows.

i) For a point $x : \text{Spec} \mathbb{F}_{q'} \to S$, consider the induced homomorphism

$$\pi^\text{ét}_1(x) : \hat{\mathbb{Z}} = \pi^\text{ét}_1(\text{Spec} \mathbb{F}_{q'}) \to \pi^\text{ét}_1(S) \to \pi^\text{ét}_1(S) \to \pi^t_1(S)^{\text{ab}}.$$ 

Send $[x]$ to $\pi^\text{ét}_1(x)(1)$. This defines a homomorphism $\iota'_S : h_0(S) \to \pi^t_1(S)^{\text{ab}}$.

ii) Clearly, the degree map $\text{deg} : h_0(S) \to \hat{\mathbb{Z}}$ is compatible with the homomorphism $\pi^t_1(S)^{\text{ab}} \to \pi^\text{ét}_1(\text{Spec} \mathbb{F}_q) = \hat{\mathbb{Z}}$ induced by the structural morphism.

iii) The homomorphism $\iota_S$ is exactly the restriction of $\iota'_S$ to $\ker \text{deg}$.

b) The map $\iota'_S$ defines an isomorphism $h_0(S) \to \pi^t_1(S)^{\text{ab}}$.

5.3 The tame fundamental group and the Picard group

5.3.1. Fact. —— Let $V$ be a cubic ruled surface defined over $\mathbb{F}_q$. Then, $\pi^t_1(V_{\text{reg}}^{\text{reg}}) = 0$.

Proof. It will suffice to show $\pi^t_1(V_{\mathbb{F}_q}^{\text{reg}}) = 0$. In the present situation, a smooth compactification of $V_{\mathbb{F}_q}^{\text{reg}}$ is given by a projective plane, blown up in one point. The preimage of the singular locus is a (double) line through the point blown up. Consequently, $V_{\mathbb{F}_q}^{\text{reg}}$ is a ruled surface over $\mathbb{A}^1$. This yields $\pi^t_1(V_{\mathbb{F}_q}^{\text{reg}}) = 0$. \hfill \Box

5.3.2. Proposition. —— Let $V$ be a geometrically irreducible cubic surface over $\mathbb{F}_q$ which is not a cone. Suppose $V$ is normal, i.e., of one of types I.i). Then,

$$\pi^t_1(V_{\text{reg}}^{\text{reg}})^{\text{ab}} = [(\text{Pic}(V_{\text{reg}})^{\prime \prime \text{top}} \otimes_{\hat{\mathbb{Z}}} \hat{\mathbb{Q}}_{\infty})^\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)]^\vee.$$ 

Here, $\vee$ denotes the Pontryagin dual, given by the functor $\text{Hom}(\cdot, \hat{\mathbb{Q}}/\mathbb{Z})$. 


Proof. First step. $p$-torsion.

We know a smooth compactification $\overline{V}$ of $V_{\text{reg}}$, explicitly. $\overline{V}_{\mathbb{F}_q}$ is isomorphic to $\mathbb{P}^2$ blown-up in six points. In particular, we have $\pi_1^{\text{et}}(\overline{V}_{\mathbb{F}_q}) = 0$. This suffices for $\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l = 0$ and $\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) = 0$.

Second step. The Pontryagin dual.

Let us compute the Pontryagin dual $(\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l)^{\vee}$. For $l$ prime to $p$, we have

$$\text{Hom}(\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l, \mathbb{Q}/\mathbb{Z}) / \text{Hom}(\pi_1(\mathbb{F}_q), \mathbb{Q}/\mathbb{Z})$$

$$= \text{Hom}(\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l, \mathbb{Q}/\mathbb{Z}) / \text{Hom}(\pi_1(\mathbb{F}_q), \mathbb{Q}/\mathbb{Z})$$

$$= H^{1}_{\text{et}}(V_{\mathbb{F}_q}, \mathbb{Z}/\mathbb{Z}) / H^{1}_{\text{et}}(\mathbb{F}_q, \mathbb{Z}/\mathbb{Z}).$$

According to the Hochschild-Serre spectral sequence

$$H^n(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q), H^q_{\text{et}}(V_{\mathbb{F}_q}, \mathbb{Z}/\mathbb{Z})) \implies H^{n+q}_{\text{et}}(V_{\mathbb{F}_q}, \mathbb{Z}/\mathbb{Z}),$$

the latter quotient is nothing but $H^{1}_{\text{et}}(V_{\mathbb{F}_q}, \mathbb{Z}/\mathbb{Z})^{\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)}$.

Third step. The torsion part of the Picard group.

