



ELSEVIER

Contents lists available at SciVerse ScienceDirect

## Journal of Number Theory

[www.elsevier.com/locate/jnt](http://www.elsevier.com/locate/jnt)

## On the number of Mordell–Weil generators for cubic surfaces

Samir Siksek<sup>1</sup>

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom

## ARTICLE INFO

## Article history:

Received 5 February 2012

Revised 7 March 2012

Accepted 29 May 2012

Available online 20 July 2012

Communicated by David Goss

## MSC:

primary 14G05

secondary 11G35, 11G25

## Keywords:

Cubic surfaces

Rational points

Mordell–Weil problem

Brauer–Manin obstruction

## ABSTRACT

Let  $S$  be a smooth cubic surface over a field  $K$ . It is well-known that new  $K$ -rational points may be obtained from old ones by secant and tangent constructions. In this paper we prove, for a cubic surface containing a pair of skew rational lines over a field with at least 13 elements, that the rational points are generated by just one point. We also prove a cubic surface analogue of the unboundedness of ranks conjecture for elliptic curves over the rationals.

© 2012 Elsevier Inc. All rights reserved.

## 1. Introduction

Let  $C$  be a smooth plane cubic curve over  $\mathbb{Q}$ . The Mordell–Weil Theorem can be restated as follows: there is a finite subset  $B$  of  $C(\mathbb{Q})$  such that the whole of  $C(\mathbb{Q})$  can be obtained from this subset by drawing secants and tangents through pairs of previously constructed points and consecutively adding their new intersection points with  $C$ . It is conjectured that a minimal such  $B$  can be arbitrarily large; this is indeed the well-known conjecture that there are elliptic curves with arbitrarily large ranks. This paper is concerned with the cubic surface analogues of the Mordell–Weil Theorem and the unboundedness of ranks.

Let  $K$  be a field and let  $S$  be a smooth cubic surface over  $K$  in  $\mathbb{P}^3$ . By a  $K$ -line we mean a line  $\ell \subset \mathbb{P}^3$  that is defined over  $K$ . If  $\ell \not\subset S$  then  $\ell \cdot S = P + Q + R$  where  $P, Q, R \in S$ . If any two of  $P,$

<sup>1</sup> E-mail address: [s.siksek@warwick.ac.uk](mailto:s.siksek@warwick.ac.uk).

<sup>1</sup> The author is supported by an EPSRC Leadership Fellowship.

$Q, R$  are  $K$ -points then so is the third. The line  $\ell$  is tangent at  $P$  if and only if  $P$  appears more than once in the sum  $P + Q + R$ . If  $B \subseteq S(K)$ , we shall write  $\text{Span}(B)$  for the subset of  $S(K)$  generated from  $B$  by successive secant and tangent constructions. More formally, we define a sequence

$$B = B_0 \subseteq B_1 \subseteq B_2 \subseteq \dots \subseteq S(K)$$

as follows. We let  $B_{n+1}$  be the set of points  $R \in S(K)$  such that either  $R \in B_n$ , or for some  $K$ -line  $\ell \not\subset S$  we have  $\ell \cdot S = P + Q + R$  where  $P, Q \in B_n$ . Then  $\text{Span}(B) = \bigcup B_n$ . In view of the Mordell–Weil Theorem for cubic curves it is natural to ask, for  $K = \mathbb{Q}$  say, if there is some finite subset  $B \subset S(K)$  such that  $\text{Span}(B) = S(K)$ . As far as we are aware, the possible existence of such an analogue of the Mordell–Weil Theorem was first mentioned by Segre [21, p. 26] in 1943. Manin [15, p. 3] asks the same question for fields  $K$  finitely generated over their prime subfields. He calls this [16] the Mordell–Weil problem for cubic surfaces. The results of numerical experiments by Zagier (described by Manin in [16]) and Vioreanu [25] lead different experts to different opinions about the validity of this Mordell–Weil Conjecture. However, Manin [16] and Kanevsky and Manin [12] prove the existence of finite generating sets for rational points on certain Zariski open subsets of rationally trivial cubic surfaces with **modified** composition operations induced by birational maps  $S \dashrightarrow \mathbb{P}^2$ . However, we are not aware of even a single example in the literature where the existence of a finite set  $B$  that generates  $S(K)$  via the secant and tangent process is proven. In this paper we give a positive answer to a special case of the Mordell–Weil problem.

**Theorem 1.** *Let  $K$  be a field with at least 13 elements. Let  $S$  be a smooth cubic surface over  $K$ . Suppose  $S$  contains a pair of skew lines both defined over  $K$ . Let  $P \in S(K)$  be a point on either line that is not an Eckardt point. Then  $\text{Span}(P) = S(K)$ .*

An Eckardt point is a point where three of the lines contained in  $S$  meet. Note that Theorem 1 does not make the assumption that the field is finitely generated over its prime subfield! It is certainly true that every smooth cubic surface over an algebraically closed field is generated by a single element. The theorem probably holds for most fields with fewer than 13 elements, but the proof is likely to involve a tedious examination of special cases and we have not attempted it. It is well-known that a cubic surface with a pair of skew  $K$ -lines  $\ell, \ell'$  is birational to  $\ell \times \ell'$ . The proof of Theorem 1 (given in Section 3) is an extension of the proof that  $S$  is birational to  $\ell \times \ell'$ .

Now let us write

$$r(S, K) := \min\{\#B : B \subseteq S(K) \text{ and } \text{Span}(B) = S(K)\}.$$

We are unable to show that  $r(S, K)$  is finite for cubic surfaces without a skew pair of  $K$ -lines. However, in some cases we can bound  $r(S, K)$  from below. We use this to show that  $r(S, \mathbb{Q})$  is arbitrarily large as  $S$  varies among smooth cubic surfaces over  $\mathbb{Q}$ . To do this we introduce and study a simple analogue of the Picard group of an elliptic curve. Let

$$G_S(K) = \bigoplus_{P \in S(K)} \mathbb{Z} \cdot P$$

be the free abelian group generated by the  $K$ -rational points of  $S$ . Let  $G'_S(K)$  be the subgroup generated by all three point sums  $P + Q + R$  with  $P, Q, R \in S(K)$  such that

- (i) there is  $K$ -line  $\ell$  not contained in  $S$  with  $\ell \cdot S = P + Q + R$ , or
- (ii) there is a  $K$ -line  $\ell$  contained in  $S$  such that  $P, Q, R \in \ell$ .

The degree map  $\text{deg} : G_S(K) \rightarrow \mathbb{Z}$  is given by  $\text{deg}(\sum a_i P_i) = \sum a_i$ . Let

$$G'_S(K) = \{D \in G_S(K) : \text{deg}(D) = 0\}.$$

Let  $H_S(K) := G_S(K)/G'_S(K)$ . If  $P \in S(K)$  we denote the image of  $P$  in  $H_S(K)$  by  $[P]$ . The degree map remains well defined on  $H_S(K)$ : we let  $\text{deg} : H_S(K) \rightarrow \mathbb{Z}$  be given by  $\text{deg}(\sum a_i [P_i]) = \sum a_i$ . We shall write

$$H^0_S(K) = \{D \in H_S(K) : \text{deg}(D) = 0\}.$$

If  $S(K) \neq \emptyset$  then the degree homomorphism clearly induces an isomorphism

$$H_S(K)/H^0_S(K) \cong \mathbb{Z}.$$

The group  $H_S(K)$  will allow us to study  $r(S, K)$ .

**Theorem 2.** Let  $p_1, \dots, p_s$  ( $s \geq 1$ ) be distinct primes such that

- (a)  $p_i \equiv 1 \pmod{3}$ ,
- (b) 2 is a cube modulo  $p_i$ .

Let  $M = \prod p_i$  and let  $S = S_M/\mathbb{Q}$  be the smooth cubic surface given by

$$S_M: x^3 + y^3 + z(z^2 + Mw^2) = 0. \tag{1}$$

Write  $H_S(\mathbb{Q})[2]$  for the 2-torsion subgroup of  $H_S(\mathbb{Q})$ . Then  $H^0_S(\mathbb{Q}) = H_S(\mathbb{Q})[2]$  and

$$r(S, \mathbb{Q}) \geq \dim_{\mathbb{F}_2} H_S(\mathbb{Q})[2] \geq 2s.$$

A prime  $p$  satisfies conditions (a) and (b) of the theorem if and only if the polynomial  $t^3 - 2$  has three roots modulo  $p$ . By the Chebotarëv Density Theorem such primes form a set with Dirichlet density  $1/6$  (see for example [10, pp. 227–229]). We thus see that  $r(S_M, \mathbb{Q})$  becomes arbitrarily large as  $M$  varies. The cubic surface  $S_M$  has precisely one  $\mathbb{Q}$ -rational line, which is given by  $x + y = z = 0$ .

Our second theorem concerns a family of diagonal cubic surfaces. To obtain a similar result for diagonal cubic surfaces we need to assume the following conjecture.

**Conjecture 1.1** (Colliot-Thélène). Let  $X$  be smooth and proper geometrically rational surface over a number field  $K$ . Then the Brauer–Manin obstruction is the only one to weak approximation on  $X$ .

This conjecture is stated as a question by Colliot-Thélène and Sansuc in [6, Section V], but since then has been stated as a conjecture by Colliot-Thélène [2, p. 319]. Indeed for the proof of Theorem 2 we need the fact that  $S_M$  satisfies weak approximation, but fortunately this follows from a theorem of Salberger and Skorobogatov on degree 4 del Pezzo surfaces.

**Theorem 3.** Let  $p_1, \dots, p_s$  ( $s \geq 1$ ) be distinct primes  $\equiv 1 \pmod{3}$ . Let  $M = 3 \prod p_i$  and let  $S = S'_M/\mathbb{Q}$  be the smooth cubic surface given by

$$S'_M: x^3 + y^3 + z^3 + Mw^3 = 0. \tag{2}$$

Assume that the Brauer–Manin obstruction is the only one to weak approximation for  $S$ . Then

$$r(S, \mathbb{Q}) \geq \dim_{\mathbb{F}_3} H_S^0(\mathbb{Q})/3H_S^0(\mathbb{Q}) \geq 2s.$$

Theorem 3 is less satisfactory than Theorem 2 in two obvious ways. The first is that it is conditional on the yet unproven (and probably very difficult) conjecture concerning weak approximation. The second is that we do not know if  $H_S^0(\mathbb{Q})$  contains any elements of infinite order or is merely a torsion group.

