THE UNIVERSITY OF WARWICK

Library Declaration and Deposit Agreement

1. STUDENT DETAILS

Please complete the following:

Full name: ……

University ID number: ……

2. THESIS DEPOSIT

2.1 Under your registration at the University, you are required to deposit your thesis with the University in BOTH hard copy and in digital format. The digital copy should normally be saved as a single pdf file.

2.2 The hard copy will be housed in the University Library. The digital copy will be deposited in the University's Institutional Repository (WRAP). Unless otherwise indicated (see 2.6 below), this will be made immediately openly accessible on the Internet and will be supplied to the British Library to be made available online via its Electronic Theses Online Service (EThOS) service.
[At present, theses submitted for a Master's degree by Research (MA, MSc, LLM, MS or MMedSci) are not being deposited in WRAP and not being made available via EthOS. This may change in future.]

2.3 In exceptional circumstances, the Chair of the Board of Graduate Studies may grant permission for an embargo to be placed on public access to the thesis **in excess of two years**. This must be applied for when submitting the thesis for examination (further information is available in the *Guide to Examinations for Higher Degrees by Research*.)

2.4 If you are depositing a thesis for a Master's degree by Research, the options below only relate to the hard copy thesis.

2.5 If your thesis contains material protected by third party copyright, you should consult with your department, and if appropriate, deposit an abridged hard and/or digital copy thesis.

2.6 Please tick one of the following options for the availability of your thesis (guidance is available in the *Guide to Examinations for Higher Degrees by Research)***:**

☐ Both the hard and digital copy thesis can be made publicly available immediately

☐ The hard copy thesis can be made publicly available immediately and the digital copy thesis can be made publicly available after a period of two years (*should you subsequently wish to reduce the embargo period please inform the Library*)

☐ Both the hard and digital copy thesis can be made publicly available after a period of two years (*should you subsequently wish to reduce the embargo period please inform the Library*)

☐ Both the hard copy and digital copy thesis can be made publicly available after _____ (insert time period in excess of two years). **This option requires the prior approval of the Chair of the Board of Graduate Studies (see 2.3 above)**

The University encourages users of the Library to utilise theses as much as possible, and unless indicated below users will be able to photocopy your thesis.

☐ I **do not** wish for my thesis to be photocopied

3. GRANTING OF NON-EXCLUSIVE RIGHTS

Whether I deposit my Work personally or through an assistant or other agent, I agree to the following:

- Rights granted to the University of Warwick and the British Library and the user of the thesis through this agreement are non-exclusive. I retain all rights in the thesis in its present version or future versions. I agree that the institutional repository administrators and the British Library or their agents may, without changing content, digitise and migrate the thesis to any medium or format for the purpose of future preservation and accessibility.

4. DECLARATIONS

I DECLARE THAT:

- I am the author and owner of the copyright in the thesis and/or I have the authority of the authors and owners of the copyright in the thesis to make this agreement. Reproduction of any part of this thesis for teaching or in academic or other forms of publication is subject to the normal limitations on the use of copyrighted materials and to the proper and full acknowledgement of its source.

- The digital version of the thesis I am supplying is either the same version as the final, hard-bound copy submitted in completion of my degree once any minor corrections have been completed, or is an abridged version (see 2.5 above).

- I have exercised reasonable care to ensure that the thesis is original, and does not to the best of my knowledge break any UK law or other Intellectual Property Right, or contain any confidential material.

- I understand that, through the medium of the Internet, files will be available to automated agents, and may be searched and copied by, for example, text mining and plagiarism detection software.

- At such time that my thesis will be made publically available digitally (see 2.6 above), I grant the University of Warwick and the British Library a licence to make available on the Internet the thesis in digitised format through the Institutional Repository and through the British Library via the EThOS service.

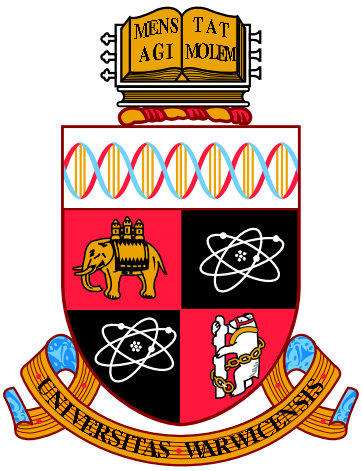
- If my thesis does include any substantial subsidiary material owned by third-party copyright holders, I have sought and obtained permission to include it in any version of my thesis available in digital format and that this permission encompasses the rights that I have granted to the University of Warwick and to the British Library.

5. LEGAL INFRINGEMENTS

I understand that neither the University of Warwick nor the British Library have any obligation to take legal action on behalf of myself, or other rights holders, in the event of infringement of intellectual property rights, breach of contract or of any other right, in the thesis.

Please sign this agreement and ensure it is bound into the final hard bound copy of your thesis, which should be submitted to Student Reception, Senate House.

Student's signature: .....…… Date: .....



Rational Points on Smooth Cubic Hypersurfaces

by

Stefanos Papanikolopoulos

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Warwick Mathematics Institute

September 2014

THE UNIVERSITY OF WARWICK

Contents

Acknowledgments

I could not put into words my gratitude for my supervisor, Samir Siksek, for his support, invaluable comments, and guidance the past four years. Without him, my research wouldn't have been so fulfilling and exciting as it has been, or even possible.

Furthermore, I would also like to thank my teachers throughout the years, especially Vassilis Papathanasiou and Maria Papatriantafillou. They are part of some of the most treasured memories I have kept from my journey in Mathematics so far.

I am also grateful to Damiano Testa, for his help, guidance, and the fact that he was there to give me the tools to formulate crucial geometric arguments of my thesis.

To my supportive partner, Martha, I would like to offer my deepest gratitude; for her peer review, emotional support, and the unmeasurable deal of help with LaTeX.

This thesis would not have been possible without my family in Greece, Katerina, Panagiota and Olymbia, as they provided more financial support they could afford. Also, their understanding to the challenges that writing a thesis poses could not go unmentioned.

My special thanks also go to my friends Agis, Dionisis and Xenia. They may have been far away, but our communication encouraged me and made this time in my life much easier.

I would also like to thank Lambros and Michalis, two peers and dear friends that I had the luck of meeting during the first year of my studies in Warwick. Their help and friendship has been invaluable.

At this point I should thank my dear friends, Kelly and Aggelos. Living in Coventry would have been a challenge, but they filled it with fun and loving memories.

Finally, I could not possibly forget to thank Sofos and Chatzakos, especially for their help with the preparation of my talk in Bristol.

Declarations

Considerable effort has been made to keep all existing results in the Introduction (Chapter 1) and all the original research carried out by the author in the Chapters 3, 4 and 5. In the cases that doing so would cause unnecessary stress to the reader, this principle is violated, and the source is clearly stated in every such result or proposition.

Chapter 2 serves as a buffer zone; most of the results are known, but they are presented with some tweaks, so that they will better serve the purposes of this thesis. Also there is a clear statement of the source of these results.

Finally, most of the material in Chapters 3, 4 and 5 will appear in a manuscript, written by the author of this thesis. This manuscript is still in preparation and will be submitted in a peer reviewed mathematical journal.

Abstract

Let S be a smooth n-dimensional cubic variety over a field K and suppose that K is finitely generated over its prime subfield. It is a well-known fact that whenever we have a set of K-points on S, we may obtain new ones, using secant and tangent constructions. A Mordell-Weil generating set $B \subseteq S(K)$ is a subset of minimal cardinality that generates $S(K)$ via these operations; we define the Mordell-Weil rank as $r(S, K) = \#B$. The Mordell-Weil theorem asserts that in the case of an elliptic curve E defined over a number field K, we have that $r(E, K) < \infty$. Manin [11] asked whether this is true or not for surfaces. Our goal is to settle this question for higher dimensions, and for as many fields as possible. We prove that when the dimension of the cubic hypersurface is big enough, if a point can generate another point, then it can generate all the points in the hypersurface that lie in its tangent plane. This gives us a powerful tool, yet a simple one, for generating sets of points starting with a single one. Furthermore, we use this result to prove that if K is a finite field and the dimension of the hypersurface is at least 5, then $r(S, K) = 1$.

On the other hand, it is natural to ask whether $r(S, K)$ can be bounded by a constant, depending only on the dimension of S. It is conjectured that such a constant does not exist for the elliptic curves (the unboundedness of ranks conjecture for elliptic curves). In the case of cubic surfaces, Siksek [16] has proven that such a constant does not exist when $K = \mathbb{Q}$. Our goal is to generalise this for cubic threefolds. This is achieved via an abelian group

$H_S(K)$, which holds enough information about the Mordell-Weil rank $r(S, K)$ in the following manner; if $H_S(K)$ becomes large, so does $r(S, K)$. Then, by using a family of cubic surfaces that is known to have an unbounded number of Mordell-Weil generators over $\mathbb{Q}$, we prove that the number of Mordell-Weil generators is unbounded in the case of threefolds too.

to V. Papathanasiou...

Chapter 1

Introduction

1.1 Background and Motivation

Looking back in history, trying to trace back this ever-increasing abstraction that we may call mathematics, we can clearly see that there are two fundamental concepts; shapes and numbers. Number theory, and especially the study of Diophantine equations, can be considered a core mathematical study. We recall that a Diophantine equation is a system of polynomial equations over a field K, and therefore it can be thought of as a subset of the affine space K^n. This simple idea gave number theorists a whole new arsenal of techniques to tackle old problems. It also paved the path to new connections in mathematics. Probably, the best example is Fermat's Last Theorem, which remained open for more than three centuries until Wiles gave his famous proof in 1995.

This interplay between number theory and algebraic geometry can be used to find a natural, though unexpected, way to categorise Diophantine equations; the dimension of the zero locus. For example, we can restrict ourselves

to one-dimensional varieties, or curves. Examples of curves are:

$$x + y + z = 0$$

in $\mathbb{P}^2$ and

$$y^2 - xz = yw - z^2 = xw - yz = 0$$

in $\mathbb{P}^3$. These two serve as a fine example of a connection that would not have been possible without the use of Algebraic Geometry in Number Theory.

A finer categorisation for curves is the genus. Curves are far more studied and understood than higher dimensional varieties, but even in this case, the only genera that we have a good understanding of are 0 and 1. If the genus of the curve over a number field K is higher than 1, we still have some deep results, such as Faltings' Theorem that asserts that the curve has only finitely many points. Elliptic curves (smooth curves of genus 1 that have a K rational point) have formed a paradigm on the way to look for results in Diophantine equations. For a number field K, the set of K-rational points on an elliptic curve E defined over K forms a finitely generated abelian group; this is the famous Mordell–Weil Theorem. This thesis is concerned with analogues of the Mordell–Weil theorem in higher dimensions, building on recent advances in the two-dimensional case, due to Siksek [16] and Cooley [2], [3].