We have $\Gamma(V_{\mathbb{F}_q}, \mathbb{G}_m) = \mathbb{F}_q^\times$. In fact, the A-, D-, and E-configurations do not contain any principal divisor. They do not even contain nontrivial divisors numerically equivalent to zero. This immediately yields $H^{1}_{\text{et}}(V_{\mathbb{F}_q}, \mu_l) = \text{Pic}(V_{\mathbb{F}_q}, \mathbb{Z}/\mathbb{Z})$, for any $l$ prime to $p$. On $V_{\mathbb{F}_q}$, the sheaves $\mu_l$ and $\mathbb{Z}/\mathbb{Z}$ coincide up to the Galois operation. We therefore have

$$\text{Hom}(\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l, \mathbb{Z}/\mathbb{Z}) = (H^{1}_{\text{et}}(V_{\mathbb{F}_q}, \mu_l) \otimes_{\mathbb{Z}} \mu_l)^{\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)}$$

$$= (\text{Pic}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l^{\vee})^{\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)}.$$

Summing this up for all $l$, we see that

$$(\pi_1^{l,\text{geo}}(V_{\mathbb{F}_q}) \otimes_{\mathbb{Z}} \mu_l)^{\vee} = (\text{Pic}(V_{\mathbb{F}_q})_{\text{prime to } p} \otimes_{\mathbb{Z}} H^{\vee}_{\infty})^{\text{Gal}(\mathbb{F}_q/\mathbb{F}_q)}$$

which is equivalent to the assertion. \hfill \square

5.4 The 21 types of normal cubic surfaces not being cones

5.4.1. Fact. —— Let $V$ be a normal, proper surface over an algebraically closed field and $\overline{V}$ its desingularization. Then,

$$\text{Pic}(V_{\text{reg}}) = \text{Pic}(\overline{V})/(E_1, \ldots, E_k),$$

where $E_1, \ldots, E_k$ denote the irreducible components of the preimages of the singularities on $\overline{V}$. \hfill \square
5.4.2. Theorem. —— Let $V$ be an irreducible cubic surface over $\overline{\mathbb{F}}_q$, not being a cone. Suppose $V$ is normal, i.e., of one of types I.i).

Then, the Picard group $\text{Pic}(V^{\reg})$ is torsion-free in every case except for I.i.XVI), I.i.XVIII), I.i.XIX) and I.i.XXI). In these cases, the following is true.

I.i.XVI) $(4A_1)$ $\text{Pic}(V^{\reg})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}$,

I.i.XVIII) $(A_3 + 2A_1)$ $\text{Pic}(V^{\reg})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}$,

I.i.XIX) $(A_5 + A_1)$ $\text{Pic}(V^{\reg})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}$,

I.i.XXI) $(3A_2)$ $\text{Pic}(V^{\reg})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$.

**Proof.** We distinguish the cases systematically. Each time, we apply Fact 5.4.1.

One has $\text{Pic}(\overline{V}) \cong \mathbb{Z}^7$. The signature is $(1, -1, -1, -1, -1, -1)$. I.e., we have torsion-freeness in the case of a smooth cubic surface.

Otherwise, the $A$-, $D$-, or $E$-configuration of $(-2)$-curves generates a sublattice of $\text{Pic}(\overline{V})$. The quotient has torsion if and only if this sublattice can be refined in $\mathbb{Z}^7$ without enlarging the rank. This immediately shows torsion-freeness in the cases $A_n$ for $n \neq 3$ and $E_6$ as the lattice discriminants are square-free.

For the other cases, the constructions described in [Do, page 278] yield explicit generators for sublattices of $\mathbb{Z}^7$. We summarize them in the table below.