The paper is organized as follows. In Section 2 we briefly review what we need from the geometry of cubic surfaces. The proof of Theorem 1 is given in Section 3. In Section 4 we prove some useful results about  $H_S(K)$  that follow from the definition and the elementary geometry of cubic surfaces. In particular, we show that  $H_S^0(K) = H_S(K)[2]$  if  $S$  contains a  $K$ -line, and that  $H_S^0(K) = 0$  if  $S$  contains a pair of skew  $K$ -lines. In Section 5 we study  $H_S(K)$  for local fields  $K$ . In particular we show that  $H_S^0(K)$  is finite and that the map  $S(K) \rightarrow H_S(K)$  given by  $P \mapsto [P]$  is locally constant. In Section 6 we show that  $H_S^0(\mathbb{R}) = 0$  or  $\mathbb{Z}/2\mathbb{Z}$  depending on whether  $S(\mathbb{R})$  has one or two connected components. In Section 7, for  $K$  a number field and  $\Delta$  a finite set of places of  $K$ , we study the diagonal map  $\mu_\Delta : H_S(K) \rightarrow \prod_{v \in \Delta} H_S(K_v)$ ; for example if  $S/K$  satisfies weak approximation then we show that the map is surjective. The proofs of Theorems 2 and 3 essentially boil down to proving (enough of) weak approximation and then estimating the size of the target space of the diagonal map  $\mu_\Delta$  for  $\Delta = \{p_1, \dots, p_s\}$ . To this end we briefly introduce the Brauer–Manin obstruction (Section 8) and apply it in Sections 9 and 10 to prove (enough of) weak approximation for the surfaces  $S_M$  and  $S'_M$ , where in the latter case we are forced to assume Colliot-Thélène’s Conjecture 1.1. Finally we must study  $H_S(\mathbb{Q}_p)$  for the surfaces  $S = S_M, S = S'_M$ . Let  $C$  be the plane genus 1 curve given by the equation

$$C: x^3 + y^3 + z^3 = 0. \tag{3}$$

For a prime  $p \neq 3$  we shall denote  $C_p = C \times \mathbb{F}_p$ . For  $p = p_1, \dots, p_s$  it is easily seen that  $S_M$  and  $S'_M$  both reduce to a cone over  $C_p$ . This fact is crucial to the proofs of both Theorems 2 and 3. In Section 11 we shall briefly study  $\text{Pic}^0(C_p)/2\text{Pic}^0(C_p)$  and  $\text{Pic}^0(C_p)/3\text{Pic}^0(C_p)$ . Section 12 quickly reviews good choices of parametrizations of lines in  $\mathbb{P}^3$ : a good choice is one that still parametrizes the lines after reduction modulo  $p$ . In Section 13 we shall construct, for the surface  $S = S_M$ , a surjective homomorphism  $H_S^0(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)/2\text{Pic}^0(C_p)$ . In Section 14 we use this and the surjectivity of the diagonal map  $\mu_\Delta$  for  $\Delta = \{p_1, \dots, p_s\}$  to deduce Theorem 2. We then turn our attention to the surface  $S = S'_M$ . In Section 15 we construct a surjective homomorphism  $H_S^0(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)/3\text{Pic}^0(C_p)$ , and conclude the proof of Theorem 3 in Section 16.

One reason why  $H_S(K)$  may be of interest is that it seems to be intimately related to the Chow group  $\text{CH}_0(S)$  of zero-cycles on  $S/K$ . It is straightforward to see that elements of  $G_S''(K)$  are zero-cycles that are rationally equivalent to 0. Thus we have a natural homomorphism

$$\epsilon : H_S(K) \rightarrow \text{CH}_0(S).$$

In subsequent papers we plan to address the relationship of  $H_S(K)$  with  $\text{CH}_0(S)$ , as well as various constructions found in [15] such as Moufang loops,  $R$ -equivalence and universal equivalence. We will also make a more extensive study of  $H_S(K)$  for  $K$  a finite or local field, and the natural pairing  $\text{Br}(S) \times \prod H_S(K_v) \rightarrow \mathbb{Q}/\mathbb{Z}$  induced by the corresponding pairing for the Chow group of zero-cycles.

## 2. Some geometry

We shall need some basic material on the geometry of cubic surfaces. We do not claim any originality in this section, although we occasionally sketch proofs of well-known statements in order to verify that these hold in small positive characteristic.

**Theorem 4** (Cayley–Salmon). *Every non-singular cubic surface over an algebraically closed field contains exactly 27 lines.*

*Every line  $\ell$  on the surface meets exactly 10 other lines, which break up into 5 pairs  $\ell_i, \ell'_i$  ( $i = 1, \dots, 5$ ) such that  $\ell, \ell_i$  and  $\ell'_i$  are coplanar, and  $(\ell_i \cup \ell'_i) \cap (\ell_j \cup \ell'_j) = \emptyset$  for  $i \neq j$ .*

**Proof.** For a proof see [9, V.4] or [19, Section IV.2].  $\square$

For now  $S$  will denote a smooth cubic surface in  $\mathbb{P}^3$  over a field  $K$ , defined by homogeneous cubic polynomial  $F \in K[x_0, x_1, x_2, x_3]$ .

For a point  $P \in S(\bar{K})$ , we shall denote the tangent plane to  $S$  at  $P$  by  $\Pi_P$ . This is given by  $\Pi_P : \nabla F(P) \cdot \mathbf{x} = 0$ . We shall write  $\Gamma_P$  for the plane curve  $S \cdot \Pi_P$ . It is easy to check (using the smoothness of  $S$ ) that  $\Gamma_P$  does not contain any multiple components. It is a degree 3 plane curve which is singular at  $P$ . If  $\Gamma_P$  is irreducible, it is nodal or cuspidal at  $P$ . If  $\Gamma_P$  is reducible then it is the union of a line and an irreducible conic, or of three distinct lines.

**Lemma 2.1.** *Let  $P \in S(\bar{K})$ . The curve  $\Gamma_P$  contains every  $\bar{K}$ -line on  $S$  that passes through  $P$ .*

**Proof.** By Euler’s Homogeneous Function Theorem,  $P \cdot \nabla F(P) = 3 \cdot F(P) = 0$ . The line  $\ell$  has a parametrization of the form  $sP + t\mathbf{v}$  with  $(s : t) \in \mathbb{P}^1$ . Thus the polynomial  $F(sP + t\mathbf{v})$  vanishes identically. However, coefficient of  $ts^2$  in this polynomial is  $(\nabla F)(P) \cdot \mathbf{v}$ . This shows that  $\ell$  is also contained in  $\Pi_P$ , and hence in  $\Gamma_P$ .  $\square$

A  $\bar{K}$ -line  $\ell$  is called an *asymptotic line* (cf. [26, Section 2]) at  $P \in S(\bar{K})$  if  $(\ell \cdot S)_P \geq 3$ . As  $S$  is a cubic surface, it is seen that for an asymptotic line  $\ell$  at  $P$ , either  $(\ell \cdot S)_P = 3$  or  $\ell \subset S$ . The asymptotic lines at  $P$  are contained in  $\Pi_P$ . Any line contained in  $S$  and passing through  $P$  is an asymptotic line through  $P$ . The number of distinct asymptotic  $\bar{K}$ -lines at  $P$  is either 1, 2 or infinity. If  $S$  has either 1 or infinitely many asymptotic lines at  $P$  then we shall call  $P$  a *parabolic point*. The case where there are infinitely many asymptotic lines at  $P$  is special: in this case  $\Gamma_P$  decomposes as a union of three  $\bar{K}$ -lines lying on  $S$  and so the point  $P$  is an *Eckardt point*. If  $P$  is parabolic but not Eckardt, the curve  $\Gamma_P$  has a cusp at  $P$ . If  $P$  is non-parabolic, then  $\Gamma_P$  has a node at  $P$ .

Next we suppose  $P \in S(K)$ . Then  $\Pi_P$  and  $\Gamma_P$  are defined over  $K$ . Suppose  $P$  is non-parabolic. Thus there are precisely two (distinct) asymptotic lines at  $P$ . If these two lines are individually defined over  $K$  then we say that  $P$  is *K-hyperbolic*. Otherwise the two lines are defined over a quadratic extension of  $K$  and conjugate; in this case we shall say that  $P$  is *K-elliptic*. If  $K = \mathbb{R}$  then the terms parabolic, hyperbolic and elliptic agree with their usual meanings in differential geometry: they correspond to points where the Gaussian curvature is respectively  $= 0, > 0$  and  $< 0$ .

We shall also need to study the number of parabolic points on a line lying on a cubic surface. Let  $\mathbb{P}^{3*}$  be the dual projective space and write  $\gamma : S \rightarrow \mathbb{P}^{3*}$  for the *Gauss map* which sends a point to its tangent plane. A useful characterisation of parabolic points is that they are the points of ramification of the Gauss map [26, Section 2]. If  $\ell \subset S$  and  $P \in \ell$ , then  $\ell$  is contained in the tangent plane  $\Pi_P$ . The family of planes through  $\ell$  can be identified with  $\mathbb{P}^1$  and once such an identification is fixed we let  $\gamma_\ell : \ell \rightarrow \mathbb{P}^1$  be the map that sends a point on  $\ell$  to its tangent plane through  $\ell$ .

**Lemma 2.2.** *Let  $\ell$  be a  $K$ -line contained in  $S$ . Then every  $P \in \ell(K)$  is either parabolic or  $K$ -hyperbolic.*

- (i) *If  $\text{char}(K) \neq 2$  then  $\gamma_\ell$  is separable. Precisely two points  $P \in \ell(\bar{K})$  are parabolic, and so there are at most two Eckardt points on  $\ell$ .*
- (ii) *If  $\text{char}(K) = 2$  and  $\gamma_\ell$  is separable then there is precisely one point  $P \in \ell(\bar{K})$  which is parabolic and so at most one Eckardt point on  $\ell$ .*
- (iii) *If  $\text{char}(K) = 2$  and  $\gamma_\ell$  is inseparable then every point  $P \in \ell(\bar{K})$  is parabolic and the line  $\ell$  contains exactly 5 Eckardt points.*

**Proof.** This is a well-known classical result for cubic surfaces over the reals or complexes; see for example [20, pp. 103–104]. Let  $P \in \ell(K)$ . First we would like to show that any  $P \in \ell(K)$  is either parabolic or  $K$ -hyperbolic. Suppose  $P$  is not parabolic. Then  $S$  has precisely two asymptotic lines passing through  $P$ . One of these is  $\ell$ . Since this pair of asymptotic lines must be  $K$ -rational as a whole, the other asymptotic line is  $K$ -rational. Thus  $P$  is  $K$ -hyperbolic.

Next we would like to count the number of parabolic points on  $\ell$ . By a projective transformation defined over  $K$  we may suppose that  $\ell$  passes through the point  $(0 : 0 : 0 : 1)$ , that the tangent plane at this point is  $x_0 = 0$  and that the line is  $x_0 = x_1 = 0$ . Then  $F$  has the form

$$F = x_0Q + x_1R$$

with  $Q, R$  are homogeneous quadratic forms in  $K[x_0, x_1, x_2, x_3]$ . Now  $\gamma_\ell : \ell \rightarrow \mathbb{P}^1$  can be written as  $P \mapsto (Q(P) : R(P))$ . The fact that  $S$  is non-singular implies that  $Q$  and  $R$  do not simultaneously vanish along the line  $\ell$ . Thus  $\gamma_\ell$  has degree 2. Suppose first that  $\gamma_\ell$  is separable—this is always the case if  $\text{char}(K) \neq 2$ . Applying the Hurwitz Theorem [9, Section IV.2] to  $\gamma_\ell$  immediately gives that the ramification divisor has degree 2. If  $\text{char}(K) \neq 2$  then the ramification is tame and so  $\gamma_\ell$  is ramified at precisely two distinct  $\bar{K}$ -points. If  $\text{char}(K) = 2$ , then the ramification is wild and  $\gamma_\ell$  is ramified at precisely one point. Parts (i) and (ii) now follow as the parabolic points on  $\ell$  are the ramification points of  $\gamma_\ell$ , and as the Eckardt points are contained among the parabolic points.

Finally suppose that  $\text{char}(K) = 2$  and  $\gamma_\ell$  is inseparable. Then  $\gamma_\ell$  is ramified at every point of  $\ell$  and so every point is parabolic. To complete the proof of (iii) we must show that there are 5 Eckardt points on  $\ell$ . By Theorem 4 there are 10 lines on  $S$  that meet  $\ell$ . Let  $\ell'$  be one of these and let  $P$  be their point of intersection. Then  $\ell$  and  $\ell'$  are distinct asymptotic lines to  $S$  at  $P$ . The only way that  $P$  can be parabolic is if there is a third line passing through  $P$ . Thus there are 5 Eckardt points  $\ell$  proving (iii).  $\square$

**Example.** Many of the classical notions about cubic surfaces over  $\mathbb{C}$  break down for cubic surfaces over a field of characteristic 2. For example, a cubic surface over  $\mathbb{C}$  has 1, 2, 3, 4, 6, 9, 10 or 18 Eckardt points [20, Section 100] and any line contains at most two Eckardt points. The following example shows that this need not be the case in characteristic 2. Take  $S$  to be the smooth cubic surface over  $\mathbb{F}_2$  given by

$$S: x_0^2x_2 + x_0^2x_3 + x_0x_1^2 + x_0x_1x_2 + x_0x_3^2 + x_1^2x_2 + x_1x_2^2.$$

The 27 lines are rational over  $\mathbb{F}_{64}$ , and  $S$  has 13 Eckardt points. Three of the 27 lines have 5 Eckardt points and the remaining all have exactly one.