1.2 Thesis Layout

The rest of this chapter is a reminder of the tools that will be needed throughout this thesis. The following chapter will contain the preliminary theorems and constructions, while the main results are presented and proven

in Chapters 3, 4, and 5.

Specifically, in Chapter 3 we shall prove, conditionally on a conjecture of Colliot-Thélène, that the Mordell-Weil rank of a smooth cubic threefold is unbounded. In Chapter 4 we shall give conditions on the finiteness of the Mordell–Weil rank of a smooth cubic hypersurface over an arbitrary field, given that its dimension is big enough. Finally, in chapter 5 we prove some results for the Mordell–Weil rank over $\mathbb{F}_q$.

1.3 Varieties

In this section we suppose that K is an algebraically closed field. The definitions and notation given in this section follow [12]. Throughout this thesis, every ring will be considered to be a commutative ring with identity. Another convention that we shall use is for any points P, Q, R in general position, we write $\ell_{P,Q}$ for the line passing through P and Q, and $\Pi_{P,Q,R}$ for the unique plane that passes through P, Q, and R.

1.3.1 Affine Varieties

Let K be a field and $A = K[x_1, \ldots, x_n]$. We shall write $\mathbb{A}^n_K = K^n$ for an n-dimensional affine space over K. We remark that there is a distinction on how we perceive $\mathbb{A}^n_K$ and K^n, as the latter is treated as just the point-set $K \times K \times \ldots \times K$.

Consider the following correspondence:

$$V : \{I \mid I \trianglelefteq A\} \to \{X \mid X \subseteq \mathbb{A}_K^n\}$$
$$I \mapsto \{P \in \mathbb{A}_K^n \mid \text{ for all } f \in I : f(P) = 0\}.$$

An **algebraic set** is a subset in the image of this correspondence. Moreover, if $X = V(I)$, for a prime ideal I, then X is called an **affine variety**.

In order to simplify the notation, for a principal ideal $I = (f)$, we shall write $V(f)$ for $V(I)$. The **dimension** of a variety $V(I)$ is defined as the Krull dimension of $K[x_1, \ldots, x_n]/I$. The algebraic sets form the closed sets of a topology on $\mathbb{A}_K^n$, which is called the **Zariski topology**.

Let $V = V(I)$ be an affine variety. We define the **tangent space** on V at a point $P = (p_1, \ldots, p_n) \in V$ to be

$$T_P V = \bigcap_{f \in I} V\left(\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P) \cdot (x_i - p_i)\right).$$

A point $P \in V = V(I)$ is called **singular** if $\dim V < \dim T_P V$.

In many a case throughout this thesis I will be a principal ideal, generated by a function that has zero in its zero locus, so we will give a formula for the tangent space at this special case.

Observation 1.3.1. *Suppose that $V = V(I)$ is the algebraic set corresponding to a principal ideal $I = (f)$, and that $f(0) = 0$. Let l be the sum of the first degree monomials in f. Then,*

$$T_0 V = \{x \in \mathbb{A}_K^n \mid l(x) = 0\}.$$

Proof. We may assume that $f = c + l + h$, where c is a constant, and h is the sum of higher order terms. As $f(0) = 0$, it follows that $c = 0$. From the definition of the tangent space we have that

$$T_0V = V\left(\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(0) \cdot (x_i)\right) = V\left(\sum_{i=1}^{n} \frac{\partial l}{\partial x_i}(0) \cdot (x_i) + \sum_{i=1}^{n} \frac{\partial h}{\partial x_i}(0) \cdot (x_i)\right).$$

The polynomial h is the sum of monomials of degree at least 2. Therefore the derivative of each of these monomials vanishes when it is evaluated at zero. Hence,

$$T_0V = V\left(\sum_{i=1}^{n} \frac{\partial l}{\partial x_i}(0) \cdot (x_i)\right) = V(l) = \{x \in \mathbb{A}_K^n \mid l(x) = 0\}.$$

□

1.3.2 Projective Varieties

A polynomial $f \in K[x_0, \ldots, x_n]$ is **homogeneous of degree** d if

$$f = \sum a_{i_0 \ldots i_n} x_0^{i_0} \ldots x_n^{i_n},$$

with $a_{i_0 \ldots i_n} \neq 0$ only when $i_0 + \cdots + i_n = d$. Any polynomial $f \in K[x_0, \ldots, x_n]$ has a unique expression $f = f_0 + \cdots + f_N$, for some $N \geq 0$, such that, for all $i = 1 \ldots, N$, the polynomial f_i is homogeneous of degree i. The aforementioned expression is called the **homogeneous decomposition** of the polynomial f, and the polynomials f_i are the **homogeneous components** of f.

An ideal $I \subset K[x_0, \ldots, x_n]$ is a **homogeneous ideal** or simply homogeneous if for all polynomials $f \in I$, when $f = f_0 + \cdots + f_N$ is the homogeneous

decomposition of f then for all $i = 1, \ldots, N$, we have that $f_i \in I$. In other words, I is homogeneous if the homogeneous components of any polynomial $f \in I$ are contained in I. Equivalently, the ideal I is homogeneous if it is generated by finitely many homogeneous polynomials.

Now, let us consider the following relation, for $\overrightarrow{x}$, $\overrightarrow{y} \in K^{n+1}$:

$$\overrightarrow{x} \sim \overrightarrow{y} \text{ if and only if there exists } \lambda \in K^* \text{ such that } \overrightarrow{x} = \lambda \overrightarrow{y}.$$

This is an equivalence relation in K^{n+1} and the space $K^{n+1}/\sim$ is the n-dimensional **projective space**, which we shall denote by $\mathbb{P}^n_K$. In this setting, analogously to the correspondence V in affine varieties, we define:

$$\mathbb{V} : \left\{ I \;\middle|\; \begin{array}{l} I \trianglelefteq K[x_0, \ldots, x_n], \\ I \text{ homogeneous} \end{array} \right\} \to \{X \mid X \subseteq \mathbb{P}^n_K\}$$

$$I \mapsto \left\{ P \in \mathbb{P}^n_K \;\middle|\; \begin{array}{l} \text{for all homogeneous } f \in I \\ \text{such that } f(P) = 0 \end{array} \right\}$$

If $X = \mathbb{V}(I)$ for a homogeneous prime ideal $I \subset K[x_0 \ldots, x_n]$, then X is called a **projective variety**. In other words, a projective variety V is the zero locus in $\mathbb{P}^n_K$ of a finite family of homogeneous polynomials that generate a prime ideal. The dimension and the tangent space of a projective variety are defined analogously to the case of the affine variety. If all the polynomials in the family are of the same degree, then the variety shall be named according to the degree (e.g. quadratic, cubic, quartic, etc.). In this thesis, unless otherwise stated, when we consider a variety it will be assumed to be a projective variety.

It is easy to see that:

$$\mathbb{P}^n_K = \bigcup_{i=0}^{n} U_i,$$

where U_i is the Zariski open set $\mathbb{P}^n_K \setminus \mathbb{V}(x_i)$. A point $[p_0 : p_1 : \cdots : p_n] \in U_i$ corresponds to the point $(\frac{p_0}{p_i}, \ldots, \frac{p_{i-1}}{p_i}, \frac{p_{i+1}}{p_i}, \ldots, \frac{p_n}{p_i}) \in \mathbb{A}^n$.

Definition 1.3.2. Let $V \subseteq \mathbb{P}^n$ be an affine variety, and suppose for simplicity that $V \not\subset \mathbb{V}(x_i)$ for any i. We have seen that $\mathbb{P}^n$ is covered by $(n+1)$ affine pieces $\mathbb{A}^n_{(i)}$, with affine coordinates $x_0^{(i)}, \ldots, x_{i-1}^{(i)}, x_{i+1}^{(i)}, \ldots, x_n^{(i)}$, where:

$$x_j^{(i)} = x_j / x_i \quad \text{for } j \neq i.$$

Write $V_{(i)} = V \cap \mathbb{A}^n_{(i)}$. Then $V_{(i)} \subseteq \mathbb{A}^n_{(i)}$ is clearly an affine algebraic set, because:

$$\begin{aligned} & V_{(i)} \ni P = (p_0^{(i)}, \ldots, p_{i-1}^{(i)}, 1, p_{i+1}^{(i)}, \ldots, p_n^{(i)}) \\ \iff & f(p_0^{(i)}, \ldots, p_{i-1}^{(i)}, 1, p_{i+1}^{(i)}, \ldots, p_n^{(0)}) = 0 \quad \forall \text{ homogeneous } f \in I(V), \end{aligned}$$

which is a set of polynomial relations in the coordinates $(x_1^{(0)}, \ldots, x_n^{(0)})$ of P. The $V_{(i)}$ are called **standard affine pieces** of V.

Theorem 1.3.3 (Harnack's Theorem)**.** *Let C be a curve of degree m in the real projective plane. Then the number c of its components is bounded by:*

$$\frac{1-(-1)^m}{2} \leqslant c \leqslant 1 + \frac{(m-1)(m-2)}{2}$$

Proof. For proof see [5]. □

A **hypersurface** is a special case of a variety $\mathbb{V}(I)$, where I is a principal ideal. A generalisation of hypersurfaces is **complete intersections**. We recall

that a complete intersection is a variety $\mathbb{V}(I)$, such that the minimum number of polynomials required to generate I is equal to its co-dimension.

1.4 Elliptic curves

One of the most interesting types of varieties in Number Theory are elliptic curves. An **elliptic curve** is a pair (E, O), where E is a non-singular curve of genus one and $O \in E$. We generally denote the elliptic curve simply by E, the point O being understood. The elliptic curve E is defined over K, written E/K, if E is defined over K as a curve and $O \in E(K)$. We remark that E can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point O, on the line at ∞. Then, after X and Y are scaled appropriately, E has an equation of the form:

$$Y^2Z + \alpha_1 XYZ + \alpha_3 YZ^2 = X^3 + \alpha_2 X^2 Z + \alpha_4 XZ^2 + \alpha_6 Z^3,$$

where $O = [0 : 1 : 0]$ is considered to be the base point and $\alpha_1, \ldots, \alpha_6 \in \overline{K}$. An equation of this form is called a **Weierstrass equation** .

The Weierstrass equation for an elliptic curve is usually written using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ as follows:

$$E : y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6,$$

having in mind that there is an extra point O at infinity. If $\alpha_1, \ldots, \alpha_6 \in K$, then we say that E is defined over K.

A point $P \in E$ is a **point of inflexion**, or simply a **flex**, if the tangent line $T_P E$ to E at P meets E with multiplicity 3.