| $2A_1$ | $(2, -1, -1, -1, -1, -1, -1)$
|        | $(0, 0, 0, 0, 0, 1, -1)$ |
| $A_3$  | $(0, 0, 0, 0, 0, 1, -1)$
|        | $(0, 0, 0, 1, -1, 0, 0)$ |
| $A_2 + A_1$ | $A_1$: $(2, -1, -1, -1, -1, -1)$
|          | $A_2$: $(0, 0, 0, 0, 0, 1, -1)$
|          | $A_2$: $(0, 0, 0, 0, 1, -1, 0)$ |
| $3A_1$ | $(2, -1, -1, -1, -1, -1, -1)$
|        | $(0, 0, 0, 0, 0, 1, -1)$
|        | $(0, 0, 0, 1, -1, 0, 0)$ |
| $2A_2$ | $A_1$: $(0, 0, 0, 0, 0, 1, -1)$
|        | $A_2$: $(0, 0, 0, 0, 1, -1, 0)$
|        | $A_2$: $(0, 0, 0, 0, 0, 1, -1)$ |
| $A_3 + A_1$ | $A_1$: $(2, -1, -1, -1, -1, -1, -1)$
|            | $A_2$: $(0, 0, 0, 0, 0, 1, -1)$
|            | $A_3$: $(0, 0, 0, 1, -1, 0, 0)$ |
| $D_4$  | $(1, -1, -1, -1, 0, 0, 0)$
|        | $(0, 1, 0, 0, 0, -1, 0)$
|        | $(0, 0, 0, 0, 0, 0, 1)$ |
| $A_2 + A_1$ | $A_1$: $(2, -1, -1, -1, -1, -1, -1)$
|            | $A_2$: $(0, 0, 0, 0, 0, 1, -1)$
|            | $A_2$: $(0, 0, 0, 1, -1, 0, 0)$ |
| $A_4 + A_1$ | $A_1$: $(2, -1, -1, -1, -1, -1, -1)$
|            | $A_4$: $(0, 0, 0, 0, 0, 1, -1)$
|            | $A_4$: $(0, 0, 0, 1, -1, 0, 0)$
|            | $A_4$: $(0, 0, 1, -1, 0, 0)$ |
BY

The refined lattice has discriminant 3 and is, therefore, not refinable.

Consider the cases 4̂A1. Then, we have subsets of the lattice base consisting of 2ep − e2 − · · · − e7, e1 − ep+1 for i = 3, . . . , 6, e1, and e7.

In the cases 4̂A1, A3 + 2A1, and A5 + A1, the lattices may indeed be extended by the vector (1, 0, −1, 0, −1, 0, −1) without changing the ranks. The lattices obtained in this way are not further refinable within Z7.

In the case 3A2, the vector (v1 + v3 − v4) − (v2 + v5 − v6) = −3e3 + 3e6 is obviously 3-divisible. The refined lattice has discriminant 3 and is, therefore, not refinable any further.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
D5 & (1,−1,−1, 0, 0, 0,−1) \\
   & (0, 1,−1, 0, 0, 0, 0) \\
   & (0, 0, 1,−1, 0, 0, 0) \\
   & (0, 0, 0, 1,−1, 0, 0) \\
   & (0, 0, 0, 0, 1,−1, 0) \\
\hline
4A1 & (2,−1,−1,−1,−1,−1) \\
   & (0, 0, 0, 0, 0, 1,−1) \\
   & (0, 0, 0, 1,−1, 0, 0) \\
   & (0, 1,−1, 0, 0, 0, 0) \\
\hline
2A2 + A1 & A1: (2,−1,−1,−1,−1,−1,−1) \\
       & 1. A2: (0, 0, 0, 0, 0, 0, 1,−1) \\
       & 1. A2: (0, 0, 0, 0, 0, 1,−1, 0) \\
       & 2. A2: (0, 0, 1,−1, 0, 0, 0) \\
       & 2. A2: (0, 1,−1, 0, 0, 0, 0) \\
\hline
A3 + 2A1 & A1: (2,−1,−1,−1,−1,−1,−1) \\
       & 1. A1: (0, 0, 0, 0, 0, 0, 1,−1) \\
       & A5: (0, 0, 0, 0, 0, 0, 1,−1, 0) \\
       & A5: (0, 0, 0, 0, 1,−1, 0, 0) \\
       & A5: (0, 0, 1,−1, 0, 0, 0) \\
       & A5: (0, 1,−1, 0, 0, 0, 0) \\
\hline
A5 + A1 & A1: (2,−1,−1,−1,−1,−1,−1) \\
       & A5: (0, 0, 0, 0, 0, 0, 1,−1) \\
       & A5: (0, 0, 0, 0, 0, 1,−1, 0) \\
       & A5: (0, 0, 0, 1,−1, 0, 0) \\
       & A5: (0, 0, 1,−1, 0, 0, 0) \\
\hline
3A2 & 1. A2: (1,−1,−1,−1, 0, 0, 0) \equiv v1 \\
     & 1. A2: (1, 0, 0, 0,−1,−1,−1) \equiv v2 \\
     & 2. A2: (0, 1,−1, 0, 0, 0, 0) \equiv v3 \\
     & 2. A2: (0, 0, 1,−1, 0, 0, 0) \equiv v4 \\
     & 3. A2: (0, 0, 0, 0, 1,−1, 0) \equiv v5 \\
     & 3. A2: (0, 0, 0, 0, 1,−1,−1) \equiv v6 \\
\hline
\end{tabular}
\caption{Sublattices in Z7 generated by the \(A\)-, \(D\)-, and \(E\)-configurations}
\end{table}

The assertions now follow from mechanical calculations.