### 3. Proof of Theorem 1

Throughout this section we shall assume that  $\#K \geq 13$ .

**Lemma 3.1.** *Let  $\ell$  be a  $K$ -line on  $S$ . Let  $P \in \ell(K)$  be a point that does not lie on any other line belonging to  $S$ . Then*

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \text{Span}(P).$$

**Proof.** By Lemma 2.1, we know  $\ell \subseteq \Gamma_P$ . Thus  $\Gamma_P = \ell \cup C$  where  $C$  is a conic contained in  $\Pi_P$ . Since  $P$  does not lie on any other line belonging to  $S$ , we know that  $C$  is irreducible over  $\bar{K}$ . Now  $P \in \ell \cap C$  since  $P$  is either parabolic or  $K$ -hyperbolic by Lemma 2.2. Thus  $\ell \cdot C = P + P'$  where  $P'$  is also  $K$ -rational.

Let  $Q \in C(K) \setminus \{P, P'\}$ . Let  $\ell'$  be the  $K$ -line joining  $P$  and  $Q$ . Then  $\ell' \cdot S = 2P + Q$  and so  $Q \in \text{Span}(P)$ . Hence  $C(K) \setminus \{P'\} \subseteq \text{Span}(P)$ .

Now let  $R \in \ell(K) \setminus \{P, P'\}$ . Let  $Q_1 \in C(K) \setminus \{P, P'\}$  and let  $\ell'$  be the  $K$ -line connecting  $R$  and  $Q_1$ . Then  $\ell' \cdot S = R + Q_1 + Q_2$  where  $Q_2 \in C(K) \setminus \{P, P'\}$ . By the above,  $Q_1, Q_2 \in \text{Span}(P)$ . Hence  $R \in \text{Span}(P)$ . This shows that  $\ell(K) \setminus \{P'\} \subseteq \text{Span}(P)$ .

Finally we must show that  $P' \in \text{Span}(P)$ . There is nothing to prove if  $P = P'$ . Thus suppose  $P \neq P'$ . Note that  $\Pi_P = \Pi_{P'}$ . By the proof of Lemma 2.2, the morphism  $\gamma_\ell$  that sends points on  $\ell$  to their tangent planes has degree 2, so for any  $R \in \ell \setminus \{P, P'\}$ ,  $P'$  will be a non-singular point of  $\Gamma_R$ . The line  $\ell$  meets precisely 10 other lines lying on  $S$  by Theorem 4. The assumption that  $\#K \geq 13$  forces the existence of  $R \in \ell(K)$ , different from  $P$  and  $P'$ , and not lying on any line. Using the above argument with  $R$  instead of  $P$  we see that  $P' \in \text{Span}(R)$ . However,  $R \in \text{Span}(P)$ . This completes the proof.  $\square$

We now relax the hypotheses of Lemma 3.1.

**Lemma 3.2.** *Let  $\ell$  be a  $K$ -line on  $S$ . Let  $P \in \ell(K)$  and suppose that  $P$  is not an Eckardt point. Then*

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \text{Span}(P).$$

**Proof.** To ease notation, we write  $\ell_1$  for the line  $\ell$ . If  $P$  does not lie on any other line then this follows from Lemma 3.1. Thus we may suppose that  $P \in \ell_2$  where  $\ell_1 \neq \ell_2$  but is not Eckardt. So  $\ell_1$  and  $\ell_2$  are distinct asymptotic lines at  $P$ , and so  $P$  is non-parabolic. By Lemma 2.2, the point  $P$  must be  $K$ -hyperbolic, and so  $\ell_2$  is defined over  $K$ . Now  $\Gamma_P = \ell_1 \cup \ell_2 \cup \ell_3$  where  $\ell_3 \subset S$  is a  $K$ -line not passing through  $P$ . Write  $P_{ij} = \ell_i \cdot \ell_j$ ; thus  $P_{12} = P$  and the points  $P_{ij}$  are distinct. Since the field is large enough, there is a point  $Q \in \ell_3(K)$  such that  $Q \neq P_{13}, P_{23}$ , and  $Q$  does not lie on any other line contained in  $S$ . By Lemma 3.1 we know that  $\ell_3(K) \subseteq \text{Span}(Q)$ . But if we let  $\ell_Q$  be the line joining  $Q$  with  $P_{12}$ , then  $\ell_Q \cdot S = 2P_{12} + Q$  and so  $Q \in \text{Span}(P_{12})$ . Thus  $\ell_3(K) \subseteq \text{Span}(P_{12})$ . Similarly  $\ell_1(K) \subseteq \text{Span}(P_{23})$  and  $\ell_2(K) \subseteq \text{Span}(P_{13})$ . However,  $P_{23}, P_{13} \in \ell_3(K)$ . It follows that  $\ell_i(K) \subseteq \text{Span}(P_{12})$  for  $i = 1, 2, 3$ . This completes the proof.  $\square$

**Lemma 3.3.** *Suppose  $S$  contains two skew  $K$ -lines  $\ell, \ell'$ . Then*

$$\ell'(K) \subset \text{Span}(\ell(K)).$$

**Proof.** As in Section 2, let  $\gamma_\ell$  be the map that sends a point  $P \in \ell$  to the tangent plane  $\Pi_P$  to  $S$  at  $P$ . We know by the proof of Lemma 2.2 that  $\gamma_\ell$  has degree 2. Since  $\ell \subset \Pi_P$  and  $\ell, \ell'$  are skew, we see that  $\ell' \cdot \Pi_P$  is a single point on  $\ell'$ . Thus we can think of  $\gamma_\ell$  as a map  $\ell \rightarrow \ell'$  given by  $P \mapsto \ell' \cdot \Pi_P$ .

We claim the existence of some  $P \in \ell(K)$  that is not Eckardt such that  $\gamma_\ell(P)$  is not Eckardt. Assume this for the moment. It is clear that  $\gamma_\ell(P) \in \Gamma_P(K)$ . By Lemma 3.2, we see that  $\gamma_\ell(P) \in \text{Span}(P)$  and  $\ell'(K) \subseteq \text{Span}(\gamma_\ell(P))$ . Thus to complete the proof it is enough to establish our claim.

By Lemma 2.2,  $\ell'$  contains at most 5 Eckardt points and so it is enough to show that

$$\#\gamma_\ell(\ell(K) \setminus \{\text{Eckardt points}\}) \geq 6.$$

Suppose first that  $\gamma_\ell$  is separable. The Eckardt points on  $\ell$  are at most 2 by Lemma 2.2. As  $\gamma_\ell$  has degree 2,

$$\#\gamma_\ell(\ell(K) \setminus \{\text{Eckardt points}\}) \geq \frac{\#\ell(K) - 2}{2} \geq 6.$$

Finally suppose  $\gamma_\ell$  is inseparable. Then  $\gamma_\ell : \ell(K) \rightarrow \ell'(K)$  is injective. Now there are 5 Eckardt points on  $\ell$  and

$$\#\gamma_\ell(\ell(K) \setminus \{\text{Eckardt points}\}) \geq \#\ell(K) - 5 \geq 9. \quad \square$$

I am grateful to Damiano Testa for pointing out to me that a cubic surface containing skew  $K$ -lines  $\ell, \ell'$  is birational to  $\ell \times \ell'$  over  $K$ . This in essence is what the proof of the following lemma is using.

**Lemma 3.4.** *Suppose  $S$  contains a pair of skew lines  $\ell_1$  and  $\ell_2$  both defined over  $K$ . Then*

$$\text{Span}(\ell_1(K) \cup \ell_2(K)) = S(K).$$

**Proof.** Let  $P$  be a  $K$ -point on  $S$  not belonging to either line; we will show that  $P$  belongs to the span of  $\ell_1(K) \cup \ell_2(K)$ . Let  $\Pi_1$  be the unique plane containing  $\ell_2$  and  $P$ , and  $\Pi_2$  the unique plane containing  $\ell_1$  and  $P$ . Since  $\ell_1$  and  $\ell_2$  are skew we know that  $\ell_i \not\subset \Pi_i$ . Write  $Q_i = \ell_i \cap \Pi_i$ . Note that  $P, Q_1$  and  $Q_2$  are distinct points on  $S$  that also belong to the  $K$ -line  $\ell = \Pi_1 \cap \Pi_2$ . Suppose first that  $\ell \not\subset S$ . Then  $\ell \cdot S = P + Q_1 + Q_2$ . Thus  $P \in \text{Span}(\ell_1(K) \cup \ell_2(K))$  as required.

Next suppose that  $\ell \subset S$ . Then  $\ell \subset \Gamma_{Q_1}$ . If  $Q_1$  is not Eckardt, then by Lemma 3.2,

$$P \in \ell(K) \subseteq \Gamma_{Q_1}(K) \subseteq \text{Span}(Q_1) \subseteq \text{Span}(\ell_1(K)).$$

Thus we may assume that  $Q_1$  is Eckardt. Then  $\Gamma_{Q_1} = \ell \cup \ell_1 \cup \ell_3$  where  $\ell_3$  is also  $K$ -rational. Now, as  $\ell_1$  and  $\ell_2$  are skew,  $\ell_2$  meets the plane  $\Pi_{Q_1}$  in precisely one point and this is  $Q_2$ . In particular,  $\ell_2$  and  $\ell_3$  are skew. Thus  $\ell_3(K) \subseteq \text{Span}(\ell_2(K))$  by Lemma 3.3. Now let  $Q \in \ell_1(K) \setminus \{Q_1\}$ . The line connecting  $Q$  and  $P$  meets  $\ell_3$  in a  $K$ -point  $R$ , and so

$$P \in \text{Span}(\ell_1(K) \cup \ell_3(K)) \subseteq \text{Span}(\ell_1(K) \cup \ell_2(K)). \quad \square$$

**Proof of Theorem 1.** This follows from Lemmas 3.2, 3.3 and 3.4.  $\square$

#### 4. Preliminaries on $H_5(K)$

We now begin our study of the group  $H_5(K)$ . Our eventual aim is to prove Theorems 2 and 3, but we will see other reasons why  $H_5(K)$  is a worthwhile object of study.

**Lemma 4.1.** *Let  $C \subset S$  be either a  $K$ -line, a smooth plane conic defined over  $K$ , or an irreducible plane cuspidal or nodal cubic defined over  $K$ . Suppose  $P, Q \in S(K)$  are points lying on  $C$ . Moreover, in the cuspidal or nodal cubic case, suppose that  $P, Q$  are non-singular points on  $C$ . Then  $[P - Q] = 0$  in  $H_5(K)$ .*

**Proof.** Suppose first that  $C = \ell$  is a  $K$ -line lying on  $S$  and  $P, Q$  are  $K$ -points lying on  $\ell$ . By definition of  $G'_5(K)$ , we see that  $3P, 2P + Q \in G'_5(K)$ . Thus  $[P - Q] = [3P - (2P + Q)]$  is zero in  $H_5(K)$ .

Next suppose that  $C \subset S$  is a smooth plane conic defined over  $K$ , and let  $\Pi$  be the plane containing  $C$ . Then  $S \cap \Pi = C \cup \ell$  where  $\ell$  is a  $K$ -line. Let  $P, Q$  be  $K$ -points on  $C$ . The line joining  $P$  and  $Q$  meets  $\ell$  in a  $K$ -point  $P'$ . Likewise, the tangent to  $C$  at  $Q$  meets  $\ell$  in a  $K$ -point  $Q'$ . Thus  $P + Q + P', 2Q + Q' \in G'_5(K)$ . Hence

$$[P - Q] = [(P + Q + P') - (2Q + Q')] + [Q' - P'] = [Q' - P'].$$

But by the previous part,  $[Q'] = [P']$  as both points are on  $\ell \subset S$ . Hence  $[P - Q] = 0$ .