We continue by assuming that the field has char(()$\overline{\mathrm{K}}$) $\neq 2, 3$, as we are mainly interested in these cases. Let $P = (x_0, y_0)$ be a point satisfying a Weierstrass equation:

$$f(x, y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6 = 0,$$

and assume that P is a singular point on the curve $f(x, y) = 0$. It follows that there are $\alpha, \beta \in \overline{K}$ such that the Taylor series expansion of $f(x, y)$ at P has the form:

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

The singular point P is a **node** if $\alpha \neq \beta$. In this case the lines

$$y - y_0 = \alpha(x - x_0) \quad \text{and} \quad y - y_0 = \beta(x - x_0)$$

are the tangent lines at P. Conversely, if $\alpha = \beta$, then we say that P is a **cusp** and in this case the tangent line at P is given by:

$$y - y_0 = \alpha(x - x_0).$$

1.4.1 The composition law

Let E be an elliptic curve given by a Weierstrass equation (we assume that $O = [0 : 1 : 0]$ is the point at infinity). Any line in $\mathbb{P}^2$, by Bezout's Theorem, meets E in exactly three points, counting multiplicity. We define a composition law $\oplus$ on E as follows. Let $P, Q \in E$ and ℓ the line that passes

from P, Q (if $P = Q$ then ℓ is the tangent line to E at P). Also, let R' be the third point in the intersection of ℓ with E, and ℓ' to be the line that joins R' to the point at infinity, O. Then, ℓ' intersects E at O, R' and a third point R. That third point, R, is denoted by $P \oplus Q$. We remark that this process of obtaining the point R from the points P and Q is called the **chord-and-tangent process**.

Proposition 1.4.1 (Properties of the composition law)**.** *The composition law satisfies the following:*

1. *For any $P, Q, R \in E$, we have that*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$$

2. *If a line intersects E at the points P, Q, R (not necessarily distinct), then*

$$P \oplus Q \oplus R = O.$$

3. *For all $P \in E$, we have that $P \oplus O = P$.*

4. *For all $P, Q \in E$, we have that $P \oplus Q = Q \oplus P$.*

5. *For any $P \in E$ there is a point in E, denoted by $\ominus P$, such that*

$$P \oplus (\ominus P) = O$$

It follows that the composition law makes E into an abelian group with identity element the point at infinity, O.

Proof. We refer the reader to [17] □

1.4.2 Picard group

We follow the description in [17, Chapter 2]. Let K be a field, and C a curve defined over K. The **divisor group** of a curve C, denoted by $\mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}})$, is the free abelian group generated by the $\overline{K}$-points of C. Thus a divisor $D \in \mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}})$ is a formal sum

$$D = \sum_{P \in C(\overline{K})} n_P(P),$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C(\overline{K})$. The **degree** of D is defined by

$$\deg D = \sum_{P \in C(\overline{K})} n_P.$$

The **divisors of degree 0** form a subgroup of $\mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}})$, which we denote by

$$\mathrm{Div}^0(\mathrm{C}/\overline{\mathrm{K}}) = \{\mathrm{D} \in \mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}}) \mid \deg \mathrm{D} = 0\}.$$

A divisor $D \in \mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}})$ is **principal** if it has the form $D = \mathrm{div}(\mathrm{f})$ for some $f \in \overline{K}(C)^*$. Two divisors are linearly equivalent, written $D_1 \sim D_2$ if $D_1 - D_2$ is principal. The principal divisors form a subgroup of $\mathrm{Div}^0(\mathrm{C}/\overline{\mathrm{K}})$. The **divisor class group** or **Picard group** of C, denoted by $\mathrm{Pic}(\mathrm{C}/\overline{\mathrm{K}})$, is the quotient of $\mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}})$ by its subgroup of principal divisors, and we define $\mathrm{Pic}^0(\mathrm{C}/\overline{\mathrm{K}})$ to be the quotient of $\mathrm{Div}^0(\mathrm{C}/\overline{\mathrm{K}})$ by the subgroup of principal divisors. The Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $\mathrm{Pic}(\mathrm{C}/\overline{\mathrm{K}})$ and $\mathrm{Pic}^0(\mathrm{C}/\overline{\mathrm{K}})$ via its natural action on $\mathrm{Div}(\mathrm{C}/\overline{\mathrm{K}})$ and $\mathrm{Div}^0(\mathrm{C}/\overline{\mathrm{K}})$, and we let

$$\mathrm{Pic}(\mathrm{C}) = \mathrm{Pic}(\mathrm{C}/\overline{\mathrm{K}})^{\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})}, \qquad \mathrm{Pic}^0(\mathrm{C}) = \mathrm{Pic}^0(\mathrm{C}/\overline{\mathrm{K}})^{\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})},$$

that is the subgroups of elements invariant under $\mathrm{Gal}(\overline{K}/K)$.

1.5 Cubic hypersurfaces

Let S be a smooth n-dimensional cubic hypersurface over a field K, such that $S(K) \neq \varnothing$. Consider a K-line ℓ that is not contained in S. Then ℓ meets the hypersurface in exactly three points counting multiplicity over $\overline{K}$, and if two of them are K-rational so is the third.

These observations allow us, when we have some K-rational points of $S(K)$, to use secant and tangent constructions to obtain new ones. An interesting question is how big is the smallest set of K-rational points that generates all other points through this process. In the case that S is a curve defined over a number field, the Mordell–Weil Theorem asserts that this set is finite, but it is still unknown if it can be arbitrarily large. There is a fundamental difference between curves and varieties of higher dimension, concerning a possible generalisation of the composition law; the latter can contain lines as subvarieties.

Let $S \subseteq \mathbb{P}^{n+1}$ be a smooth n-dimensional cubic variety over a field K, such that $S(K) \neq \varnothing$, and $n \geqslant 2$. Three points $P, Q, R \in S(K)$ (not necessarily distinct) are called **collinear** if:

1. P, Q, R lie on a K-line belonging to S, or
2. $P + Q + R$ is the intersection cycle of S with a K-line ℓ in $\mathbb{P}^{n+1}$.

By the latter we mean that the intersection of S and ℓ is exactly P, Q and R counting multiplicities. If P, Q, R are collinear, we write $R = P \circ Q$ (we remark that the order of P, Q and R does not matter). This composition law

has an obvious problem. Suppose that $n \geqslant 3$, and the field K is not $\mathbb{F}_2$. As $K \neq \mathbb{F}_2$, any K-line contains more than 3 points. Now, suppose there exists a K-line ℓ, such that $\ell \subseteq S$, and choose two points P and Q on that line. For any other point $A \in \ell$ we have that $P \circ Q = A$. Thus, $\circ$ is a (multivalued) composition law on $S(K)$, which is a great difference from the elliptic curve case, as we cannot hope for an analogue of the Mordell–Weil group.

1.5.1 Lines on Cubic Hypersurfaces

The arrangement of lines on a cubic surface was well-understood in the 19th century. In general, the theory of lines on a cubic surface was first studied in correspondence between Cayley and Salmon. Specifically, Cayley was the first to notice that a definite number of lines lie on the surface and then Salmon showed that that number was indeed 27. Their results were first published independently in 1849. Their combined result is known as the Cayley–Salmon Theorem.

Theorem 1.5.1 (Cayley–Salmon)**.** *Let $S \subset \mathbb{P}^3$ be a smooth cubic surface over a field K. Then S contains precisely* 27 *lines defined over $\overline{K}$.*

Proof. We refer the reader to [6, Chapter V.4]. □

Example 1.5.2. Consider the following cubic surface

$$S \ : \ x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$$

in $\mathbb{P}^3$ over $\mathbb{Q}$. Let ζ be a primitive cube root of unity. Observe that

$$x_0 = -\zeta^i x_1, \qquad x_2 = -\zeta^j x_3$$

defines a line that lies on S, for $0 \leq i, j \leq 2$. This gives 9 lines. Another 9 lines are given by

$$x_0 = -\zeta^i x_2, \qquad x_1 = -\zeta^j x_3,$$

and yet another 9 are given by

$$x_0 = -\zeta^i x_3, \qquad x_1 = -\zeta^j x_2.$$

The Cayley–Salmon Theorem says that these are all the lines on S.

By contrast a smooth cubic hypersurface of dimension $n \geqslant 3$ contains infinitely many lines. Indeed, let $S \subset \mathbb{P}^{n+1}$ be a smooth cubic hypersurface of dimension $n \geqslant 2$. The lines on S are parametrized by the points of the **Fano variety** $F(S)$. If $n = 2$ (i.e. S is a cubic surface) then $F(S)$ consists of 27 points. However if $n \geqslant 3$ then $F(S)$ is a smooth projective variety of dimension $2n - 4$. For this we refer to [4].

Example 1.5.3. Let K be a field, and let $S \subset \mathbb{P}^4$ be the cubic threefold

$$S \ : \ x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0\,.$$

We assume that the characteristic of K is not 3. In this case S is smooth. The Fano variety $F(S)$ has dimension 2 and so S has infinitely many lines defined over $\overline{K}$. However, we can easily deduce this fact using the Cayley–Salmon Theorem. Let $\lambda \in \overline{K}$, $\lambda^3 \neq -1$. Let Π_λ be the hyperplane

$$\Pi_\lambda \ : \ x_4 = \lambda x_3.$$

Then $S \cap \Pi_\lambda$ is a cubic surface with equations

$$x_4 = \lambda x_3, \qquad x_0^3 + x_1^3 + x_2^3 + (1+\lambda^3)x_3^3 = 0\,.$$

The condition $\lambda^3 \neq -1$ ensures that this is smooth. Hence $S \cap \Pi_\lambda$ has 27 lines over $\overline{K}$. Let us denote the set of these 27 lines on $S \cap \Pi_\lambda$ by A_λ. Suppose $\lambda \neq \mu$. Then any line in $A_\lambda \cap A_\mu$ is contained in $S \cap \Pi_\lambda \cap \Pi_\mu$. This is the cubic curve

$$x_3 = x_4 = 0, \qquad x_0^3 + x_1^3 + x_2^3 = 0.$$

This curve is irreducible and does not contain lines, so $A_\lambda \cap A_\mu = \emptyset$. As $\overline{K}$ is infinite, we see that

$$\bigcup_{\lambda \in \overline{K},\, \lambda^3 \neq 1} A_\lambda$$

is an infinite set of lines on S.

1.5.2 Eckardt Points

In this section S denotes a smooth cubic surface $\subset \mathbb{P}^3$ defined over K.

Definition 1.5.4. Let $P \in S(\overline{K})$. Let $T_P S$ be the tangent plane to S at P. We say that P is an **Eckardt point** if $T_P S \cap S$ is the union of three $\overline{K}$-lines passing through P.

We shall need the following well-known result. For a proof, see [16, Lemma 2.2].

Lemma 1.5.5. *Let ℓ be an $\overline{K}$-line contained in S. If* $\mathrm{char}(()\mathrm{K}) \neq 2$*, then ℓ contains at most* 2 *Eckardt points. If* $\mathrm{char}(\mathrm{K}) = 2$*, then ℓ contains at most* 5 *Eckardt points.*

1.6 Polynomial Equations

We recall a theorem that settles a conjecture made by Artin in 1935, namely whether finite fields are quasi-algebraically closed. Specifically, the theorem discusses the number of solutions of a specific system of polynomial equations over a finite field. This was proven by Chevalley in 1936, and a refined version was proven by Warning in the same year.