In the cases where torsion-freeness is claimed, one may easily extend the basis of the sublattice given to a basis of Z7. For example, consider the types \(A_n + A_1\). Then, we have subsets of the lattice base consisting of \(2e_1 - e_2 - \cdots - e_7, e_1 - e_{i+1}\) for \(i = 3, \ldots, 6, e_1, \text{ and } e_7\).

\begin{proof}
In the cases 4A1, A3 + 2A1, and A5 + A1, the lattices may indeed be extended by the vector (1, 0, −1, 0, −1, 0, −1) without changing the ranks. The lattices obtained in this way are not further refinable within Z7.

In the case 3A2, the vector \((v_1 + v_3 - v_4) - (v_2 + v_5 - v_6) = -3e_3 + 3e_6\) is obviously 3-divisible. The refined lattice has discriminant 3 and is, therefore, not refinable any further.
\end{proof}

5.4.3. Summary. Let V be a geometrically irreducible cubic surface over a finite field \(\mathbb{F}_q\) for \(q = p^r\). Suppose that V is not a cone.

i) In all cases except for 4A1, A3 + 2A1, A5 + A1, 3A2, one has \(A_0(V^{\text{reg}}) = 0\).

ii) Consider the cases 4A1, A3 + 2A1, and A5 + A1. Then, \(A_0(V^{\text{reg}}) = \mathbb{Z}/2\mathbb{Z}\). Indeed, the Galois operation is necessarily trivial.
iii) In the case $3A_2$, the Galois group may act nontrivially on $\text{Pic}(V_{\text{reg}})^{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$. 
$\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ operates on this group as the sign of the permutation on the three singularities. Hence,

\[
A_0(V_{\text{reg}}) = \begin{cases} 
\mathbb{Z}/3\mathbb{Z} & \text{if the operation of Frob on the singularities is even and } \mathbb{F}_q \supset \mu_3 \\
0 & \text{if the operation of Frob on the singularities is odd and } \mathbb{F}_q \not\supset \mu_3, \\
\end{cases}
\]

6 Surjectivity

6.1. Corollary. Let $V$ be a geometrically irreducible cubic surface over $\mathbb{F}_q$, not being a cone. If 

\[
\pi_V: \text{MW}(V) \longrightarrow A_0(V_{\text{reg}})
\]

is not surjective then $V_{\text{reg}}$ has a nontrivial finite covering which is trivial over every $\mathbb{F}_q$-rational point.

Proof. Under the assumption, the image of the canonical map $V_{\text{reg}}(\mathbb{F}_q) \rightarrow h_0(V_{\text{reg}})$ generates a subgroup which is not dense. Hence, there are $l > 1$ and a surjective, continuous homomorphism $\alpha: h_0(V_{\text{reg}}) \rightarrow \mathbb{Z}/l\mathbb{Z}$ sending the whole image of $V_{\text{reg}}(\mathbb{F}_q)$ to zero.

The same is true for the composition $\alpha \circ \iota_{V_{\text{reg}}}: \pi_1^{\text{reg}}(V_{\text{reg}}) \rightarrow \mathbb{Z}/l\mathbb{Z}$. But this simply means that the $l$-sheeted covering of $V_{\text{reg}}$ defined by $\alpha \circ \iota_{V_{\text{reg}}}$ has exactly $l$ $\mathbb{F}_q$-rational points above every $x \in V_{\text{reg}}(\mathbb{F}_q)$. \hfill $\Box$

6.2. Remark. Suppose, $\pi_V$ were not surjective. Then, according to the lemma, we have a nontrivial covering $W$ such that $\#W(\mathbb{F}_q) = l \cdot \#V_{\text{reg}}(\mathbb{F}_q)$. The Weil conjectures, proven by P. Deligne, assure that this may be possible only for very small $q$.

6.3. Example. Let $V$ be a cubic surface of type $4A_1$, i.e., a Cayley cubic, over the finite field $\mathbb{F}_q$. Then, the canonical homomorphism 

\[
\pi_V: \text{MW}(V) \longrightarrow A_0(V_{\text{reg}})
\]

is surjective for $q > 13$.