Finally, suppose  $C \subset S$  is a cuspidal or nodal plane cubic defined over  $K$ , and let  $R \in S(K)$  be the singular point on  $C$ . Let  $P, Q \in S(K)$  be non-singular points on  $C$ . By considering the lines joining  $P$  with  $R$  and  $Q$  with  $R$ , we see that  $P + 2R, Q + 2R \in G'_5(K)$ . Then  $[P - Q] = 0$ .  $\square$

The reader will recall that whilst any rational point on a cubic curve can be taken as the zero element, the description of the group law is simpler and more pleasant if this point is a flex. We shall now introduce a cubic surface analogue of flexes. Let  $P \in S(K)$ . We shall say that  $P$  is  $K$ -ternary if at least one of the asymptotic lines to  $S$  through  $P$  is defined over  $K$ .



**Lemma 4.2.** *If  $P$  is  $K$ -hyperbolic then  $P$  is  $K$ -ternary. If  $P$  is Eckardt then  $P$  is  $K$ -ternary. If  $P$  is parabolic and  $\text{char}(K) \neq 2$  then  $P$  is  $K$ -ternary.*

**Proof.** The first part follows from the definition of  $K$ -hyperbolic.

Suppose  $P$  is Eckardt. Of course each of the three lines through  $P$  contained in  $S$  is an asymptotic line. So we may suppose that none of these is  $K$ -rational. Now let  $\ell$  be any  $K$ -line in  $\Pi_P$  through  $P$ . Then  $(\ell \cdot S)_P = 3$  and  $\ell$  is an asymptotic  $K$ -line as required.

Finally, suppose  $P$  is parabolic and  $\text{char}(K) \neq 2$ . We may suppose that  $P$  is non-Eckardt. Then  $S$  has a unique asymptotic line  $\ell$  through  $P$ . The asymptotic lines are obtained by solving a quadratic equation, and as there is exactly one solution and  $\text{char}(K) \neq 2$  the solution must be  $K$ -rational.  $\square$

**Theorem 5.** *Suppose  $P_0 \in S(K)$  is  $K$ -ternary. Let  $B \subseteq S(K)$  such that  $\text{Span}(B) = S(K)$ . Then the set  $\{[P - P_0] : P \in B\}$  generates  $H_S^0(K)$ . In particular, for any prime  $p$ ,*

$$r(S, K) \geq \dim_{\mathbb{F}_p} H_S^0(K)/pH_S^0(K).$$

**Proof.** Note that if  $\ell$  is a  $K$ -rational line and  $\ell \cdot S = P + Q + R$  with  $P, Q, R \in S(K)$  then  $P + Q + R$  and  $3P_0$  both belong to  $G'_S(K)$  and so  $[P - P_0] + [Q - P_0] + [R - P_0] = 0$ . The first part of the lemma follows easily from this and the fact that  $H_S^0(K)$  is generated by elements of the form  $[P - P_0]$  with  $P \in S(K)$ .

For the second part, note that any set which generates  $H_S^0(K)$  also generates the  $\mathbb{F}_p$ -vector space  $H_S^0(K)/pH_S^0(K)$ .  $\square$

**Theorem 6.** *Suppose  $S$  contains a  $K$ -rational line  $\ell$ . Then  $H_S^0(K) = H_S(K)[2]$ , where  $H_S(K)[2]$  is the 2-torsion subgroup of  $H_S(K)$ .*

**Proof.** Let  $Q$  be a  $K$ -rational point on  $\ell$ . We claim that  $2P + Q \in G'_K$  for all  $P \in S(K)$ . Assume our claim for a moment. Now  $H_S^0(K)$  is generated by classes  $[P' - P]$  with  $P, P' \in S(K)$ . By our claim,  $2(P' - P) = (2P' + Q) - (2P + Q)$  is an element of degree 0 in  $G'_S(K)$ , proving the theorem.

To prove our claim let  $P \in S(K)$ . If  $P \in \ell$  then  $2P + Q \in G'_S(K)$  by definition of  $G'_S(K)$ . Thus suppose  $P \notin \ell$  and let  $\Pi_P$  be the tangent plane to  $S$  at  $P$ . Now either  $\Pi_P$  contains  $\ell$  or it meets  $\ell$  in precisely one  $K$ -rational point. In either case, there is some  $K$ -rational point  $Q' \in \Pi_P \cap \ell$ . Since  $P$  is not on  $\ell$ , we have  $P \neq Q'$ . Let  $\ell'$  be the unique  $K$ -line connecting  $P$  and  $Q'$ . Now  $\Gamma_P = \Pi_P \cap S$  is singular at  $P$ . Thus  $\ell'$  is tangent to  $S$  at  $P$ , and hence  $2P + Q' \in G'_S(K)$ . However  $Q - Q' \in G'_S(K)$  by Lemma 4.1. This proves the claim.  $\square$

The proof of the following theorem is in essence a simplification of the proof of Lemma 3.4.

**Theorem 7.** *Suppose  $S$  contains a pair of skew  $K$ -lines. Then  $H_S^0(K) = 0$ .*

**Proof.** This can in fact be easily recovered from Theorem 1 if  $\#K \geq 13$ . In any case, let  $\ell_1$  and  $\ell_2$  be a pair of skew  $K$ -lines contained in  $S$ . Fix some  $Q_i \in \ell_i(K)$ . We claim that  $P + Q_1 + Q_2 \in G'_S(K)$  for every  $P \in S(K)$ . Let us assume this for the moment. By the proof of Theorem 6, we know that  $2P + Q_2 \in G'_S(K)$ . Hence  $P - Q_1 \in G''_K$ ; in other words  $P - Q_1 \equiv 0$  in  $H_S^0(K)$ . Since classes of the form  $[P - Q_1]$  generate  $H_S^0(K)$ , we see that  $H_S^0(K) = 0$ .

It remains to prove our claim. Note, by Lemma 4.1, any two points on  $\ell_i$  are equivalent. Moreover, if  $P \in \ell_1(K)$  then all we have to show is that  $2Q_1 + Q_2 \in G'_S(K)$  which is true from the proof of Theorem 6. Thus we may suppose that  $P \notin \ell_i, i = 1, 2$ . Let  $\Pi_1$  be the unique plane containing  $\ell_2$  and  $P$ , and  $\Pi_2$  the unique plane containing  $\ell_1$  and  $P$ . Since  $\ell_1$  and  $\ell_2$  are skew we know that  $\ell_i \not\subset \Pi_j$ . Write  $Q_i = \ell_i \cap \Pi_j$ . Note that  $P, Q_1$  and  $Q_2$  are distinct points on  $S$  that also belong to the  $K$ -line  $\Pi_1 \cap \Pi_2$ . By the definition of  $G'_S(K)$  we have  $P + Q_1 + Q_2 \in G'_S(K)$ .  $\square$

**Corollary 4.3.** *Let  $K$  be algebraically closed. Then  $H_S^0(K) = 0$ .*

**5.  $H_S(K)$  for local fields  $K$**

In this section we let  $K$  be a local field. This means that  $K = \mathbb{R}$  or  $\mathbb{C}$ , or that  $K$  is a finite extension of  $\mathbb{Q}_p$  for some prime  $p$ . The purpose of this section is to prove the following theorem.

**Theorem 8.** *Let  $K$  be a local field and let  $S$  be a smooth cubic surface over  $K$ . Then the following hold.*

- (i) *The group  $H_S^0(K)$  is finite.*
- (ii) *The natural map  $S(K) \rightarrow H_S(K)$  given by  $P \mapsto [P]$  is locally constant, where  $S(K)$  has the topology induced by  $K$ .*

Of course, if  $S(K)$  is empty there is nothing to prove, so we shall suppose  $S(K) \neq \emptyset$ . Then  $S(K)$  is a 2-dimensional  $K$ -manifold, and in particular has  $K$ -points not lying on the 27 lines. Such a  $K$ -point is called a *general point*.

The proof of Theorem 8 requires a series of lemmas. The key lemma is the following.

**Lemma 5.1.** *There exists some non-empty  $W \subset S(K)$ , open in the topology induced by  $K$ , such that for all  $P_1, P_2 \in W$  we have  $[P_1] = [P_2]$  in  $H_S(K)$ .*

**Proof.** It is well known that the existence of a general  $K$ -point makes  $S$  unirational, and makes the set  $S(K)$  dense in the Zariski topology. One proof of this is found in Manin’s book [15, Chapter II, Theorem 12.11]. Our lemma follows from a modification, given below, of Manin’s proof.

Let  $R$  be a general  $K$ -point on  $S$ . Observe that the plane cubic curve  $\Gamma_R$  is irreducible, defined over  $K$  and singular only at  $R$ . Let  $\mathcal{T}_S$  be the projectivized tangent bundle of  $S$ . In other words,  $\mathcal{T}_S$  parametrizes pairs  $(Q, \ell)$  where  $Q$  is a point on  $S$  and  $\ell$  is a line tangent to  $S$  at  $Q$ . As the bundle  $\mathcal{T}_S$  is locally trivial, there is a Zariski open subset  $U \subset S$  containing  $R$  and a local isomorphism  $U \times \mathbb{P}^1 \rightarrow \mathcal{T}_S$  defined over  $K$ . Remove from  $U$  the 27 lines on  $S$ . Then the local isomorphism induces a morphism  $\phi : U \times \mathbb{P}^1 \rightarrow S$  defined over  $K$  as follows: if  $Q \in U$ ,  $\alpha \in \mathbb{P}^1$  and  $\ell_\alpha$  is the line tangent to  $S$  at  $Q$  corresponding to  $\alpha$  then let  $\phi(Q, \alpha)$  be the third point of intersection of  $\ell$  with  $S$ . Consider the restriction of  $\phi$  to  $(\Gamma_R \cap U) \times \mathbb{P}^1$ . The image must be irreducible and contains  $\Gamma_Q$  for all  $Q \in \Gamma_R \cap U$  (including  $\Gamma_R$ ). If the image is 1-dimensional then  $\Gamma_Q = \Gamma_R$  which is impossible for  $Q \neq R$  since  $Q$  is non-singular in  $\Gamma_R$  but singular in  $\Gamma_Q$ . This shows that  $(\Gamma_R \cap U) \times \mathbb{P}^1 \rightarrow S$  is dominant.

Let  $V$  be a non-empty subset of  $\Gamma_R(K) \cap U(K)$ , open in the topology induced by  $K$ , such that  $R \notin V$ . Then  $\phi(V \times \mathbb{P}^1(K))$  contains a non-empty subset  $W$  open in  $S(K)$ . To complete the proof it is enough to show that the map  $P \mapsto [P]$  is constant on  $\phi(V \times \mathbb{P}^1(K))$ . Suppose  $P_1, P_2$  are in this set. So  $P_i + 2Q_i = \ell_i \cdot S$  for some  $K$ -lines  $\ell_1, \ell_2$  and for some  $Q_1, Q_2 \in V$ . Now  $Q_1, Q_2 \in \Gamma_R$ , but neither is equal to  $R$ . Thus  $[Q_1] = [Q_2]$  by Lemma 4.1. It follows that  $[P_1] = [P_2]$  as desired.  $\square$

**Lemma 5.2.** *The map  $S(K) \rightarrow H_S(K)$  given by  $P \mapsto [P]$  is locally constant.*

**Proof.** By Lemma 5.1, there is some non-empty open  $W \subset S(K)$  on which the map  $P \mapsto [P]$  is constant. We shall prove the lemma by using secant operations to cover  $S(K)$  by ‘translates’ of  $W$ .

Let  $P_0 \in S(K) \setminus W$ . Choose  $Q_0 \in W$  such that the  $K$ -line  $\ell$  joining  $Q_0$  and  $P_0$  is not contained in  $S$  and is not tangent to  $S$  at either point. Write  $R$  for the  $K$ -point such that  $\ell \cdot S = R + Q_0 + P_0$ . Consider the rational map

$$t_R : S \dashrightarrow S, \quad P \mapsto Q \quad \text{if } P, Q \text{ and } R \text{ are collinear.}$$

Clearly  $t_R$  restricts to a local homeomorphism of neighbourhoods of  $P_0$  and  $Q_0$ . Thus there is some open  $V$  containing  $P_0$ , contained in the domain of this local homeomorphism, such that  $t_R(V) \subset W$ .