Theorem 1.6.1 (Chevalley–Warning Theorem)**.** *Let $\mathbb{F}$ be a finite field of characteristic p and let $\{f_i\}_{i=1}^{r} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be polynomials of degree $d_i < n$ such that the number of variables satisfies*

$$n > \sum_{i=1}^{r} d_i \,.$$

Consider the system of polynomial equations:

$$f_i(x_1, \ldots, x_n) = 0, \qquad i = 1, \ldots, r. \tag{1.1}$$

The number of common solutions of these equations is divisible by p.

Proof. Let $q = p^n = \#\mathbb{F}$. It is a well-known fact that if $i < q - 1$, then

$$\sum_{\alpha \in \mathbb{F}} \alpha^i = 0.$$

Therefore, the sum over all $\beta \in \mathbb{F}^n$ of any polynomial of degree less that $n(q-1)$ also vanishes. So, this leads to:

$$\sum_{\beta \in \mathbb{F}^n} (1 - f_1^{q-1}(\beta)) \cdot \ldots \cdot (1 - f_r^{q-1}(\beta)) \equiv 0 \pmod{p}. \tag{1.2}$$

On the other hand, as $\#\mathcal{U}(\mathbb{F}) = q - 1$, we have that for an $\alpha \in \mathbb{F}$:

$$f^{q-1}(\alpha) = \begin{cases} 0 & \text{if } f(\alpha) = 0 \\ 1 & \text{otherwise} \end{cases}$$

Thus, the left hand side of Equivelance (1.2) is exactly the number of solutions of (1.1). □

1.7 Number Fields

An **algebraic number field**, or simply number field, is a field of finite degree over the field $\mathbb{Q}$ of rational numbers. In other words, a number field K is a finite extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$, for some $\alpha \in K$. Hence, K is a field that contains $\mathbb{Q}$ and a finite dimensional vector space over $\mathbb{Q}$. The dimension of K as a vector space over $\mathbb{Q}$ is simply called the **degree** of K. A **valuation** $|\cdot|$ on K is a function from K to the non-negative real numbers such that, for all $\alpha, \beta \in K$:

1. $|\alpha| = 0$ if and only if $\alpha = 0$,
2. $|\alpha\beta| = |\alpha||\beta|$,
3. there is a constant $C > 0$ such that $|\alpha + 1| \leqslant C$ whenever $|\alpha| = 1$.

The trivial valuation on K is that for which $|\alpha| = 1$ for all $\alpha \neq 0$. A valuation $|\cdot|$ on K is **non-archimedean** if condition (3) holds for $C = 1$. In other words if for all $\alpha, \beta \in K$ we have

$$|\alpha + \beta| \leqslant \max\{|\alpha|, |\beta|\}.$$

Two valuations $|\cdot|_1$, $|\cdot|_2$ on the same field are equivalent if there is $c > 0$ so that, for all $\alpha \in K$:

$$|\alpha|_1 = |\alpha|_2^c.$$

Trivially, every valuation is equivalent to one with $C = 2$. For such a valuation it can be shown that

$$|\alpha + \beta| \leqslant |\alpha| + |\beta|.$$

A **place** on a number field is an equivalence class of its valuations.

1.7.1 Weak Approximation

Lemma 1.7.1. *Let $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be non trivial inequivalent valuations of a field K, then there is an element $\alpha \in K$ such that*

$$\begin{cases} |\alpha|_1 > 1 \\ |\alpha|_i < 1, \quad i \neq 1. \end{cases}$$

Proof. First let $n = 2$. Because $|\cdot|_1$ and $|\cdot|_2$ are inequivalent, there are elements b and c such that

$$\begin{cases} |b|_1 < 1, \quad |b|_2 \geqslant 1 \\ |c|_1 \geqslant 1, \quad |c|_2 < 1. \end{cases}$$

Now $a = \frac{c}{b}$ has the required properties.

We proceed by induction assuming that the lemma is true for $n - 1$

valuations. There exist elements b, c such that

$$\begin{cases} |b|_1 > 1, \quad |b|_i < 1, \quad i = 2, 3, \ldots, n-1 \\ |c|_1 < 1, \quad |c|_n > 1. \end{cases}$$

If $|b|_n \leqslant 1$, then $a = cb^r$ works for sufficiently large r. If $|b|_n > 1$, then $a_r = \frac{cb^r}{1+b^r}$ works for sufficiently large r, because $\frac{b^r}{1+b^r}$ converges to 0 or 1 according as $|b| < 1$ or $|b| > 1$. □

Lemma 1.7.2. *In the situation of the last lemma, there exists an element of K that is close to 0 for $|\cdot|_i$, $i = 2, \ldots, n$.*

Proof. Choose a as in Lemma 1.7.1, and consider $a_r = \frac{a^r}{1+a^r}$. Then

$$|a_r - 1|_1 = \frac{1}{|1 + a^r|_1} \leqslant \frac{1}{|a|_1^r - 1} \to 0$$

as $r \to \infty$. For $i \geqslant 2$,

$$|a_r|_i = \frac{|a|_i^r}{|1 + a|_i^r} \leqslant \frac{|a|_i^r}{1 - |a|_i^r} \to 0$$

as $r \to 0$. □

Theorem 1.7.3. *Let $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be non trivial inequivalent valuations of a field K, and let $a_1, \ldots, a_n$ be elements of K. For any $\varepsilon > 0$, there is an element $a \in K$ such that $|a - a_i|_i < \varepsilon$ for all i.*

Proof. Choose b_i, $i = 1, \ldots, n$, close to 1 for $|\cdot|_i$ and close to 0 for $|\cdot|_j$, $j \neq i$. Then

$$a = a_1 b_1 + \cdots + a_n b_n$$

works. □

1.7.2 Adèles

Let K be a global field. For each normalised valuation $|\cdot|_v$ of K, let K_v be the completion of K. If $|\cdot|_v$ is non archimedean we denote by $\mathcal{O}_v$ the ring of integers of K_v. The **adèle ring** $\mathbb{A}_K$ of K is the topological ring whose underlying topological space is the restricted product of the K_v with respect to the $\mathcal{O}_v$ and where addition and multiplication are defined component wise:

$$(\alpha\beta)_v = \alpha_v\beta_v \quad (\alpha+\beta)_v = \alpha_v + \beta_v \quad \alpha,\beta \in \mathbb{A}_K. \tag{1.3}$$

It is readily verified that:

1. this definition makes sense, i.e. if $\alpha, \beta \in \mathbb{A}_K$, then $\alpha\beta$, $\alpha+\beta$ whose components are given by Equation (1.3) are also in $\mathbb{A}_K$ and,

2. addition and multiplication are continuous in the $\mathbb{A}_K$-topology, so $\mathbb{A}_K$ is a topological ring as asserted.

$\mathbb{A}_K$ is locally compact because the K_v are locally compact and the $\mathcal{O}_v$ are compact.

There is a natural mapping of K into $\mathbb{A}_K$ which maps $\alpha \in K$ into the adele everyone of which components is α: this is an adele because $\alpha \in \mathcal{O}_v$ for almost all v. The map is an injection because the map of K into K_v is an injection. The image of K under this injection is the ring of **principal adeles**. It will cause no trouble to identify K with the principal adeles, so we shall speak of K as a subring of $\mathbb{A}_K$.

Let $\hat{\mathbb{Z}}$ be the profinite completion of the integers, i.e. the inverse limit:

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

We remark that, by the Chinese remainder theorem, $\hat{\mathbb{Z}}$ is isomorphic to the product of all the rings of p-adic integers. The **ring of integral adèles** $\mathbb{A}_{\mathbb{Z}}$ is the product $\mathbb{A}_{\mathbb{Z}} = \mathbb{R} \times \hat{\mathbb{Z}}$. Let K be a number field. The ring of adeles $\mathbb{A}_K$ of K is the tensor product:

$$\mathbb{A}_K = K \otimes_{\mathbb{Z}} \mathbb{A}_{\mathbb{Z}}.$$

1.7.3 The Brauer Group of Field

In this Section we follow Serre's article [15] to define the Brauer group of a field and study it for local fields. Let K be a field. The easiest way to define the **Brauer group** $\mathrm{Br}(K)$ may be to define it in terms of Galois cohomology

$$\mathrm{Br}(K) = H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*),$$

where $\overline{K}$ is the separable closure of K.

Now let K be a non-archimedean local field (by which we mean a finite extension of $\mathbb{Q}_p$ for some prime p). We follow Serre [15] in defining the invariant map $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$. Write $K_{nr} \subset \overline{K}$ for the maximal unramified extension of K. As $\mathrm{Gal}(K_{nr}/K)$ is a quotient of $\mathrm{Gal}(\overline{K}/K)$, we have a natural map

$$H^2(\mathrm{Gal}(K_{nr}/K), K_{nr}^*) \to \mathrm{Br}(K)$$

obtained by inflation. This inflation map turns out to be an isomorphism [15, Theorem 1], and we shall henceforth identify $\mathrm{Br}(K)$ with the cohomology group on the left. The Galois group $\mathrm{Gal}(K_{nr}/K)$ is isomorphic topologically

to $\widehat{\mathbb{Z}}$. Then, the valuation map $v : K_{nr}^* \to \mathbb{Z}$ defines a map

$$Br(K) \cong H^2(\mathrm{Gal}(K_{nr}/K), K_{nr}^*) \to H^2(\widehat{\mathbb{Z}}, \mathbb{Z}),$$

which will also be denoted by v. This v is an isomorphism [15, Theorem 2].

Let us consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

of $\widehat{\mathbb{Z}}$-modules with trivial action. The module $\mathbb{Q}$ has trivial cohomology, since it is uniquely divisible, and so the coboundary

$$\delta : H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to H^2(\widehat{\mathbb{Z}}, \mathbb{Z})$$

is an isomorphism. On the other hand,

$$H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}).$$

as $\widehat{\mathbb{Z}}$ is acting trivially. Hence, we have the isomorphism,

$$\delta^{-1} : H^2(\widehat{\mathbb{Z}}, \mathbb{Z}) \to \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})\,.$$

Finally, define

$$\gamma : \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}, \qquad \varphi \mapsto \varphi(1)\,.$$

We define **local invariant map** $\mathrm{inv_K} : \mathrm{Br(K)} \to \mathbb{Q}/\mathbb{Z}$ as the composition $\gamma \circ \delta^{-1} \circ v$.

For $K = \mathbb{C}$, the Brauer group $\mathrm{Br}(\mathbb{C})$ is clearly trivial and we define $\mathrm{inv}_{\mathbb{C}} = 0$. For $K = \mathbb{R}$ a similar construction gives an invariant map

$$\mathrm{inv}_{\mathbb{R}} : \mathrm{Br}(\mathbb{R}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}.$$

Finally, let K be a number field, and Ω the set of places of K. For a place $v \in \Omega$ we shall write inv_v for inv_{K_v}. The **Hasse reciprocity law** states that the following sequence of abelian groups is exact:

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

Here the third map is the sum of local invariants $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$.