Proof. Assume the contrary. Then, according to Corollary 6.1, we have a twofold covering $p: V' \rightarrow V$ ramified at the four singularities such that, over every smooth $\mathbb{F}_q$-rational point of $V$, there are two of $V'$. Being a cubic surface, $V$ has at least $q^2 - 5q + 1$ points. Hence, $\#V_{\text{reg}}(\mathbb{F}_q) \geq q^2 - 5q - 3$.

On the other hand, $\chi_{\text{top}}(V) = 3 + 6 - 4 \cdot 2 = 1$, as $V_{\text{reg}}$ is $\mathbb{P}^2$ blown up in six points with four lines deleted. Therefore, $\chi_{\text{top}}(V') = 6$. Indeed, $V'$ consists of the two sheets above $V_{\text{reg}}$ and four points of ramification.
We claim $\#V'(F_q) \leq q^2 + 4q + 1$. For this, first observe that $V'$ is simply connected as, otherwise, $V^{\text{reg}}$ had more coverings than the twofold one. Let $k$ be the number of blow-ups necessary in order to desingularize $V'$. Then, $\dim H^2_{\text{ét}}(V, \mathbb{Q}_l) = k + 4$ and one has the naive estimate $\#V(F_q) \leq q^2 + (k + 4)q + 1$. The claim follows.

Consequently, 

$$2(q^2 - 5q - 3) \leq 2 \cdot \#V^{\text{reg}}(F_q) \leq \#(V')^{\text{reg}}(F_q) \leq q^2 + 4q + 1$$

which implies $q \leq 14$, immediately. \hfill $\square$

7 Some observations

7.1. It is quite surprising that an irreducible cubic surface $V$ over $F_q$ may naturally have two or three classes of $F_q$-rational points. It turns out that, further, three classes are always equinumerous while two classes always differ in size by $q$.

When there are two classes, $V$ has a double cover and the two classes are essentially the points that split and the points that don’t. The cover is actually given by the Hessian.

7.2. Lemma. Let $V$ be a cubic surface over the finite field $F_q$. Suppose that, in every equivalence class of $V^{\text{reg}}(F_q)$, there is a point not contained in any of the lines lying on $V$.

i) Suppose $\#\text{MW}(V) = 2$. Assume further that not all points of $V^{\text{reg}}(F_q)$ are contained in a plane. Then, for the two equivalence classes $M_0, M_1$ of $V^{\text{reg}}(F_q)$, we have the relation $\#M_1 - \#M_2 = \pm q$.

ii) Suppose $\#\text{MW}(V) = 3$. Then, the three equivalence classes $M_0, M_1, M_2$ of $V^{\text{reg}}(F_q)$ are of the same size.

Proof. i) Without restriction, assume that the classes are denoted in such a way that a line not entirely contained in $V$ always meets zero or two points from $M_1$.

Then, fix a point $x \in M_1$ not contained in a line lying on $V$. By assumption, not the whole of $V^{\text{reg}}(F_q)$ is contained in the plane tangent at $x$. Consequently, there is some $x' \in V^{\text{reg}}(F_q)$ outside this tangent plane. The line $g$ connecting $x$ and $x'$ is not contained in $V$. It meets $V$ in two distinct points $x, y \in M_1$ and in $z \in M_0$.

Now, we intersect $V$ with the planes containing $g$. We assert that every of the curves $C_t$ arising contains as many points from $M_0$ as from $M_1$. This immediately implies the assertion as we have $(q + 1)$ planes. Hence, equinumerosity occurs as soon as we count the points $x, y, z$ multiply, $(q + 1)$ times.

Let now $C_t$ be one of the intersection curves. We first observe that $x \in C_t$ is a smooth point. In fact, we do not intersect $V$ with the tangent plane at $x$ since that does not contain $g$. $C_t$ may be reducible. However, $x$ is, by assumption, not contained in a line. Therefore, for every $p \in C_t(F_q)$ there is a uniquely determined
\[ p' \in C_t(\mathbb{F}_q) \text{ such that } x, p, \text{ and } p' \text{ are collinear. As } p \text{ and } p' \text{ are in different classes, the assertion follows from this.} \]

ii) Here, there are two cases.

First case. If \( x \in M_i, y \in M_j, \) and \( z \in M_k \) are the three points of intersection of a line with \( V \) then \( i + j + k \equiv 0 \pmod{3} \).

We choose a point \( x \in M_0 \) which is not contained in any of the lines on \( V \). Then, for every \( p \in M_1 \), there is a unique \( p' \in M_2 \) such that \( x, p, \) and \( p' \) are collinear. As this assignment is invertible, one has \( \#M_1 = \#M_2 \).

Analogously, a starting point \( x \in M_1 \) immediately yields the equality \( \#M_2 = \#M_0 \).