Now let  $P \in V$ . Then  $Q_0 + P_0 + R \in G'_S(K)$  and  $t_R(P) + P + R \in G'_S(K)$ . Thus  $[Q_0 - t_R(P)] + [P_0 - P] = 0$ . But  $[t_R(P)] = [Q_0]$  as both  $t_R(P)$  and  $Q_0$  are in  $W$ . Thus  $[P] = [P_0]$ . Hence  $P \mapsto [P]$  is constant on the open neighbourhood  $V$  of  $P_0$ .  $\square$

**Proof of Theorem 8.** By Lemma 5.2 there is a covering of  $S(K)$  by open sets  $U$  such that the function  $P \mapsto [P]$  is constant when restricted to  $U$ . As  $S(K)$  is compact, we can assume that we have finitely many such  $U$ , say  $U_1, \dots, U_m$ . Fix  $P_i \in U_i$  for  $i = 1, \dots, m$ . The abelian group  $H^0_S(K)$  is then generated by the differences  $[P_i - P_j]$ .

It will be sufficient to show that for any two points  $P, Q \in S(K)$  the class  $[P - Q]$  has finite order. Let  $\ell$  be the  $K$ -line joining  $P$  and  $Q$ . If  $\ell \subset S$  then  $[P - Q] = 0$  by Lemma 4.1, so suppose that  $\ell \not\subset S$ . Let  $\Pi$  be a  $K$ -plane through  $\ell$  that misses all the lines on  $S$  and such that the irreducible plane cubic  $E = S \cap \Pi$  is non-singular at  $P$  and  $Q$ .

If  $E$  is singular, then  $[P - Q] = 0$  by Lemma 4.1. Thus we may suppose that  $E$  is non-singular. Consider the elliptic curve  $(E, Q)$ . For an integer  $n$ , there is a unique  $R_n \in E(K)$  such that  $n(P - Q) \sim R_n - Q$ , where  $\sim$  denotes linear equivalence on  $E$ . Now the group operations on  $(E, Q)$  are given by secants and tangents, so we know that  $n[P - Q] = [R_n - Q]$ . However, from the properties of elliptic curves over local fields, we may choose values  $n \neq 0$  so that  $R_n$  is arbitrarily close to  $Q$ . But we already know that if  $R_n$  is sufficiently close to  $Q$  then  $[R_n] = [Q]$ . This completes the proof.  $\square$

**6.  $H_5(\mathbb{R})$**

Let  $S$  be a smooth cubic surface defined over  $\mathbb{R}$ . We quickly summarize some well-known facts; for details see [17,24]. The cubic surface  $S$  contains 3, 7, 15 or 27 real lines, and  $S(\mathbb{R})$  has either one or two connected components. If  $S(\mathbb{R})$  has one connected component then this component is non-convex. If  $S(\mathbb{R})$  has two connected components then one is convex and the other non-convex. The non-convex component contains all the real lines.

**Theorem 9.** *If  $S(\mathbb{R})$  consists of one connected component then  $H^0_S(\mathbb{R}) = 0$ . If  $S(\mathbb{R})$  consists of two connected components then  $H^0_S(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ . This isomorphism may be given explicitly as follows. Let  $P_0$  be a point on the non-convex component. The map*

$$[P - P_0] \mapsto \begin{cases} \bar{0} & \text{if } P \text{ is in the non-convex component,} \\ \bar{1} & \text{if } P \text{ is in the convex component} \end{cases}$$

*extends to an isomorphism  $H^0_S(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ .*

**Proof.** By Theorem 8, the map  $P \mapsto [P]$  is locally constant, and hence constant on each connected component. Now  $H^0_S(\mathbb{R})$  is generated by classes of differences  $[P - Q]$ , and so if there is only one component then  $H^0_S(\mathbb{R}) = 0$ .

Now suppose  $S(\mathbb{R})$  has two components. To see that the map given in the theorem extends to an isomorphism  $H^0_S(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ , it is enough to observe that if  $P, Q, R$  are collinear real points on  $S$ , then either all three are on the non-convex component, or precisely one is on the non-convex component.  $\square$

**Remark.** I am grateful to the referee for the following remark. By a result of Colliot-Thélène and Ischebeck [4], the degree 0 part of  $\text{CH}_0(S/\mathbb{R})$  is isomorphic  $(\mathbb{Z}/2\mathbb{Z})^{s-1}$ , where  $s$  is the number of real components. It follows from this and Theorem 9 that the natural map  $H_5(\mathbb{R}) \rightarrow \text{CH}_0(S/\mathbb{R})$  is an isomorphism.

**7. Weak approximation and  $H_5$**

In this section  $K$  denotes a number field and  $\Omega$  the set of places of  $K$ . Denote the adèles of  $K$  by  $\mathbb{A}_K$ . As usual,  $S$  is a smooth cubic surface over  $K$ , but we shall further suppose that  $S(\mathbb{A}_K) \neq \emptyset$ .

We say  $S$  satisfies *weak approximation* if the image of  $S(K)$  in  $S(\mathbb{A}_K)$  is dense. More generally, let  $\Sigma$  be a finite subset of  $\Omega$ , and denote by  $\mathbb{A}_K^\Sigma$  the adèles of  $K$  with the  $\Sigma$ -components removed. We say that  $S$  satisfies *weak approximation away from  $\Sigma$*  if the image of  $S(K)$  in  $S(\mathbb{A}_K^\Sigma)$  is dense. If we assume Colliot-Thélène’s Conjecture 1.1, then it is easy in any given case to write down a finite set of places  $\Sigma$  such that  $S$  satisfies weak approximation away from  $\Sigma$ . We shall not do this in general, but only for the surfaces  $S_M$  and  $S'_M$  in Theorems 2 and 3.

**Theorem 10.** *Let  $K$  be a number field and  $\Omega$  its places. Let  $\Sigma$  be a subset of  $\Omega$  and let  $\mathbb{A}_K^\Sigma$  denote the adèles of  $K$  with the  $\Sigma$  components removed. Suppose that the image of  $S(K)$  in  $S(\mathbb{A}_K^\Sigma)$  is dense. Let  $\Delta$  be a finite subset of  $\Omega \setminus \Sigma$ . Then the diagonal map*

$$H_S^0(K) \rightarrow \prod_{v \in \Delta} H_S^0(K_v) \tag{4}$$

is surjective.

**Proof.** The target space of the homomorphism in (4) is generated by elements of the form  $([P_v - Q_v])_{v \in \Delta}$ , thus it is enough to show that such elements are in the image. By the hypotheses,  $S(K)$  is dense in  $\prod_{v \in \Delta} S(K_v)$ . Recall, from Theorem 8, that the maps  $R \rightarrow [R]$  are locally constant on the  $S(K_v)$ . Thus choosing  $P, Q \in S(K)$  that sufficiently approximate  $(P_v)_{v \in \Delta}$  and  $(Q_v)_{v \in \Delta}$  will give an element  $[P - Q] \in H_S^0(K)$  whose image under (4) is  $([P_v - Q_v])_{v \in \Delta}$ .  $\square$

At first sight it seems that this theorem enables us to disprove the Mordell–Weil Conjecture for cubic surfaces simply by taking the set  $\Delta$  to be arbitrarily large and forcing  $H_S^0(K)$  to surject onto larger and larger groups. However, extensive—though not systematic—experimentation with cubic surfaces, which we do not describe here, suggests that  $H_S^0(K_v) = 0$  if  $v$  is a non-Archimedean place of good reduction for  $S$  and  $v \nmid 2$ . By a place of good reduction we mean a non-Archimedean place  $v$  such that the polynomial defining  $S$  has  $v$ -integral coefficients, and the reduction of that polynomial modulo  $v$  defines a smooth cubic surface over the residue field. We remark that for any place  $v$  of good reduction for  $S$ , it is known (e.g. [3, Theorem A]) that the degree 0 part of the Chow group vanishes for  $S \times K_v$ .

We shall use Theorem 10 to prove Theorems 2 and 3. The first step is to prove weak approximation for the surfaces  $S_M/\mathbb{Q}$  in Theorem 2 and weak approximation away from {3} for the surfaces  $S'_M/\mathbb{Q}$  in Theorem 3; in the latter case our result will be conditional on Colliot-Thélène’s Conjecture 1.1. To prove weak approximation we introduce the Brauer–Manin obstruction and study it for the surfaces  $S_M$  and  $S'_M$ .

**8. Brauer–Manin obstruction: a brief overview**

To proceed further we need to recall some facts about the Brauer–Manin obstruction; for fuller details see [22, Section 5.2]. We continue with the notation of the previous section:  $K$  is a number field,  $\mathbb{A}_K$  the adèles of  $K$  and  $\Omega$  the set of places of  $K$ . The *Hasse reciprocity law* states that the following sequence of abelian groups is exact:

$$0 \rightarrow \text{Br}(K) \rightarrow \sum_{v \in \Omega} \text{Br}(K_v) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

Here the third map is the sum of local invariants  $\text{inv}_v : \text{Br}(K_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ . Let  $X$  be a smooth, projective and geometrically integral variety over a number field  $K$ . Let  $\text{Br}(X)$  be the Brauer group of  $X$  and denote by  $\text{Br}_0(X)$  the image of  $\text{Br}(K)$  in  $\text{Br}(X)$ . Consider the pairing

$$(\cdot, \cdot) : \text{Br}(X) \times X(\mathbb{A}_K) \rightarrow \mathbb{Q}/\mathbb{Z}, \quad (A, (P_v)) = \sum_{v \in \Omega} \text{inv}_v(A(P_v)).$$

This is the *adelic Brauer–Manin pairing* and satisfies the following properties.

- (i) If  $A \in \text{Br}_0(X) \subset \text{Br}(X)$  and  $(P_v) \in X(\mathbb{A}_K)$  then  $\langle A, (P_v) \rangle = 0$ .
- (ii) If  $P \in X(K)$  then  $\langle A, P \rangle = 0$  for every  $A \in \text{Br}(X)$ .
- (ii) For any  $A \in \text{Br}(X)$ , the map

$$X(\mathbb{A}_K) \rightarrow \mathbb{Q}/\mathbb{Z}, \quad (P_v) \mapsto \langle A, (P_v) \rangle$$

is continuous where  $\mathbb{Q}/\mathbb{Z}$  is given the discrete topology.

We define

$$X(\mathbb{A}_K)^{\text{Br}(X)} = \{(P_v) \in X(\mathbb{A}_K) : \langle A, (P_v) \rangle = 0 \text{ for all } A \in \text{Br}(X) / \text{Br}_0(X)\}.$$

By the above we know that

$$\overline{X(K)} \subseteq X(\mathbb{A}_K)^{\text{Br}(X)},$$

where  $\overline{X(K)}$  is the closure of  $X(K)$ . We say that the *Brauer–Manin obstruction is the only obstruction to weak approximation* if  $\overline{X(K)} = X(\mathbb{A}_K)^{\text{Br}(X)}$ .

### 9. The Brauer–Manin obstruction for $S_M$

In this section we prove the following proposition.

**Proposition 9.1.** *Let  $p_1, \dots, p_s$  ( $s \geq 1$ ) and  $M$  be as in Theorem 2. Let  $S = S_M/\mathbb{Q}$  be the cubic surface given by (1). Then  $S$  satisfies weak approximation. In particular, the homomorphism*

$$H_S^0(\mathbb{Q}) \rightarrow \prod_{p=p_1}^{p=p_s} H_S^0(\mathbb{Q}_p)$$

is surjective.