1.7.4 Brauer-Manin Obstruction

In this section we recall some facts about the Brauer–Manin obstruction; for further details on the Brauer–Manin obstruction see [18, Section 5.2].

Let X be a smooth, projective variety over a number field K. Let $\mathrm{Br}(X)$ be the Brauer group of X and denote by $\mathrm{Br}_0(X)$ the image of $\mathrm{Br}(K)$ in $\mathrm{Br}(X)$. Consider the pairing:

$$\langle\ ,\ \rangle : \mathrm{Br}(X) \times X(\mathbb{A}_K) \to \mathbb{Q}/\mathbb{Z}, \qquad \langle A, (P_v)\rangle = \sum_{v \in \Omega} \mathrm{inv}_v(A(P_v)).$$

This is the **adelic Brauer-Manin pairing** and satisfies the following properties:

(i) If $A \in \mathrm{Br}_0(X) \subset \mathrm{Br}(X)$ 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 $A \in \mathrm{Br}(X)$.

(iii) For any $A \in \mathrm{Br}(X)$, the map

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

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

We define:

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

By the above we know that:

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

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

We shall give an example of a cubic surface that fails the weak approximation.

Example 1.7.4. Let

$$S : x^3 + y^3 + z^3 - 2w^3 = 0.$$

Let $(x : y : z : w) \in S(\mathbb{Q})$ be a point; without loss of generality x, y, z, w are integers with greatest common divisor 1. Then we have that one of x, y and z is divisible by 6; for a proof, see [7]. This means that this surface fails weak approximation as it cannot have a rational point close to both $(1 : 0 : 1 : 1) \in S(\mathbb{Q}_2)$ and and $(0 : 1 : 1 : 1) \in S(\mathbb{Q}_3)$.

Ideally, we would like to know if all the restrictions are the ones imposed by the Brauer-Manin obstruction. Although that is the case in the aforementioned example, it is not known whether this holds for all smooth cubic surfaces.

In this thesis, we shall use the following conjecture of Colliot-Thélène; see [16].

Conjecture 1.7.5 (Colliot-Thélène)**.** *Let X be a smooth, projective, geometrically rational surface over a number field K. Then the Brauer-Manin obstruction is the only one to weak approximation on X.*

The term **geometrically rational** means that X is birational to $\mathbb{P}^2$ over $\overline{K}$. It is known that smooth cubic surfaces are geometrically rational [8, Section 5.3].

1.8 Bertini's Theorem

The **dual space** of $\mathbb{P}^n$ parametrizes hyperplanes in $\mathbb{P}^n$ and is denoted by $\mathbb{P}^{n*}$. It is canonically isomorphic to $\mathbb{P}^n$ by identifying $[a_0 : a_1 : \cdots : a_n]$ with the hyperplane

$$a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0.$$

By a **linear system of hyperplanes** in $\mathbb{P}^n$ we mean a linear subvariety of $\mathbb{P}^{n*}$.

Example 1.8.1. Let $P = [p_0 : p_1 : \cdots : p_n] \in \mathbb{P}^n$. The set of hyperplanes

passing through P is a linear system:

$$L_P = \{[a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^{n*} \ : \ p_0a_0 + \cdots + p_na_n = 0\}.$$

Note that as a subvariety of $\mathbb{P}^n$, the linear system L_P has dimension $n-1$ and is in fact isomorphic to $\mathbb{P}^{n-1}$. This is easier to see if we move the point P to $[1 : 0 : 0 : \cdots : 0]$ and so

$$L_P = \{[0 : a_1 : \cdots : a_n] \ : \ [a_1 : \cdots : a_n] \in \mathbb{P}^{n-1}\}.$$

By this we mean that the hyperplanes through P are the ones of the form

$$a_1x_1 + \cdots + a_nx_n = 0$$

where $[a_1 : \cdots : a_n] \in \mathbb{P}^{n-1}$.

Likewise if P, Q are distinct points, we can define the linear system $L_{P,Q} = L_P \cap L_Q$ of hyperplanes passing through P, Q. This has dimension $n-2$ and is isomorphic to $\mathbb{P}^{n-2}$. It is easy to see this by moving P to $[1 : 0 : \cdots : 0]$ and Q to $[0 : 1 : 0 : \cdots : 0]$, and then

$$L_{P,Q} = \{[0 : 0 : a_2 : \cdots : a_n] \ : \ [a_2 : \cdots : a_n] \in \mathbb{P}^{n-2}\}.$$

If P, Q, R are distinct points then $L_{P,Q,R}$ is isomorphic to $\mathbb{P}^{n-3}$ unless P, Q, R are collinear, in which case it is just $L_{P,Q}$.

Let $V \subset \mathbb{P}^n$ be a smooth variety over a field K. Let $L \subset \mathbb{P}^{n*}$ be a linear system of hyperplanes defined over K, and let $H \in L(K)$. Then $V \cap H$ is a hyperplane section of V. Is there such an $H \in L(K)$ so that $V \cap H$ is smooth?

This is a question that can be answered with the help of a version of Bertini's Theorem. This version of Bertini's theorem is not a powerful as other versions of it, but has the advantage that it applies to fields of arbitrary characteristic; for a proof see [13].

Theorem 1.8.2 (Bertini's Theorem)**.** *Let K be a field. Let $V \subset \mathbb{P}^n$ be a smooth variety over K, and let $L \subset \mathbb{P}^{n*}$ be a linear system of hyperplanes defined over K of positive dimension. Then there is a Zariski dense open subset $L' \subset L$ such that for every $H \in L'$, the hyperplane section $H \cap V$ is smooth away from the base locus $(\cap L) \cap V$.*

The **base locus** is the set of points in V contained in all the hyperplanes in L.

Example 1.8.3. Let P, $Q \in V \subset \mathbb{P}^n$ and consider the linear system $L_{P,Q}$ of hyperplanes passing passing through P and Q as above. Then the intersection of all the hyperplanes in $L_{P,Q}$ is the line $\ell_{P,Q}$ connecting P, Q. If $\ell_{P,Q} \subset V$, then $\ell_{P,Q}$ is the base locus. If $\ell_{P,Q} \not\subset V$, then $\ell_{P,Q} \cap V$ is the base locus, and this is a finite set.

Lemma 1.8.4. *Let $f \in K[x_0, \ldots, x_n]$ be a non-zero polynomial where K is an infinite field. There are values $a_0, \ldots, a_n \in K$ such that $f(a_0, a_1, \ldots, a_n) \neq 0$.*

Proof. We prove this by induction on $n \geqslant 0$. If $n = 0$ then f is a polynomial in one variable and has finitely many roots in K. As K is infinite, there exists $a_0 \in K$ so that $f(a_0) \neq 0$.

Suppose $n > 0$ and write

$$f = \sum_{j=0}^{m} g_j(x_1, \ldots, x_n) x_0^j.$$

As f is non-zero, at least one of the g_j is non-zero, and so by the inductive hypothesis $g_j(a_1, \ldots, a_n) \neq 0$ for some $a_1, \ldots, a_n \in K$. Hence, $f(x_0, a_1, \ldots, a_n)$ is a non-zero polynomial in $K[x_0]$, and therefore there exists $a_0 \in K$ such that $f(a_0, a_1, \ldots, a_n) \neq 0$. □

If K is a finite field, then the above lemma does not have to hold. For example in $K = \mathbb{F}_p$ where p is a prime, $f = x_0^p - x_0$ takes only the value 0.

Lemma 1.8.5. *Let K be an infinite field. Let A be a dense Zariski open subset of $\mathbb{P}^m$ ($m > 0$) defined over K. Then $A(K) \neq \emptyset$.*

Proof. We can write $A = \mathbb{P}^m - Z$ where Z is a Zariski closed subset defined over K. The set Z is given by

$$Z \ : \ f_1 = f_2 = \cdots = f_r = 0,$$

where f_j are homogeneous non-zero polynomials (otherwise $Z = \mathbb{P}^n$ contradicting the fact that A is Zariski dense). Hence by Lemma 1.8.4 we can find $P = [a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^m(K)$ such that $f_1(P) \neq 0$. Thus $P \in A(K)$. □

Corollary 1.8.6. *Let K be an infinite field, and let $V \subset \mathbb{P}^n$ be a smooth variety over K, where $n \geqslant 3$. Let P, $Q \in V(K)$ and denote the line joining P, Q by $l_{P,Q}$. Suppose $l_{P,Q} \not\subset V$. Then there is a hyperplane H defined over K such that P, $Q \in H$ and $H \cap V$ is smooth.*

Proof. We apply Bertini's Theorem to the linear system $L_{P,Q}$ which is isomorphic to $\mathbb{P}^{n-2}$. Then there is a Zariski dense open subset $L' \subset L$ such that if $H \in L'$ then $H \cap V$ is smooth away from the base points. Since $l_{P,Q} \not\subset V$, we know the set of base points is finite, given by $l_{P,Q} \cap V = \{P_1, P_2, \ldots, P_r\}$

where $P_1 = P$ and $P_2 = Q$. A hyperplane H has intersection $H \cap V$ singular at P_j if and only if H is the tangent hyperplane T_{V,P_j} to V at P_j. Let

$$L'' = L' - \{T_{V,P_1}, \ldots, T_{V,P_r}\}.$$

This is also a Zarski dense open subset of $L_{P,Q}$ as we removed finitely many points from L'. Using Lemma 1.8.5 we have $L''(K) \neq \emptyset$. Let $H \in L''(K)$. Then $H \cap V$ is smooth and H contains P, Q. □

Corollary 1.8.7. *Let K be an infinite field, and let $V \subset \mathbb{P}^n$ be a smooth variety over K, where $n \geqslant 4$. Let l be a K-line contained in V. Then there is a hyperplane H defined over K such that $l \subset H$ and $H \cap V$ is smooth.*

Proof. This proof is a modification of the previous proof. Let P, Q be any two K-points on l and consider the linear system $L_{P,Q}$ which is isomorphic to $\mathbb{P}^{n-2}$. Clearly every $H \in L_{P,Q}$ contains l. Again there is a Zariski dense open subset $L' \subset L$ such that if $H \in L'$ then $H \cap V$ is smooth away from the base locus, which is now l. The hyperplane H is singular at $P \in l$ if and only if $H = T_{V,P}$. Let W be the image in L of the map

$$l \to L, \qquad P \mapsto T_{V,P}.$$

As l has dimension 1, the image W has dimension at most 1. But L' has dimension $n - 2 \geqslant 2$ (as we assumed that $n \geqslant 4$ in this corollary). Let

$$L'' = L' \backslash W.$$

This must be Zariski dense open in L, and every $H \in L$ satisfies $H \cap V$ is

smooth. We can complete the proof as before. □

Chapter 2

Properties of $H_S(K)$

2.1 Background

Let $S \subset \mathbb{P}^{n+1}$ be a smooth cubic hypersurface over a field K of dimension $n \geqslant 1$. The tangent and secant operations give us new points from old ones. We would like to understand the **Mordell–Weil problem** for $S(K)$, which asks whether $S(K)$ can be generated by repeated tangent and secant operations starting from a finite set. This problem was posed by Segre [14] for cubic surfaces over $\mathbb{Q}$, and by Manin [10] for general cubic hypersurfaces over fields K that are finitely generated over their prime subfields (e.g. number fields, $\mathbb{F}_p(t)$).