Second case. If \( x \in M_i, y \in M_j, \) and \( z \in M_k \) are the three points of intersection of a line with \( V \) then \( i + j + k \not\equiv 0 \pmod{3} \).

We may assume without restriction that \( i + j + k \equiv 1 \pmod{3} \). Choose a point \( x \in M_0 \) which is not contained in any of the lines on \( V \). The tangent plane \( T_x \) contains, besides \( x \), only points from \( M_1 \). Further, there are exactly \( q + 1 \) of them, as, by the assumption of this case, there is no line tangent at \( x \) of order three.

On the other hand, outside \( T_x \), the sets \( M_0 \) and \( M_1 \) are equinumerous since the lines through \( x \) cause a bijection. Consequently, \( \#M_1 = \#M_0 + q \).

Analogously, we obtain \( \#M_2 = \#M_1 + q \) and \( \#M_0 = \#M_2 + q \) when starting with a point \( x \in M_1 \) or \( x \in M_2 \), respectively. Thus, the second case is contradictory. \( \square \)

7.3. Definition. —— Let \( V \) be a cubic surface over the finite field \( \mathbb{F}_q \) such that \( \#MW(V) = 2 \). Then, \( V^{\text{reg}}(\mathbb{F}_q) \) decomposes into exactly two equivalence classes. Further, there is at least one line meeting \( V \) in three smooth \( \mathbb{F}_q \)-rational points.

We will call that equivalence class positive that occurs an odd number of times on each line. The other class will be called negative.

7.4. Lemma (Connection to the Hessian). —— Let \( V \), given by \( F(X_0, \ldots, X_3) = 0 \), be a cubic surface over the finite field \( \mathbb{F}_q \) of characteristic \( \neq 2 \). Suppose \( \#MW(V) = 2 \). Then, the following is true.

If \( p \in V^{\text{reg}}(\mathbb{F}_q) \) is a negative point not lying on a line contained in \( V \) then the Hessian

\[
\det \frac{\partial^2 F}{\partial X_i \partial X_j}(p)
\]

is a non-square in \( \mathbb{F}_q \).

Proof. Consider the tangent plane \( T_p \) at \( p \). The intersection \( C_p := V \cap T_p \) is a cubic curve with a singularity at \( p \). Thus, in affine coordinates and locally near \( p \), the equation of \( C_p \) is of the form \( Q(x, y) + K(x, y) = 0 \) for a quadratic form \( Q \) and a cubic form \( K \).
By assumption, there is no line in \( T_p \) meeting \( p \) with multiplicity 3. This means, in particular, that \( p \in C_p \) is a double point, not a triple point. Further, the two tangent directions at \( p \) are not defined over \( \mathbb{F}_q \). In other words, the binary quadratic form \( Q \) does not represent zero over \( \mathbb{F}_q \). This exactly means that minus the discriminant of \( Q \) is a non-square in \( \mathbb{F}_q \).

We claim that \((-\text{disc } Q)\) coincides, up to square factors, with the Hessian of \( F \) at \( p \). For this, we assume without restriction that \( p = (1 : 0 : 0 : 0) \) and that the tangent plane \( T_p \) is given by \( X_1 = 0 \). Then,

\[
F(0, \ldots , X_3) = CX_0^2X_1 + X_0\tilde{Q}(X_1, X_2, X_3) + \tilde{K}(X_1, X_2, X_3)
\]

for \( C \neq 0 \), \( Q(x, y) = \tilde{Q}(0, x, y) \), and \( K(x, y) = \tilde{K}(0, x, y) \). A direct calculation shows that the Hessian matrix at \((1 : 0 : 0 : 0)\) is equal to

\[
\begin{pmatrix}
0 & 2C & 0 & 0 \\
2C & \frac{\partial^2 \tilde{Q}}{\partial X_1^2} & \frac{\partial^2 \tilde{Q}}{\partial X_2^2} & \frac{\partial^2 \tilde{Q}}{\partial X_3^2} \\
0 & \frac{\partial^2 \tilde{Q}}{\partial X_1 \partial X_2} & \frac{\partial^2 \tilde{Q}}{\partial X_1 \partial X_3} & \frac{\partial^2 \tilde{Q}}{\partial X_2 \partial X_3} \\
0 & \frac{\partial^2 \tilde{Q}}{\partial X_1 \partial X_3} & \frac{\partial^2 \tilde{Q}}{\partial X_2 \partial X_3} & 0
\end{pmatrix}
\]

The assertion follows immediately from this. \( \square \)