To prove this proposition we shall need a theorem of Salberger and Skorobogatov on del Pezzo surfaces of degree 4. The cubic surface  $S_M$  is birational to a degree 4 del Pezzo  $X$  given by the following smooth intersection of two quadrics in  $\mathbb{P}^4$ :

$$X_M: \begin{cases} x^2 - xy + y^2 + zt = 0, \\ z^2 + Mw^2 - xt - yt = 0. \end{cases}$$

The map  $X_M \dashrightarrow S_M$  is the obvious one  $(x, y, z, w, t) \mapsto (x, y, z, w)$ .

**Lemma 9.2.**  $\text{Br}(X_M) / \text{Br}_0(X_M)$  is trivial.

**Proof.** To determine  $\text{Br}(X_M) / \text{Br}_0(X_M)$  we can use the recipe in [23] or the more detailed recipe in [1]. The first step is to write down the 16 lines on  $X_M$ . We did this by writing down and solving the equations for the corresponding 0-dimensional Fano scheme (see for example [8, Section IV.3]). Write  $\theta = \sqrt[3]{2}$  and let  $\zeta$  be a primitive cube root of unity. There are two Galois orbits of lines. The first orbit has four lines and a representative is

$$L_1: \begin{cases} x + \zeta y = 0, \\ z + \sqrt{-M}w = 0, \\ t = 0. \end{cases}$$

The second orbit has 12 lines and a representative is

$$L_2: \begin{cases} -\theta z + \theta\sqrt{-M}w + t = 0, \\ 3\theta^2x + (2\zeta - 2)\theta z + (\zeta + 2)t = 0, \\ 3\theta^2y + (-2\zeta - 4)\theta z + (-\zeta + 1)t = 0. \end{cases}$$

From the size of these orbits we know [1, Proposition 13] that  $\text{Br}(X_M)/\text{Br}_0(X_M)$  is trivial.  $\square$

We shall also need the following theorem.

**Theorem.** (See Salberger and Skorobogatov [18, Theorem 6.5].) *Let  $K$  be a number field and  $X$  a del Pezzo surface of degree 4 over  $K$  containing a rational point. Then  $X(K)$  is dense in  $X(\mathbb{A}_K)^{\text{Br}(X)}$ .*

**Proof of Proposition 9.1.** By the above theorem of Salberger and Skorobogatov we know that  $X_M$  satisfies weak approximation. Now  $S_M$  is birational to  $X_M$ , and so by [18, Lemma 5.5(c)] also satisfies weak approximation. The last part of the proposition follows from Theorem 10.  $\square$

### 10. The Brauer–Manin obstruction for $S'_M$

In this section we prove the following proposition.

**Proposition 10.1.** *Let  $p_1, \dots, p_s$  and  $M$  be as in Theorem 3. Let  $\Sigma = \{3\}$ . Let  $S = S'_M/\mathbb{Q}$  be the cubic surface in (2) and suppose that the Brauer–Manin obstruction is the only obstruction to weak approximation on  $S$ . Then  $S$  satisfies weak approximation away from  $\{3\}$ . In particular, the homomorphism*

$$H^0_S(\mathbb{Q}) \rightarrow \prod_{p=p_1}^{p=p_s} H^0_S(\mathbb{Q}_p)$$

is surjective.

**Proof.** All the results we need for this proof are due to Colliot-Thélène, Kanevsky and Sansuc [5], though Jahnke’s Habilitation summarizes these results in one convenient theorem [11, Chapter III, Theorem 6.4]. Indeed, we know that:

- (i)  $\text{Br}(S)/\text{Br}_0(S) \cong \mathbb{Z}/3\mathbb{Z}$ . Fix  $A \in \text{Br}(S)$  that represents a non-trivial coset of  $\text{Br}(S)/\text{Br}_0(S)$ .
- (ii) The image of

$$\langle \cdot, \cdot \rangle : \text{Br}(S) \times S(\mathbb{A}_{\mathbb{Q}}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

is  $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$ .

- (iii) The map

$$S(\mathbb{Q}_p) \rightarrow \frac{1}{3}\mathbb{Z}/\mathbb{Z}, \quad P \mapsto \text{inv}_p(A, P)$$

is surjective for all  $p \mid M$ .

Now the strategy is clear. Suppose that  $\mathcal{P} = (P_\nu) \in S(\mathbb{A}_{\mathbb{Q}}^S)$ . Choose  $P_3 \in S(\mathbb{Q}_3)$  such that

$$\text{inv}_3(A, P_3) = - \sum_{\nu \neq 3} \text{inv}_\nu(A, P_\nu).$$

Let  $\mathcal{P}' \in S(\mathbb{A}_{\mathbb{Q}})$  be the point obtained from  $\mathcal{P}$  by taking  $P_3$  to be the component at 3. Then  $\langle A, \mathcal{P}' \rangle = 0$ . Since  $A$  generates  $\text{Br}(S)/\text{Br}_0(S)$  we know that  $\mathcal{P}' \in S(\mathbb{A}_{\mathbb{Q}})^{\text{Br}(S)}$ . By our assumption that the Brauer–Manin obstruction is the only one to weak approximation we have that  $\mathcal{P}'$  is in the closure of the rational points in  $S(\mathbb{A}_{\mathbb{Q}})$ . The proposition follows.  $\square$

### 11. A plane cubic

We shall need to study the reduction of the cubic surfaces (1) and (2) at the primes  $p \mid M$ . We note that modulo  $p$  they both reduce to cones over the plane cubic curve  $x^3 + y^3 + z^3 = 0$ . In this section we collect some information we need regarding the Picard group of this cubic curve.

In this section  $K$  is a field of characteristic  $\neq 3$ . Throughout the rest of the paper,  $C/\mathbb{Q}$  will denote the plane genus 1 curve given by (3). Note that with the restriction imposed on the characteristic,  $C \times K$  is smooth. Let  $\mathcal{O} = (1 : -1 : 0) \in C$ . We note that  $\mathcal{O}$  is a flex and so  $C$  can be put into Weierstrass form by a projective transformation that sends  $\mathcal{O}$  to the point at  $\infty$  (see for example [13, Proposition 2.14]). It follows for  $P, Q, R \in C(K)$  that  $P + Q + R - 3\mathcal{O} = 0$  in  $\text{Pic}^0(C \times K)$  if and only if there is  $K$ -line  $\ell$  in  $\mathbb{P}^2$  such that  $\ell \cdot C = P + Q + R$ .

**Lemma 11.1.** *Let  $p \equiv 1 \pmod{3}$  be a prime and write  $C_p$  for  $C \times \mathbb{F}_p$ . Then*

$$\dim_{\mathbb{F}_3} \text{Pic}^0(C_p)/3 \text{Pic}^0(C_p) = 2.$$

Moreover, each of the 9 elements of  $\text{Pic}^0(C_p)/3 \text{Pic}^0(C_p)$  can be represented by the class of  $P - \mathcal{O}$  for some  $P \in C(\mathbb{F}_p)$ .

**Proof.**  $\text{Pic}^0(C_p)$  is a finite abelian group isomorphic to  $E(\mathbb{F}_p)$  where  $E$  is the elliptic curve  $(C, \mathcal{O})$ . Hence we have isomorphisms

$$\text{Pic}^0(C_p)/3 \text{Pic}^0(C_p) \cong \text{Pic}^0(C_p)[3] \cong E(\mathbb{F}_p)[3],$$

the first of which is of course non-canonical. The assumption that  $p \equiv 1 \pmod{3}$  ensures that the nine flex points of  $C$  are defined over  $\mathbb{F}_p$ ; these have the form  $(1 : -\omega : 0)$  and permutations of these coordinates, where  $\omega^3 = 1$ . Now the 3-torsion in  $\text{Pic}^0(C_p)$  consists of the nine classes  $[\mathcal{O}' - \mathcal{O}]$  where  $\mathcal{O}'$  is a flex point. Hence

$$\text{Pic}^0(C_p)/3 \text{Pic}^0(C_p) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

This proves the first part of the lemma. The second part of the lemma follows since every element of  $\text{Pic}^0(C_p)$  is the class of  $P - \mathcal{O}$  for some  $P \in C(\mathbb{F}_p)$ .  $\square$

**Lemma 11.2.** *Let  $p \equiv 1 \pmod{3}$  be a prime such that 2 is a cube modulo  $p$ . Then*

$$\dim_{\mathbb{F}_2} \text{Pic}^0(C_p)/2 \text{Pic}^0(C_p) = 2.$$

Moreover, each of the 4 elements of  $\text{Pic}^0(C_p)/2 \text{Pic}^0(C_p)$  can be represented by the class of  $P - \mathcal{O}$  for some  $P \in C(\mathbb{F}_p)$ .

**Proof.** We can put  $E = (C, \mathcal{O})$  in Weierstrass form by sending  $\mathcal{O}$  to the point at infinity. A Weierstrass model is

$$y^2 + y = x^3 - 7.$$

The 2-division polynomial of this model is  $4x^3 - 27$ . The assumptions on  $p$  ensure that the 2-division polynomial splits completely over  $\mathbb{F}_p$ ; thus  $E$  has full 2-torsion over  $\mathbb{F}_p$ .  $\square$

**12. Reduction of lines**

In what follows we would like to conveniently parametrize a  $\mathbb{Q}_p$ -line  $\ell$  in  $\mathbb{P}^3$ . Of course if  $P$  and  $Q$  are two distinct points on  $\ell$  then  $\ell(\mathbb{Q}_p) = \{sP + tQ : (s : t) \in \mathbb{P}^1(\mathbb{Q}_p)\}$ . Now if  $S$  is a cubic surface given by  $F = 0$  then the points of  $\ell \cdot S$  correspond to the roots of  $F(sP + tQ)$  with the correct multiplicity. The problem with such a parametrization is that it is possible that  $\bar{P} = \bar{Q}$  and so we do not obtain a parametrization of  $\bar{\ell}$  by reducing the parametrization of  $\ell$ . In this brief section we indicate how to make a good choice of parametrization. It will be convenient to use the identification of lines in  $\mathbb{P}^3$  with planes in 4-dimensional space passing through the origin. Let  $V_\ell$  be the 2-dimensional  $\mathbb{Q}_p$ -subspace of  $\mathbb{Q}_p^4$  generated by the points of  $\ell(\mathbb{Q}_p)$ . Let  $W_\ell = V_\ell \cap \mathbb{Z}_p^4$ . This  $W_\ell$  is a  $\mathbb{Z}_p$ -module of rank 2 and we let  $\mathbf{u}, \mathbf{v}$  be a  $\mathbb{Z}_p$ -basis. Then the line  $\ell$  can be parametrized as  $s\mathbf{u} + t\mathbf{v}$ , and  $\bar{\ell}$  as  $s\bar{\mathbf{u}} + t\bar{\mathbf{v}}$ . We shall call this a *good* parametrization for  $\ell$ . We note that if  $P \in \ell(\mathbb{Q}_p)$  then there is a coprime pair of  $p$ -adic integers  $\lambda, \mu$  such that  $P = \lambda\mathbf{u} + \mu\mathbf{v}$ ; this can be easily seen by regarding  $P$  as a primitive element of  $W_\ell$ .

We now turn our attention to the surfaces of Theorems 2 and 3. Let  $M$  denote a non-zero square-free integer and let  $S$  be either of the surfaces in (1) or (2). Let  $p \neq 3$  be a prime dividing  $M$ ; we would like to study the group  $H_S(\mathbb{Q}_p)$ . Denote the reduction of  $S$  modulo  $p$  by  $\bar{S}$ . It is seen that  $\bar{S}$  is a cone over  $C_p = C \times \mathbb{F}_p$ , where  $C$  is given in (3), with vertex at  $(\bar{0} : \bar{0} : \bar{0} : \bar{1})$ . It is convenient to split the set of  $p$ -adic points on  $S$  into subsets of bad and good reduction:

$$S^{\text{bd}} = \{P \in S(\mathbb{Q}_p) : \bar{P} = (\bar{0} : \bar{0} : \bar{0} : \bar{1})\}, \quad S^{\text{gd}} = \{P \in S(\mathbb{Q}_p) : \bar{P} \neq (\bar{0} : \bar{0} : \bar{0} : \bar{1})\}.$$

We note however that  $S^{\text{bd}} = \emptyset$  in the case of the surface  $S'_M$  of (2). Now we can think of points on  $S^{\text{gd}}$  as reducing to points on  $C(\mathbb{F}_p)$ . We define  $\phi : S^{\text{gd}} \rightarrow C(\mathbb{F}_p)$  by  $\phi(x : y : z : w) = (\bar{x} : \bar{y} : \bar{z})$  where the four coordinates  $x, y, z, w$  are taken to be coprime in  $\mathbb{Z}_p$ .