Let us give a formal statement of the problem. Let B be a subset of $S(K)$. Define the following sequence:

$$B_0 \subseteq B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots \subseteq S(K),$$

where $B_0 = B$, and for every $i \geqslant 0$, we let B_{i+1} be the set of points $R \in S(K)$

such that:

- either $R \in B_i$, or
- there exists a K-line $\ell \not\subset S$ and points P, $Q \in B_i$, such that $\ell \cdot S = P + Q + R$.

We define the **Mordell–Weil span of** B, to be

$$\langle B \rangle_{MW} = \bigcup_{i=0}^{\infty} B_n.$$

We say that B **generates** $S(K)$ if $\langle B \rangle_{MW} = S(K)$.

Remark 2.1.1. Obviously, the Mordell-Weil span of a set B depends on the chosen field K. However, in an effort to simplify our notation we simply write $\langle B \rangle_{MW}$, omitting any reference to the field K.

We say that a subset B of $S(K)$ is a **Mordell–Weil generating set** for $S(K)$ if:

1. B generates $S(K)$, and
2. when A generates $S(K)$, then $\#B \leqslant \#A$.

We define the **Mordell–Weil rank** $r(S, K)$ of the cubic hypersurface S/K as the cardinality of such a set B. The Mordell–Weil problem for S/K can now be formally formulated as follows:

Mordell–Weil Problem. *Is there a* finite *Mordell–Weil generating set for* S/K*? Or equivalently, is* $r(S, K) < \infty$*?*

If K is a number field and S has dimension 1, then the answer is yes by the Mordell–Weil Theorem. For arbitrary dimension n and K a finite field the

answer is obviously yes. There are very few known cases for dimension $n \geqslant 2$, and K a number field.

Theorem 2.1.2. *(Siksek) et $S \subset \mathbb{P}^3$ be a cubic surface over a field K satisfying $\#K \geqslant 13$. Suppose S contains a skew pair of K-lines. Then $r(S, K) = 1$.*

Proof. We refer to [16, Theorem 1]. □

Due to the geometric nature of $r(S, K)$, it is very hard to compute it directly. In order to study $r(S, K)$ for cubic surfaces S, Siksek [16] introduced a group $H_S(K)$, which can yield a lower bound for $r(S, K)$. Here we generalize Siksek's construction to arbitrary dimension $n \geqslant 1$.

We define $G_S(K)$ to be the free abelian group generated by the K-rational points of S:

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

Let $G'_S(K)$ be the subgroup of $G_S(K)$ generated by the formal sums $P+Q+R$ with $P, Q, R \in S(K)$ **collinear**, i.e.:

(i) there is a K-line $\ell \nsubseteq S$, such that $\ell \cdot S = P + Q + R$, or

(ii) there is a K-line $\ell \subseteq S$, such that $P, Q, R \in \ell$.

The **degree map**

$$\deg : G_S(K) \to \mathbb{Z}$$

is defined by

$$\deg(\sum_{i=0}^{n} a_i P_i) = \sum_{i=0}^{n} a_i.$$

Moreover, let

$$G''_S(K) = \{D \in G'_S(K) \mid \deg(D) = 0\}$$

and

$$H_S(K) = G_S(K)/G''_S(K).$$

If $D \in G_S(K)$, then we denote the image of D in $H_S(K)$ by $[D]$. It is evident that the degree map is well-defined on $H_S(K)$, so we can define the group:

$$H^0_S(K) = \{[D] \in H_S(K) \mid \deg([D]) = 0\}.$$

Here, for an abelian group G, we denote the subgroup of points of order dividing m by $G[m]$.

Remark 2.1.3. Clearly, for any positive integer n, we have that

$$H_S(K)[n] \subseteq H^0_S(K).$$

We are interested in the case that $S(K) \neq \varnothing$, therefore the degree map is a well define epimorphism onto $\mathbb{Z}$ and $H^0_S(K)$ is its kernel, hence we have that

$$H_S(K)/H^0_S(K) \cong \mathbb{Z}. \tag{2.1}$$

It is unknown if for smooth cubic curve S over $\mathbb{Q}$ whether $r(S, \mathbb{Q})$ can be arbitrarily large. This is the famous question of whether ranks of elliptic curves can be arbitrarily large (Conjecture VIII.10.1 in Silverman's book [17]). For cubic surfaces over $\mathbb{Q}$ the same question has an affirmative answer.

Theorem 2.1.4. *(Siksek) Let $p_1, p_2, \ldots, p_s$ 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 $S = S_M$ be the cubic surface in $\mathbb{P}^3$ given by

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

Then

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

Proof. See [16], Theorem 2. □

Theorem 2.1.5. *(Siksek) Let $p_1, p_2, \ldots, p_s$ be distinct primes such that $p_i \equiv 1 \pmod 3$. Let $M = 3\prod p_i$ and let $S = S_M$ be the cubic surface in $\mathbb{P}^3$ given by*

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

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

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

Proof. See [16], Theorem 3. □

2.2 First Results

In this section, $S \subset \mathbb{P}^n$ ($n \geqslant 3$) denotes a smooth cubic hypersurface over a field K; we generalize several results of Siksek [16] for the case $n = 2$.

Lemma 2.2.1. *Let $\ell \subset S$ be a K-line. Let P, $Q \in \ell(K)$. Then $P - Q \in G'_S(K)$. In particular, $[P] = [Q]$ in $H_S(K)$.*

Proof. From the definition of $G'_S(K)$, we see that it contains $3P$ and $2P+Q$. Thus $P-Q = 3P-(2P+Q)$ is contained in the group $G'_S(K)$. Moreover, $P-Q$ has degree 0, so $P-Q \in G''_S(K)$. This shows that $[P-Q]=0$ in $H_S(K)$. □

Lemma 2.2.2. *Let $P \in S(K)$. If $Q \in (T_P \cap S)(K)$ is distinct from P, then the line joining P, Q is tangent to S at P, so that $2P+Q \in G'_S(K)$.*

Proof. We may choose an affine chart that contains P, Q. Without loss of generality we may also assume that $P=(0,0,\ldots,0)$, the tangent space is $x_n=0$ and $Q=(1,0,0,\ldots,0)$. Thus S is defined by the equation:

$$0 = f(x_1,x_2,\ldots,x_n) = x_n + q(x_1,x_2,\ldots,x_n) + c(x_1,x_2,\ldots,x_n),$$

for a homogeneous quadratic polynomial q and a homogeneous cubic polynomial c. Let ℓ be the line that joins P and Q. Therefore, ℓ has the parametrization $(t,0,0,\ldots,0)$. It is clear that this is contained in the plane $x_n=0$. If $\ell \subset S$ then the lemma follows from Lemma 2.2.1. So suppose $\ell \not\subset S$. The points of intersection of ℓ with S correspond to the solutions to the equation

$$0 = f(t,0,\ldots,0) = t^2 q(1,0,\ldots,0) + t^3 c(1,0,\ldots,0).$$

As this has a double root at $t=0$ (which corresponds to the point P on ℓ) we see that ℓ meets S with multiplicity $\geqslant 2$ at P. But ℓ meets S at Q also. Since ℓ meets S in exactly three points counting multiplicity, we have that $\ell \cdot S = 2P+Q$. Thus $2P+Q \in G'_S(K)$. □

The following theorem is a crucial part of our study of the group $H_S(K)$.

Theorem 2.2.3. *Suppose that $S(K)$ contains a K-line ℓ, and let $Q_0 \in \ell(K)$. Then, for all $P \in S(K)$ we have that $2P + Q_0 \in G'_S(K)$.*

Proof. Let $P \in S(K)$. By the definition of $G'_S(K)$, if $P \in \ell(K)$ there is nothing to prove. Hence, we may assume that $P \notin \ell(K)$. Let $T_P S$ be the tangent space of S at P. If $\ell \subset T_P S$, then $Q_0 \in T_P S$ and we complete the proof using Lemma 2.2.2. Thus suppose $\ell \not\subset T_P S$. Then ℓ and $T_P S$ intersect in a unique K-point Q, and this is contained in S as $\ell \subset S$. By Lemma 2.2.2 we have $2P + Q \in G'_S(K)$, and by Lemma 2.2.1 we have $Q_0 - Q \in G'_S(K)$. As $G'_S(K)$ is a group, it contains $2P + Q_0 = (2P + Q) + (Q_0 - Q)$. □

Corollary 2.2.4. *If $S(K)$ contains a K-line, then $H^0_S(K) = H_S(K)[2]$.*

Proof. From Remark 2.1.3, we only need to show that $H^0_S(K) \subseteq H_S(K)[2]$. Let $[D] \in H^0_S(K)$, for some $D = \sum_{i=0}^{n} a_i P_i \in G_S(K)$ with $\sum_{i=0}^{n} a_i = 0$. Since $S(K)$ contains a K-line, from Theorem 2.2.3 we have that, for all i, $2P_i + Q_0 \in G'_S(K)$ for some Q_0 on the K-line. Therefore,

$$\sum_{i=0}^{n} 2a_i P_i + \sum_{i=0}^{n} a_i Q_0 \in G'_S(K) \Rightarrow$$
$$2\sum_{i=0}^{n} a_i P_i = 2D \in G'_S(K),$$

and so $[D] \in H_S(K)[2]$. □

Corollary 2.2.5. *Let ℓ_1 and ℓ_2 be K-lines contained in S. Suppose $Q_1 \in \ell_1(K)$ and $Q_2 \in \ell_2(K)$. Then $Q_1 - Q_2 \in G'_S(K)$.*

Proof. From Theorem 2.2.3 we have that

$$2Q_1 + Q_2,\ 2Q_2 + Q_1 \in G'_S(K).$$

Therefore,

$$Q_1 - Q_2 = 2Q_1 + Q_2 - (Q_1 + 2Q_2) \in G'_S(K).$$

□

Theorem 2.2.6. *If K is algebraically closed, then for all $P \in S(K)$ we have that $3P \in G'_S(K)$.*

Proof. Using the same technique as in the proof of the previous theorem, we may take an affine chart and suppose that $P = (0, 0, \ldots, 0)$ and that $T_P S$ is given by $x_n = 0$. Any non-zero $a \in K^{n-1} \times \{0\}$ defines a line ℓ passing through P and contained in $T_P S$, with parametrization $t_a = t(a_1, a_2, \ldots, a_{n-1}, 0)$. The points of intersection of this line with S correspond to the roots of a polynomial

$$t^2 q(a_1, \ldots, a_{n-1}) + t^3 c(a_1, \ldots, a_{n-1}), \tag{2.2}$$

where q and c are respectively homogeneous quadratic and cubic. Since K is algebraically closed there are $a_1, \ldots, a_{n-1} \in K$, not all zero, so that $q(a_1, \ldots, a_{n-1}) = 0$. Now either $c(a_1, \ldots, a_{n-1}) = 0$ in which case ℓ is contained in S, or $c(a_1, \ldots, a_{n-1}) \neq 0$, so 0 is a triple root of (2.2). In either case we conclude that $3P \in G'_S(K)$. □

The following are immediate from the theorem.