### 8 Algorithms

#### 8.1. Algorithm (Equivalent points)

- i) Using a random number generator, choose four distinct points \( x_{11}, x_{12}, x_{21}, x_{22} \in V_{\text{reg}}(\mathbb{F}_q) \).
- ii) Determine four points \( x_{13}, x_{23}, x_{31}, x_{32} \in V_{\text{reg}}(\mathbb{F}_q) \) such that the relations \([x_{11}, x_{12}, x_{13}], [x_{21}, x_{22}, x_{23}], [x_{11}, x_{21}, x_{31}], \text{ and } [x_{12}, x_{22}, x_{32}]\) are fulfilled. If this turns out to be impossible as \((x_{11}, x_{12}), (x_{21}, x_{22}), (x_{11}, x_{21}), \text{ or } (x_{12}, x_{22})\) are lying on a line completely contained in \( V \) then output FAIL and terminate prematurely.
- iii) Now, determine points \( x_{33} \) and \( x'_{33} \) such that \([x_{13}, x_{23}, x_{33}] \text{ and } [x_{31}, x_{32}, x'_{33}]\). If this turns out to be impossible as \((x_{13}, x_{23}) \text{ or } (x_{31}, x_{32})\) are lying on a line completely contained in \( V \) then output FAIL and terminate prematurely.
- iv) Output “\( x_{33} \) and \( x'_{33} \) are equivalent.”

#### 8.2. Algorithm (A point being equivalent to a given \( x_0 \in V_{\text{reg}}(\mathbb{F}_q) \))

- i) Execute Algorithm 8.1 in order to find two mutually equivalent points \( x_1 \) and \( x_2 \).
- ii) Determine a point \( x'_1 \) such that \([x_1, x_0, x'_1] \). If this turns out to be impossible as \((x_1, x_0)\) are lying on a line completely contained in \( V \) then output FAIL and terminate prematurely.
iii) Now, determine a point $x_0'$ such that $[x_1', x_2, x_0']$. If this turns out to be impossible as $(x_1', x_2)$ are lying on a line completely contained in $V$ then output FAIL and terminate prematurely.

iv) Output “$x_0'$ is equivalent to $x_0$.”

8.3. Algorithm (Partition of the points). ——

i) Choose a natural number $N$.

ii) Decompose $V_{\text{reg}}(\mathbb{F}_q)$ into a set $\mathcal{M} = \{N_1, \ldots, N_m\} = \{\{x_1\}, \ldots, \{x_m\}\}$ of singletons.

iii) Execute Algorithm 8.1, $Nq^2$ times. When two equivalent points $x_1 \in M_k$ and $x_2 \in M_l$ for $k \neq l$ are found, unite $M_k$ with $M_l$ and reduce $m$ by 1.

iv) List the singletons still contained in $\mathcal{M}$, i.e., the points that were never met in step iii). For each element in the list obtained, execute Algorithm 8.2 $N$ times. When two equivalent points $x_1 \in M_k$ and $x_2 \in M_l$ for $k \neq l$ are found, unite $M_k$ with $M_l$ and reduce $m$ by 1.

v) If sets of size less than $q$ remain in $\mathcal{M}$ then choose a single element from each of these sets. For each element in the list obtained, execute Algorithm 8.2 $N$ times. When two equivalent points $x_1 \in M_k$ and $x_2 \in M_l$ for $k \neq l$ are found, unite $M_k$ with $M_l$ and reduce $m$ by 1.

vi) Output the partition of $V_{\text{reg}}(\mathbb{F}_q)$ found.

8.4. Remarks. —— i) Algorithm 8.3 finds a partition which is possibly too fine in comparison with the actual partition into equivalence classes.

ii) In practice, the value $N = 7$ seems to work perfectly, for $p = 5$ as well as for the biggest primes for which such an algorithm seems reasonable.

8.5. Lemma. —— Let $V$ be a cubic surface over the finite field $\mathbb{F}_q$. Suppose that, in every equivalence class of $V_{\text{reg}}(\mathbb{F}_q)$, there is a point not contained in any of the lines lying on $V$. Then, the following statements are true.

i) Let $x_0 \in V_{\text{reg}}(\mathbb{F}_q)$ be arbitrary. Then, every element in $\text{MW}(V)$ is of the form $[x] - [x_0]$.

ii) In particular, $\#\text{MW}(V)$ is equal to the number of equivalence classes of $V_{\text{reg}}(\mathbb{F}_q)$.

Proof. i) The elements given clearly form a system of generators. It will therefore suffice to show closedness under formation of differences. This means, every $[x_1] - [x_2]$ has to be expressed as $[x] - [x_0]$.