**Lemma 12.1.** *Let  $M$  denote a non-zero squarefree integer and  $S$  either of the surfaces in (1) or (2). Let  $p \neq 3$  be a prime dividing  $M$ . Let  $\ell$  be a  $\mathbb{Q}_p$ -line such that  $\ell \cdot S = P_1 + P_2 + P_3$  with  $P_i \in S^{\text{gd}}$ . Suppose  $\bar{\ell} \not\subset \bar{S}$ . Then  $\phi(P_1) + \phi(P_2) + \phi(P_3) \sim 3\bar{\mathcal{O}}$  in  $\text{Pic}(C_p)$ .*

**Proof.** Let  $s\mathbf{u} + t\mathbf{v}$  be a good parametrization of  $\ell$  in the above sense. There are coprime pairs  $\lambda_i, \mu_i \in \mathbb{Z}_p$  for  $i = 1, 2, 3$  such that  $P_i = \lambda_i\mathbf{u} + \mu_i\mathbf{v}$  for  $i = 1, 2, 3$ . Since  $\ell \cdot S = P_1 + P_2 + P_3$  we have

$$F(s\mathbf{u} + t\mathbf{v}) = \alpha \prod_{i=1}^3 (\mu_i s - \lambda_i t) \tag{5}$$

for some  $\alpha$  in  $\mathbb{Z}_p$ . Moreover  $\alpha \not\equiv 0 \pmod{p}$  as  $\bar{\ell} \not\subset \bar{S}$ . Write  $\mathbf{u} = (u_0, u_1, u_2, u_3)$  and  $\mathbf{v} = (v_0, v_1, v_2, v_3)$  and let  $\mathbf{u}' = (\bar{u}_0, \bar{u}_1, \bar{u}_2)$  and  $\mathbf{v}' = (\bar{v}_0, \bar{v}_1, \bar{v}_2)$ . We first show that  $\mathbf{u}'$  and  $\mathbf{v}'$  are  $\mathbb{F}_p$ -linearly independent. If not, then  $\bar{\ell}$  passes through the vertex  $(\bar{0} : \bar{0} : \bar{0} : \bar{1})$  as well as the  $\bar{P}_i$  which are distinct from the vertex. This forces  $\bar{\ell} \subset \bar{S}$  contradicting the lemma's assumption that  $\bar{\ell} \not\subset \bar{S}$ . Thus  $\mathbf{u}'$  and  $\mathbf{v}'$  are  $\mathbb{F}_p$ -linearly independent.



Let  $\ell' \subset \mathbb{P}^2$  be the  $\mathbb{F}_p$  line  $su' + tv'$ . Reducing (5) modulo  $p$  we instantly see that  $\ell' \cdot C_p = \phi(P_1) + \phi(P_2) + \phi(P_3)$  which concludes the proof of the lemma.  $\square$

### 13. A homomorphism for $H_{S_M}(\mathbb{Q}_p)$

In this section  $M$  denotes a non-zero squarefree integer, and  $S$  the cubic surface denoted by  $S_M$  in (1):

$$S: x^3 + y^3 + z(z^2 + Mw^2) = 0.$$

Let  $C$  be the plane cubic curve (3). Again, let  $p$  be a prime divisor of  $M$  different from 3 and let  $C_p = C \times \mathbb{F}_p$ . In this section we shall define a surjective homomorphism  $H_S(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)/2\text{Pic}^0(C_p)$ . As previously observed, the reduction of  $S$  modulo  $p$  is a cone over  $C_p$  with vertex at  $(\bar{0} : \bar{0} : \bar{0} : \bar{1})$ . What makes the situation here somewhat tricky is that this singular point lifts to  $p$ -adic (and even rational) points on  $S$ ; for example  $(0 : 0 : 0 : 1) \in S(\mathbb{Q})$  is such a lift. Thus  $S^{\text{gd}}$  is strictly smaller than  $S(\mathbb{Q}_p)$ . We shall extend  $\phi : S^{\text{gd}} \rightarrow C(\mathbb{F}_p)$  defined in Section 12 to  $\phi : S(\mathbb{Q}_p) \rightarrow C(\mathbb{F}_p)$  where  $\phi(P) = \bar{O}$  for any  $P \in S^{\text{bd}}$ .

**Proposition 13.1.** *Let  $\psi : S(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)$  be given by  $\psi(P) = \phi(P) - \bar{O}$ . Then  $\psi$  induces a well-defined surjective homomorphism*

$$\psi : H_S(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)/2\text{Pic}^0(C_p), \quad \psi([P]) = \psi(P) \pmod{2\text{Pic}^0(C_p)}.$$

Before proving Proposition 13.1 we shall need the following three lemmas.

**Lemma 13.2.** *Suppose  $P \in S(\mathbb{Q}_p)$  such that  $\bar{P}$  lies in the plane  $z = \bar{0}$ . Then  $\psi(P) \in 2\text{Pic}^0(C_p)$ .*

**Proof.** If  $P \in S^{\text{bd}}$  then  $\psi(P) = 0$ . Otherwise,  $\phi(P)$  is a flex point on  $C_p$ . Hence  $\psi(P) = \phi(P) - \bar{O}$  is a difference of two flexes and so is an element of order dividing 3 in  $\text{Pic}^0(C_p)$ . It follows that  $\psi(P) \in 2\text{Pic}^0(C_p)$ ; indeed  $\psi(P) = -2\psi(P)$ .  $\square$

**Lemma 13.3.** *Let  $\ell$  be a  $\mathbb{Q}_p$ -line not contained in  $S$ . Suppose that  $\ell \cdot S = P_1 + P_2 + P_3$  where  $P_i \in S(\mathbb{Q}_p)$ . Suppose moreover that  $\bar{\ell} \subset \bar{S}$ . Then  $\psi_1(P) + \psi_2(P) + \psi_3(P) \in 2\text{Pic}^0(C_p)$ .*

**Proof.** Let  $su + tv$  be a good parametrization of  $\ell$ . In particular we know that  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_p^4$  and  $\bar{\mathbf{u}}, \bar{\mathbf{v}}$  are independent modulo  $p$ , and that there are coprime pairs  $\lambda_i, \mu_i$  such that  $P_i = \lambda_i \mathbf{u} + \mu_i \mathbf{v}$ . Now  $\bar{\ell}$  is contained in  $\bar{S}$  and so must pass through the vertex  $(\bar{0} : \bar{0} : \bar{0} : \bar{1})$ . Thus, applying a unimodular transformation, we may assume that our pair  $\mathbf{u}, \mathbf{v}$  have the form

$$\mathbf{u} = (u_1, u_2, u_3, 0), \quad \mathbf{v} = (pv_1, pv_2, pv_3, 1), \quad u_i, v_i \in \mathbb{Z}_p. \tag{6}$$

Let  $F = x^3 + y^3 + z^3 + Mzw^2$ . We can also assume that  $F(\mathbf{v}) \neq 0$ , by replacing  $\mathbf{v}$  with  $\mathbf{v} + \alpha p\mathbf{u}$  for an appropriate  $\alpha \in \mathbb{Z}_p$ . It follows that the polynomial  $F(\mathbf{u} + t\mathbf{v})$  is of degree 3 and has precisely 3 roots in  $\mathbb{Q}_p$ : namely  $\mu_i/\lambda_i$  for  $i = 1, 2, 3$ . However, expanding  $F(\mathbf{u} + t\mathbf{v})$  we obtain

$$\sum u_i^3 + 3p \left( \sum u_i^2 v_i \right) t + \left( 3p^2 \sum u_i v_i^2 + Mu_3 \right) t^2 + \left( p^3 \sum v_i^3 + pMv_3 \right) t^3. \tag{7}$$

Write  $F(\mathbf{u} + t\mathbf{v}) = a_0 + a_1t + a_2t^2 + a_3t^3$ , and let  $\alpha_i = \text{ord}_p(a_i)$ . Since  $\bar{\ell} \subset \bar{S}$  we see that  $\alpha_i \geq 1$ . Suppose first that  $p \nmid u_3$ . As  $M$  is squarefree and  $p \mid M$ , we see that

$$\alpha_0 \geq 1, \quad \alpha_1 \geq 1, \quad \alpha_2 = 1, \quad \alpha_3 \geq 2.$$

We shall need to study the Newton polygon of this polynomial which is the convex hull of the four points  $(i, \alpha_i)$ ; see for example [14, p. 19]. The Newton polygon contains precisely one segment of positive slope joining  $(2, 1)$  with  $(3, \alpha_3)$ . The other segments have non-positive slope. Hence the polynomial has precisely one root with negative valuation and two roots in  $\mathbb{Z}_p$ . By reordering the  $P_i$  we may suppose that  $\mu_1/\lambda_1$  has negative valuation and  $\mu_i/\lambda_i \in \mathbb{Z}_p$  for  $i = 2, 3$ . From the expressions  $P_i = \lambda_i\mathbf{u} + \mu_i\mathbf{v}$  we see that  $P_1 \in S^{\text{bd}}$  and  $P_2, P_3 \in S^{\text{gd}}$ . Moreover  $\phi(P_2) = \phi(P_3) = (u_1 : u_2 : u_3) \in C(\mathbb{F}_p)$ . Hence  $\psi(P_1) + \psi(P_2) + \psi(P_3) \in 2\text{Pic}^0(C_p)$ .

Finally we must deal with the case  $p \mid u_3$ . In this case  $\bar{P}_i$  lie in the plane  $z = \bar{0}$ . The lemma follows from Lemma 13.2.  $\square$

**Lemma 13.4.** *Let  $\ell$  be a  $\mathbb{Q}_p$ -line contained in  $S$ . For every  $P \in \ell(\mathbb{Q}_p)$ , we have  $\psi(P) \in 2\text{Pic}^0(C_p)$ .*

**Proof.** Since  $\bar{\ell}$  passes through the vertex of  $\bar{S}$  we may parametrize as  $\mathbf{su} + t\mathbf{v}$  where  $\mathbf{u}, \mathbf{v}$  are as in (6). Now the polynomial in (7) vanishes identically. From the coefficient of  $t^2$  we see that  $p \mid u_3$ . Hence  $\bar{\ell}$  lies in the plane  $z = \bar{0}$ . Now the lemma follows from Lemma 13.2.

In fact, more is true: the only  $\mathbb{Q}_p$ -lines on  $S$  are contained in the  $z = 0$  plane, but we do not need this.  $\square$

**Proof of Proposition 13.1.** Hensel’s Lemma shows that the map  $\phi : S^{\text{gd}} \rightarrow C(\mathbb{F}_p)$  is surjective, and thus  $\psi$  is surjective. Therefore, it is enough to show that  $\psi(P_1) + \psi(P_2) + \psi(P_3) \in 2\text{Pic}^0(C_p)$  whenever  $P_1, P_2, P_3 \in S(\mathbb{Q}_p)$  and

- (i) either there is a  $\mathbb{Q}_p$ -line  $\ell$  not contained in  $S$  with  $\ell \cdot S = P_1 + P_2 + P_3$ , or
- (ii) there is a  $\mathbb{Q}_p$ -line  $\ell$  contained in  $S$  with  $P_1, P_2, P_3 \in \ell$ .

For (ii) we know by Lemma 13.4 that  $\psi(P_i) \in 2\text{Pic}^0(C_p)$ , so it remains to deal with (i). Thus suppose that  $\ell$  is a  $\mathbb{Q}_p$ -line not contained in  $S$  and  $\ell \cdot S = P_1 + P_2 + P_3$  where  $P_i \in S(\mathbb{Q}_p)$ . If all three  $P_i \in S^{\text{bd}}$  then the required result follows from the definition of  $\psi$ . Suppose that at least one  $P_i \in S^{\text{gd}}$ .