Corollary 2.2.7. *If K is algebraically closed, then $H^0_S(K)$ is trivial.*

Proof. Since K is algebraically closed, $S(K)$ contains a K-line ℓ (see Subsection 1.5.1). From Corollary 2.2.4 we have that

$$H^0_S(K) = H_S(K)[2]. \tag{2.3}$$

On the other hand, from Theorem 2.2.3 we have that

$$H_S^0(K) = H_S(K)[3]. \tag{2.4}$$

The result follows from Equations (2.3) and (2.4). □

Corollary 2.2.8. *If K is algebraically closed, then $H_S(K) \cong \mathbb{Z}$.*

Proof. Immediate from Equation (2.1) and Corollary 2.2.7. □

2.2.1 Relation between $H_S^0(K)$ and $r(S, K)$

We say that $P_0 \in S(K)$ is K-**ternary** if there is a K-line $\ell \not\subset S$ such that $\ell \cdot S = 3P_0$. The following is Theorem 5 of [16].

Lemma 2.2.9. *Let P_0 be K-ternary. Let B be a generating set for $S(K)$. Then $\{[P - P_0] : P \in B\}$ generates $H_S^0(K)$. In particular, if p is a prime*

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

Proof. We follow the proof of Theorem 5 of [16] which is stated for cubic surfaces but the same argument applies in higher dimension. First note that by definition, $3P_0 \in G'_S(K)$. Suppose now that P, Q, $R \in S(K)$ are collinear. Then $P + Q + R \in G'_S(K)$ and so $[P - P_0] + [Q - P_0] + [R - P_0] = 0$.

Let $B_0 = B$ and let B_i be as defined in Section 2.1, so that $S(K) = \langle B \rangle_{MW} = \cup_{i=0}^{\infty} B_i$. Suppose $R \in B_1$. We will show that $[R - P_0]$ is in the subgroup generated by $\{[P - P_0] : P \in B\}$. But by definition of B_1, either $R \in B_0 = B$ or there are P, $Q \in B$ such that P, Q, R are collinear. In either case we see that $[R - P_0]$ is contained in the subgroup generated by $\{[P - P_0] : P \in B\}$.

Let us write B^* for the subgroup of $H^0_S(K)$ generated by $\{[P - P_0] : P \in B\}$. It follows from the above that $B_1^* \subseteq B_0^*$. But as $B_0 \subseteq B_1$ we have $B_1^* = B_0^*$. Similarly $B_2^* = B_1^*$ and so on. Hence $S(K)^* = B_0^* = B^*$. However, $S(K)^* = H^0_S(K)$. This shows that $\{[P - P_0] : P \in B\}$ generates $H^0_S(K)$. $\square$

2.3 $H_S(K)$ and Hyperplane Sections

Let $S \subset \mathbb{P}^{n+1}$ be a smooth cubic hypersurface of dimension n, over a field K. Let H be a hyperplane in $\mathbb{P}^{n+1}$ defined over K. Suppose that $S' := S \cap H$ is smooth. As H is isomorphic to $\mathbb{P}^n$, we can view S' as smooth cubic hypersurface of dimension $n-1$ defined over K and lying in $\mathbb{P}^n$.

Proposition 2.3.1. *The map $H_{S'}(K) \to H_S(K)$ given by sending the class $[P]$ in $H_{S'}(K)$ to the class $[P]$ in $H_S(K)$ for $P \in S'(K) \subseteq S(K)$ is a well-defined group homomorphism.*

Proof. It is clear from the definitions in the previous section that

$$G_{S'}(K) \subseteq G_S(K), \qquad G'_{S'}(K) \subseteq G'_S(K), \qquad G''_{S'}(K) \subseteq G''_S(K).$$

Since

$$H_S(K) := \frac{G_S(K)}{G''_S(K)}, \qquad H'_S(K) := \frac{G_{S'}(K)}{G''_{S'}(K)},$$

the proposition follows. $\square$

2.4 Universal Equivalence

To study $H_S(K)$ for local fields K, we need to quote and explain some results of Manin [10, Chapter II] on universal equivalence. Let S be a smooth

cubic variety over a field K (not assumed to be local for now). Let $\sim$ be an equivalence relation on $S(K)$. We say that $\sim$ is **admissible** if it is compatible with collinearity in the following sense: if both triples P_1, P_2, P_3 and P_1', P_2', P_3' are collinear, and if $P_1 \sim P_1'$ and $P_2 \sim P_2'$ then $P_3 \sim P_3'$.

Now let U_1, U_2 be two admissible relations on $S(K)$. We say that U_1 is **finer** than U_2 (and so U_2 is **coarser** than U_1) if whenever PU_1Q then PU_2Q. It is clear that every equivalence class of U_2 is a union of equivalence classes for U_1 and so U_2 has fewer or the same number of equivalence classes as U_1.

Proposition 2.4.1 (Manin)**.** *Among all admissible relations on $S(K)$ there is a unique finest admissible relation.*

Proof. This is Proposition 11.3 of Chapter II of [10]. □

The finest admissible relation on $S(K)$ is called **universal equivalence**, and denoted by U. We denote the set of equivalence classes by $S(K)/U$.

Theorem 2.4.2 (Manin)**.** *Let K be a local field. Let S be a smooth cubic hypersurface of dimension $n \geqslant 2$ over K. Then universal equivalence partitions $S(K)$ into finitely many equivalence classes. Moreover each equivalence class is open and closed in the topology induced by K.*

Proof. This is Theorem 16.1 and Corollary 16.1.1 and Corollary 16.1.3, Chapter II of [10]. □

We use Manin's Theorem 2.4.2 to make deductions regarding $H_S(K)$ for K a local field.

Lemma 2.4.3. *Let K be local field and let S be a smooth cubic hypersurface of dimension $n \geqslant 2$ over K. Then the map that sends a point $P \in S(K)$ to its*

class $[P] \in H_S(K)$ *is locally constant, where* $S(K)$ *has the topology induced by* K*, and its image is finite.*

Proof. We define the relation $P \sim P'$ on $S(K)$ to mean $[P] = [P']$ in $H_S(K)$. It is clear that this is an equivalence relation, and it follows immediately from the definitions that it is an admissible relation. Hence every equivalence class under $\sim$ is a union of equivalence classes under universal equivalence U. By Theorem 2.4.2 the equivalence classes under U are both open and closed in the topology induced by K, and there are only finitely many. Thus the same is true for the equivalence classes under $\sim$. This shows that the map $P \mapsto [P]$ is locally constant and its image is finite. □

Note that $H^0_S(K)$ is generated by differences $[P - Q] = [P] - [Q]$. The above lemma shows that $H^0_S(K)$ is finitely generated for K a local field, since there are finitely many possibilities for the classes $[P]$, $[Q]$. We would like to show that $H^0_S(K)$ is finite. For this it is enough to show that $[P-Q]$ has finite order for all P, $Q \in S(K)$.

Lemma 2.4.4 (Siksek)**.** *If* K *is a local field and* $S \subset \mathbb{P}^3$ *is a smooth cubic surface then* $H^0_S(K)$ *is finite.*

Proof. This is Theorem 8 of [16]. □

We are now ready to prove that $H^0_S(K)$ is finite for any smooth cubic hypersurface S of dimension $n \geqslant 2$ over a local field K.

Theorem 2.4.5. *Let* S *be a smooth cubic hypersurface* $\subset \mathbb{P}^n$ *where* $n \geqslant 3$*, defined over a local field* K*. Then* $H^0_S(K)$ *is finite.*

Proof. We shall prove the theorem by induction on $n \geqslant 3$. For $n = 3$ this is Lemma 2.4.4. Suppose $n > 3$. We know from the above that we must

prove that $[P-Q]$ has finite order in $H_0(K)$ for any P, $Q \in S(K)$. Let $\ell_{P,Q}$ be the line joining P, Q. If $\ell_{P,Q} \subset S$ then we already know that $[P] = [Q]$ by Lemma 2.2.1. Thus suppose that $\ell_{P,Q} \not\subset S$. By Corollary 1.8.6 there is a hyperplane H defined over K such that $S' := S \cap H$ is smooth, and P, $Q \in H$. Thus P, $Q \in S'(K)$. Now S' has dimension $n-1$. By the inductive hypothesis, $[P-Q]$ has finite order in $H^0_{S'}(K)$. It follows from Proposition 2.3.1 that $[P-Q]$ has finite order in $H^0_S(K)$. This completes the proof. □

2.5 Weak Approximation and $H_S(K)$

Theorem 2.5.1. *Let K be a number field and Ω its places. Let Σ be a finite subset of Ω and write $\mathbb{A}_K^{\Sigma}$ for the adèles of K with Σ removed. Let $S \subset \mathbb{P}^n$ be a smooth cubic hypersurface defined over K. Further, suppose that the image of $S(K)$ is dense in $S(\mathbb{A}_K^{\Sigma})$. For any finite subset, Δ, of $\Omega \smallsetminus \Sigma$ the diagonal map:*

$$\delta \ : \ H^0_S(K) \to \prod_{u \in \Delta} H^0_S(K_u)$$

is a surjective homomorphism.

Proof. We know that δ is a homomorphism and that $\prod_{u\in\Delta} H^0_S(K_u)$ is generated by elements of the form $([P_u - Q_u])_{u\in\Delta}$. Therefore, it suffices to show that all the elements of this form are contained in the image of δ. We have that the image of $S(K)$ is dense in $\prod_{u\in\Delta} S(K_u)$ and that the map that sends a point of $S(K)$ to its equivalence class in $H_S(K)$ is locally constant. As Δ is finite, we can find P and $Q \in S(K)$ that sufficiently approximate $(P_u)_{u\in\Delta}$ and $(Q_u)_{u\in\Delta}$. Then, these points define a class $[P-Q] \in H^0_S(K)$ that has the desired image. □

2.6 $H_S(\mathbb{R})$

We will now consider the group $H_S(K)$, where K is a local field of characteristic zero. As we have already considered the case where K is an algebraically closed field, the cases that we should also consider are $K = \mathbb{R}$ and $K = \mathbb{Q}_p$. We shall start with the case that $K = \mathbb{R}$.