For this, we may assume without restriction that neither $x_1$, nor $x_2$ are contained in a line lying on $V$. Then, there are a point $x_1' \in V_{\text{reg}}(\mathbb{F}_q)$ such that $[x_1, x_0, x_1']$ and, finally, a point $x \in V_{\text{reg}}(\mathbb{F}_q)$ such that $[x_1', x_2, x]$. In $\text{MW}(V)$, we now have the relation $[x_1] + [x_0] + [x_1'] - [x_1'] - [x_2] - [x] = 0$. This is precisely the assertion.

ii) is clear. □
9 Experiments

9.1. Description of the sample. —— We let \( p \) run through the prime numbers form 5 through 101. For each of the primes, we followed the classification of cubic surfaces as described in Remarks 2.4. For each type, we selected ten examples by help of a random number generator. For those types which clearly have no moduli, we took only one example. We avoided the surfaces decomposing into three planes over a proper extension of \( \mathbb{F}_p \) as, for these, \( \text{MW}(V) \) is known to degenerate. All in all, we worked with 330 cubic surfaces per prime.

For each surface, we determined the partition of \( V(\mathbb{F}_p) \) into equivalence classes. For this, we run an implementation of Algorithm 8.3 in magma.

9.2. The results. —— i) The partition of the points found actually allowed us to determine \( \text{MW}(V) \) for every surface in the sample.

ii) There is an observation which is by far more astonishing. In each case, according to the theory described, we know an abelian group, \( \text{MW}(V) \) naturally surjects to. It turned out that \( \text{MW}(V) \) was always equal that group with only one exception.

9.3. The exception. —— The exception occurred for \( p = 5 \). It was the cone over the elliptic curve given by \( y^2 = x^3 + 2x \). As this elliptic curve has only two \( \mathbb{F}_5 \)-rational points, the construction of \( \text{MW}(V) \) must degenerate.

9.4. Remark. —— This effect clearly becomes much worse for \( p = 2 \) or 3. This is one of the reasons why these primes were excluded from the experiments.

9.5. Summary. —— I.i) Among the normal cubic surfaces having only double points, we always found \( \text{MW}(V) = 0 \) except for the cases \( 4A_1, A_3 + 2A_1, A_5 + A_1 \), and \( 3A_2 \). In the first three of these cases, we have \( \text{MW}(V) = \mathbb{Z}/2\mathbb{Z} \).

Finally, in the case \( 3A_2 \), we established that \( \text{MW}(V) = \mathbb{Z}/3\mathbb{Z} \) for \( p \equiv 1 \pmod{3} \) and Frob acting on the singular points by an even permutation and for \( p \equiv 2 \pmod{3} \) and Frob acting by an odd permutation. Otherwise, \( \text{MW}(V) = 0 \).

I.ii) and II.ii) Ignoring the exception mentioned, for the cones, \( \text{MW}(V) \) was always equal to the Mordell-Weil group of the underlying curve.

II.i) The cubic ruled surfaces always fulfilled \( \text{MW}(V) = 0 \).

Red i) When \( V \) consisted of a non-degenerate quadric and a plane, we always found that \( \text{MW}(V) = \mathbb{Z} \), two points being equivalent if and only if they belonged to the same component. When the quadric was a cone and the plane did not meet the cusp, it turned out that \( \text{MW}(V) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \), the surjection described in Example 4.2 being bijective.

A cubic surface consisting of a cone and a plane through the cusp is a cone over a reducible cubic curve. Here, \( \text{MW}(V) \) was always isomorphic to the Mordell-Weil group of the curve.
Red ii) A cubic surface consisting of three planes meeting in a point is the cone over a triangle. In the experiment, MW(V) was always equal to the Mordell-Weil group of the triangle.

Finally, three planes meeting in a line form a cone in many ways. Hence, two distinct points are never equivalent to each other. We have MW(V) ∼ (K+)2 ⊕ Z2.

9.6. Remark. —— The case of a cubic surface consisting of three planes with a line in common is the easiest from the theoretical point of view. For Algorithm 8.3, it is, however, the most complicated one. No simplification occurs as no equivalent points may be found. The running time is dominated by steps iv) and v) which are otherwise negligible. For p > 70, we excluded this case from the experiments.

9.7. Remark. —— The total running time was eight minutes for p = 5, a little less than an hour for p = 37, three and a half hours for p = 71, and more than ten hours for p = 101.

References


[El] Elsenhans, A.-S.: The Cayley cubic has infinite rank, Internal Note