- If all three  $P_i \in S^{\text{gd}}$  and  $\bar{\ell} \not\subset \bar{S}$  then we can conclude using Lemma 12.1.
- If all three  $P_i \in S^{\text{gd}}$  and  $\bar{\ell} \subset \bar{S}$  we can conclude using Lemma 13.3.

We have reduced to the case where at least one of the  $P_i$  is in  $S^{\text{gd}}$  and at least one is in  $S^{\text{bd}}$ . This forces  $\bar{\ell} \subset \bar{S}$  and again we can conclude using Lemma 13.3.  $\square$

### 14. Proof of Theorem 2

In this section we shall put together the results of the previous sections to prove Theorem 2. Thus let  $p_1, \dots, p_s$  ( $s \geq 1$ ) be primes such that  $p_i \equiv 1 \pmod{3}$  and 2 is a cube modulo each  $p_i$ . Let  $M = \prod p_i$  and  $S = S_M$  be the cubic surface in (1).

For  $p = p_i$ , Proposition 13.1 gives a surjective homomorphism

$$\psi : H_S(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)/2\text{Pic}^0(C_p).$$

Now  $\psi(1 : -1 : 0 : 0) = 0$ , thus the restriction of  $\psi$  to  $H_S^0(\mathbb{Q}_p)$  is still surjective. In particular,

$$\dim_{\mathbb{F}_2} H_S^0(\mathbb{Q}_p)/2H_S^0(\mathbb{Q}_p) \geq \dim_{\mathbb{F}_2} \text{Pic}^0(C_p)/2\text{Pic}^0(C_p) = 2$$

by Lemma 11.2. However, by Proposition 9.1, the map

$$H_S^0(\mathbb{Q})/2H_S^0(\mathbb{Q}) \rightarrow \prod_{p=p_1}^{p=p_s} H_S^0(\mathbb{Q}_p)/2H_S^0(\mathbb{Q}_p)$$

is surjective, and so

$$\dim_{\mathbb{F}_2} H_S^0(\mathbb{Q})/2H_S^0(\mathbb{Q}) \geq 2s.$$

As  $S$  contains the  $\mathbb{Q}$ -rational line  $x + y + z = 0$ , we know by Theorem 6 that  $H_S^0(\mathbb{Q}) = H_S(\mathbb{Q})[2]$ . Thus  $\dim_{\mathbb{F}_2} H_S(\mathbb{Q})[2] \geq 2s$ . Now the point  $(1 : -1 : 0 : 0)$  is  $\mathbb{Q}$ -ternary on  $S$ . Thus we can apply Theorem 5 obtaining  $r(S, \mathbb{Q}) \geq \dim_{\mathbb{F}_2} H_S(\mathbb{Q})[2] \geq 2s$ , which proves Theorem 2.

### 15. A homomorphism for $H_{S'_M}(\mathbb{Q}_p)$

In this section  $M > 1$  denotes a squarefree integer and  $S$  the cubic surface denoted by  $S'_M$  in (2):

$$S: x^3 + y^3 + z^3 + Mw^3 = 0.$$

Let  $C$  be the plane cubic curve (3). Let  $p$  be a prime divisor of  $M$  different from 3 and  $\phi : S(\mathbb{Q}_p) \rightarrow C(\mathbb{F}_p)$  as defined in Section 12; as previously observed for this surface,  $S^{\text{bd}} = \emptyset$  and so  $S^{\text{gd}} = S(\mathbb{Q}_p)$ . Let  $\psi : S(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)$  be given by  $\psi(P) = \phi(P) - \bar{O}$ .

**Proposition 15.1.** *Let  $C_p = C \times \mathbb{F}_p$ . Then  $\psi$  extends uniquely to a well-defined surjective homomorphism*

$$\psi : H_S(\mathbb{Q}_p) \rightarrow \text{Pic}^0(C_p)/3\text{Pic}^0(C_p), \quad \psi([P]) = \psi(P) \pmod{3\text{Pic}^0(C_p)}.$$

**Proof.** Surjectivity follows as in the proof of Proposition 13.1. It is therefore enough to show that  $\psi(P_1) + \psi(P_2) + \psi(P_3) \in 3\text{Pic}^0(C_p)$  whenever  $P_1, P_2, P_3 \in S(\mathbb{Q}_p)$  and

- (i) either there is a  $\mathbb{Q}_p$ -line  $\ell$  not contained in  $S$  with  $\ell \cdot S = P_1 + P_2 + P_3$ , or
- (ii) there is a  $\mathbb{Q}_p$ -line  $\ell$  contained in  $S$  with  $P_1, P_2, P_3 \in \ell$ .

The second possibility does not arise since none of the 27 lines on  $S$  are defined over  $\mathbb{Q}_p$ . Thus suppose  $\ell$  is a  $\mathbb{Q}_p$ -line not contained in  $S$  such that  $\ell \cdot S = P_1 + P_2 + P_3$ . If  $\bar{\ell} \not\subset \bar{S}$  then by Lemma 12.1 we know that  $\phi(P_1) + \phi(P_2) + \phi(P_3) \sim 3\bar{O}$  in  $\text{Pic}(C_p)$ . In this case  $\psi(P_1) + \psi(P_2) + \psi(P_3) = 0$  in  $\text{Pic}^0(C_p)$ . Thus we may suppose that  $\bar{\ell} \subset \bar{S}$ . Hence  $\bar{\ell}$  passes through the vertex  $(\bar{0} : \bar{0} : \bar{0} : 1)$ , otherwise its projection on to the  $xyz$ -projective plane would be a line contained in irreducible curve  $C_p$  which is impossible. It follows that  $\phi(P_1) = \phi(P_2) = \phi(P_3)$  and thus  $\psi(P_1) + \psi(P_2) + \psi(P_3) \in 3\text{Pic}^0(C_p)$ .  $\square$

### 16. Proof of Theorem 3

This follows from Lemma 11.1 and Propositions 10.1 and 15.1 in exactly the same way as the proof of Theorem 2 (Section 14).

## Acknowledgments

I thank Felipe Voloch for drawing my attention to [25] (via the website [mathoverflow.net](http://mathoverflow.net)). I am grateful to Martin Bright, David Holmes, Miles Reid and Damiano Testa for helpful discussions, and the referee for many corrections and comments. I would like to thank Jean-Louis Colliot-Thélène for useful correspondence regarding the above conjecture and for drawing my attention to [18]. In particular, Professor Colliot-Thélène points out that it should be possible to deduce unboundedness results for cubic surfaces similar to our Theorems 2 and 3 from unboundedness results for the number of  $R$ -equivalence classes of Châtelet surfaces [7, Theorem 8.13].

## References

- [1] M.J. Bright, N. Bruin, E.V. Flynn, A. Logan, The Brauer–Manin obstruction and III[2], *LMS J. Comput. Math.* 10 (2007) 354–377.
- [2] J.-L. Colliot-Thélène, L'arithmétique des variétés rationnelles, *Ann. Fac. Sci. Toulouse* 1 (1992) 295–336.
- [3] J.-L. Colliot-Thélène, Hilbert's Theorem 90 for  $K^2$ , with application to the Chow groups of rational surfaces, *Invent. Math.* 71 (1983) 1–20.
- [4] J.-L. Colliot-Thélène, F. Ischebeck, L'équivalence rationnelle sur les cycles de dimension zéro des variétés algébriques réelles, *C. R. Acad. Sci. Paris Sér. I Math.* 292 (15) (1981) 723–725.
- [5] J.-L. Colliot-Thélène, D. Kanevsky, J.-J. Sansuc, Arithmétique des surfaces cubiques diagonales, in: G. Wüstholz (Ed.), *Diophantine Approximation and Transcendence Theory*, in: *Lecture Notes in Math.*, vol. 1290, Springer-Verlag, 1987, pp. 1–108.
- [6] J.-L. Colliot-Thélène, J.-J. Sansuc, La descente sur les variétés rationnelles, in: A. Beauville (Ed.), *Journées de géométrie algébrique d'Angers (Juillet 1979)*, Sijthof and Noordhof, 1980, pp. 223–237.
- [7] J.-L. Colliot-Thélène, J.-J. Sansuc, H.P.F. Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces. II, *J. Reine Angew. Math.* 374 (1987) 72–168.
- [8] D. Eisenbud, J. Harris, *The Geometry of Schemes*, *Grad. Texts in Math.*, vol. 197, Springer-Verlag, 2000.
- [9] R. Hartshorne, *Algebraic Geometry*, *Grad. Texts in Math.*, vol. 52, Springer-Verlag, 1977.
- [10] H. Heilbronn, Zeta-Functions and  $L$ -Functions, in: J.W.S. Cassels, A. Fröhlich (Eds.), *Algebraic Number Theory*, Academic Press, 1967 (Chapter VIII).
- [11] J. Jahnel, Brauer groups, Tamagawa measures, and rational points on algebraic varieties, *Habilitationsschrift*, Göttingen, 2008, available from <http://www.uni-math.gwdg.de/jahnel/linkstopaperse.html>.
- [12] D. Kanevsky, Yu. Manin, Composition of points and the Mordell–Weil problem for cubic surfaces, in: *Rational Points on Algebraic Varieties*, in: *Progr. Math.*, vol. 199, Birkhäuser, Basel, 2001, pp. 199–219.
- [13] A.W. Knap, *Elliptic Curves*, *Math. Notes*, vol. 40, Princeton University Press, 1992.
- [14] N. Koblitz,  *$p$ -Adic Analysis: A Short Course on Recent Work*, *London Math. Soc. Lecture Note Ser.*, vol. 46, Cambridge University Press, 1980.
- [15] Yu.I. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic*, North-Holland, 1974 and 1986.
- [16] Yu.I. Manin, Mordell–Weil problem for cubic surfaces, in: *Advances in Mathematical Sciences: CRM's 25 Years*, Montreal, PQ, 1994, in: *CRM Proc. Lecture Notes*, vol. 11, Amer. Math. Soc., Providence, RI, 1997, pp. 313–318.
- [17] I. Polo-Blanco, J. Top, Explicit real cubic surfaces, *Canad. Math. Bull.* 51 (1) (2008) 125–133.
- [18] P. Salberger, A.N. Skorobogatov, Weak approximation for surfaces defined by two quadratic forms, *Duke Math. J.* 63 (2) (1991) 517–536.
- [19] I.R. Shafarevich, *Basic Algebraic Geometry* 1, second ed., Springer-Verlag, 1994.
- [20] B. Segre, *The Non-Singular Cubic Surfaces*, Oxford University Press, 1942.
- [21] B. Segre, A note on arithmetical properties of cubic surfaces, *J. London Math. Soc.* 18 (1943) 24–31.
- [22] A.N. Skorobogatov, *Torsors and Rational Points*, *Cambridge Tracts in Math.*, vol. 144, Cambridge University Press, 2001.
- [23] P. Swinnerton-Dyer, The Brauer group of cubic surfaces, *Math. Proc. Cambridge Philos. Soc.* 113 (1993) 449–460.
- [24] I. Szilágyi, B. Jüttler, J. Schicho, Local parametrization of cubic surfaces, *J. Symbolic Comput.* 41 (1) (2006) 30–48.
- [25] B.G. Vioreanu, Mordell–Weil problem for cubic surfaces, numerical evidence, in: *Arithmetic Geometry*, in: *Clay Math. Proc.*, vol. 8, Amer. Math. Soc., Providence, RI, 2009, pp. 223–240.
- [26] J.F. Voloch, Surfaces in  $\mathbb{P}^3$  over finite fields, in: *Topics in Algebraic and Noncommutative Geometry*, Luminy/Annapolis, MD, 2001, in: *Contemp. Math.*, vol. 324, Amer. Math. Soc., Providence, RI, 2003, pp. 219–226.