Lemma 2.6.1. *Let $S \subset \mathbb{P}^n$ be a smooth cubic hypersurface over $\mathbb{R}$ (where $n \geqslant 2$). Then $S(\mathbb{R})$ has either one or two connected components, in the topology induced by $\mathbb{R}$.*

Proof. We make use of Harnack's curve theorem (Theorem 1.3.3) which asserts that a plane cubic curve has at most 2 connected components.

Suppose that there exists a smooth cubic hypersurface $S \subset \mathbb{P}^n$ that has at least 3 connected components, where by Harnack's theorem we may suppose $n \geqslant 3$. Let P, Q, $R \in S$, such that P, Q and R are all in different connected components of the hypersurface. Let $\Pi \subset \mathbb{P}^n$ be the 2-dimensional linear subvariety that passes through these points if these points are not collinear, or, otherwise, any such 2-dimensional linear subvariety that contains the unique line they lie on. Then $\Pi \cap S(\mathbb{R})$ is a plane cubic curve with at least 3 connected components, which contradicts Harnack's curve theorem. □

Now, we shall give examples to show that there are real cubic n-folds, with precisely one and precisely two connected components, for all dimensions $n \geqslant 2$.

Lemma 2.6.2. *Let S_n be the smooth cubic n-fold given by $\sum_{i=0}^{n+1} x_i^3 = 0$, $P = [a_0 : a_1 : \ldots : a_{n+1}]$ a point in $S_n(\mathbb{R})$ and $0 \leqslant i, j \leqslant n+1$ with $i \neq j$. Then the point $Q = [b_0 : b_1 : \ldots : b_{n+1}]$, where $b_i = 0$, $b_j = (a_i^3 + a_j^3)^{\frac{1}{3}}$ and for all other*

k, $b_k = a_k$, is a point in $S_n(\mathbb{R})$ and there is a path in the n-fold connecting P and Q.

Proof. If $a_i = 0$, there is nothing to prove. Suppose that $a_i \neq 0$. For $t \in [0, 1]$ let $P(t) = [x_0(t) : x_1(t) : \ldots : x_{n+1}(t)]$, where $x_i = (a_i^3 - (a_i t)^3)^{\frac{1}{3}}$, $x_j = (a_j^3 + (a_i t)^3)^{\frac{1}{3}}$ and for all other k, $x_k(t) = a_k$. Then $P(t)$ is a path in $S_n(\mathbb{R})$ form P to Q. □

Corollary 2.6.3. *Let S_n be the n-fold defined in Lemma 2.6.2. $S_n(\mathbb{R})$ has exactly one connected component.*

Proof. For every point P in the n-fold there is a path that connects it with the point $[0 : 0 : \ldots : 0 : 1 : -1]$. □

Lemma 2.6.4. *Let S'_n be the algebraic set given by the cubic polynomial*

$$F(x) = 6x_0^3 - 11x_{n+1}x_0^2 + 6x_{n+1}^2 x_0 - x_{n+1}^3 + \sum_{i=1}^{n} x_0 x_i^2 = 0.$$

Then $S'_n(\mathbb{R})$ has 2 connected components.

Proof. Using lemma 2.6.1, it suffices to show that $S'_n(\mathbb{R})$ is not connected. If we dehomogenise F by letting $x_0 = 1$ we get

$$f = (1 - x_{n+1})(2 - x_{n+1})(3 - x_{n+1}) + \sum_{i=1}^{n} x_i^2 = 0.$$

The hyperplane $x_{n+1} = 2.5$ doesn't meet S, as if it did we would have $0.375 + \sum_{i=1}^{n} x_i^2 = 0$, which is absurd. On the other hand, the hyperplanes $x_{n+1} = 2$ and $x_{n+1} = 3$ meet the n-fold at exactly $[0 : \ldots : 0 : 2]$ and $[0 : \ldots : 0 : 3]$ respectively. This forces the number of connected components to be at least 2. □

2.7 $H_S(\mathbb{Q}_p)$

Now we shall proceed to the case that $K = \mathbb{Q}_p$, for a prime p. This case needs a lot of preliminaries, so we begin with an observation.

Suppose that we have a $\mathbb{Q}_p$-line ℓ in $\mathbb{P}^n$, and P, Q two distinct $\mathbb{Q}_p$-rational points of it. Then there is an obvious parametrisation of the $\mathbb{Q}_p$-rational points of ℓ, namely $\ell(\mathbb{Q}_p) = \{sP + tQ \mid [s : t] \in \mathbb{P}^1(\mathbb{Q}_p)\}$. If P and Q are two $\mathbb{Q}_p$-points in ℓ chosen at random, it is possible that $\overline{P} = \overline{Q}$, thus the aforementioned parametrisation of ℓ does not reduce to a parametrisation of $\overline{\ell}$. However, it is always possible to chose two points in the line such that this doesn't happen.

Lemma 2.7.1. *Let ℓ in $\mathbb{P}^n$ be a $\mathbb{Q}_p$-line. There exist P, Q two distinct $\mathbb{Q}_p$-rational points of it, such that $\overline{P} \neq \overline{Q}$. In that case, we shall call $\{sP + tQ \mid [s : t] \in \mathbb{P}^1(\mathbb{Q}_p)\}$ a good parametrisation of $\ell(\mathbb{Q}_p)$.*

Proof. We follow [16, Section 12]. Recall that we may identify lines in $\mathbb{P}^n$ with planes in the affine $(n + 1)$-dimensional space that pass through the origin. Let V_ℓ be the 2-dimensional subspace of $\mathbb{Q}_p^{n+1}$, that contains the points of $\ell(\mathbb{Q}_p)$, and $W_\ell = V_\ell \cap \mathbb{Z}^{n+1}$. This is a free $\mathbb{Z}_p$-module of rank 2, so it has a basis consisting of 2 elements; let u and v be those elements. Then $\ell(\mathbb{Q}_p) = \{su + tv \mid (s : t) \in \mathbb{P}^1(\mathbb{Q}_p)\}$, and obviously $\overline{u} \neq \overline{v}$. □

From this point, we will consider the 3-fold:

$$S_M : F(x, y, z, t, w) = x^3 + y^3 + z^3 + M(t^3 + w^3 + t^2 w) = 0, \tag{2.5}$$

where M is an odd square-free integer, whose prime divisors p have the fol-

lowing two properties

$$p \equiv 1 \pmod 3, \qquad \text{and} \qquad x^3 + x + 1 = 0 \text{ has no solutions in } \mathbb{F}_p. \tag{2.6}$$

We would like to study the reduction of the 3-fold modulo p. Let

$$\ell_1 \ : \ x = y = z = 0, \tag{2.7}$$

and

$$\Pi \ : \ t = w = 0. \tag{2.8}$$

Here ℓ_1 is a line and Π is a plane (2-dimensional linear variety). By Hensel's Lemma, we can easily see that if $R \in \overline{S}_M(\mathbb{F}_p)$ and $R \notin \ell_1(\mathbb{F}_p)$, then there exists $P \in S_M(\mathbb{Q}_p)$, such that $\overline{P} = R$. We define

$$S^{bd} = \{P \in S_M(\mathbb{Q}_p) \ \mid \ \overline{P} \in \ell_1(\mathbb{F}_p)\}$$

and

$$S^{gd} = \{P \in S_M(\mathbb{Q}_p) \ \mid \ P \notin S^{bd}\}.$$

Furthermore, if $P = [x : y : z : t : w] \in S_M(\mathbb{Q}_p)$ such that $\overline{P} \in \Pi(\mathbb{F}_p)$ then

$$\overline{x}^3 + \overline{y}^3 + \overline{z}^3 = 0.$$

Therefore, it seems reasonable to consider the plane cubic curve

$$C : x^3 + y^3 + z^3 = 0.$$

We also need to consider the variety that has the same coefficients as C does, but over another field K. We shall denote that variety by $C \times K$. In this curve we should fix a flex of it, for instance the flex $\mathcal{O} = [1 : -1 : 0]$. Now for P, Q, $R \in C(K)$, where K is a field of characteristic different than 3, $P + Q + R \sim 3\mathcal{O}$ in $\mathrm{Pic}^0(\mathrm{C} \times \mathrm{K})$ if and only if there is a K-line ℓ, such that $\ell \cdot C = P + Q + R$.

We need a lemma for the Picard group of the curve $C_p = C \times \mathbb{F}_p$. This is in fact Lemma 11.1 of [16].

Lemma 2.7.2. *Let $p \equiv 1 \pmod 3$ be a prime and write C_p for $C \times \mathbb{F}_p$. Then*

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

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

Lemma 2.7.3. *Let p be a prime divisor of M. Then, $S_M^{bd}(\mathbb{Q}_p) = \varnothing$.*

Proof. Let $[x : y : z : t : w] \in S_M^{bd}(\mathbb{Q}_p)$, such that x, y, z, t, $w \in \mathbb{Z}_p$ and $\min(v_p(x), \ldots, v_p(w)) = 0$. We have that $x \equiv y \equiv z \equiv 0 \pmod p$, so $x^3 + y^3 + z^3 \equiv 0 \pmod{p^3}$ and thus $t^3 + t^2 w + w^3 \equiv 0 \pmod p$. By the assumptions on p in (2.6) we have $t \equiv w \equiv 0 \pmod p$. This contradicts the fact that $\min(v_p(x), v_p(y), v_p(z), v_p(t), v_p(w)) = 0$. □

This lemma allows us to define the function $\phi : S_M(\mathbb{Q}_p) \to C(\mathbb{F}_p)$, as

$$\phi(P) = [\overline{x} : \overline{y} : \overline{z}].$$

We want to study this map, in order to get information about $H_{S_M}(\mathbb{Q}_p)$,

which completes the study of $H_S(K)$ for K a local field. We are interested in the relation of the images of collinear points. Suppose that P_1, P_2, P_3 are three collinear points in S_M and ℓ is the line that passes though them. We will consider two cases, based on the whether $\overline{\ell}$ is contained in $\overline{S}_M$ or not.

First, we will consider the case that $\overline{\ell} \not\subseteq \overline{S}_M$.

Lemma 2.7.4. *Let $p \mid M$ and ℓ be a $\mathbb{Q}_p$-line, not contained in S_M, and such that $\overline{\ell}$ is not contained in $\overline{S}_M$. Suppose that $\ell \cdot S = P_1 + P_2 + P_3$. Then $\phi(P_1) + \phi(P_3) + \phi(P_3) \sim 3\overline{\mathcal{O}}$.*

Proof. Let $su + tv$ be a good parametrisation of ℓ. Then we can find co-prime pairs $\lambda_i, \mu_i \in \mathbb{Z}_p$, such that $P_i = \lambda_i u + \mu_i v$. Since $\ell \cdot S = P_1 + P_2 + P_3$, we have that:

$$F(su + tv) = a \cdot \prod_{i=1}^{3} (\lambda_i t - \mu_i s)$$

for some $a \in \mathbb{Z}_p$. We remark that $a \not\equiv 0 \pmod{p}$ as $\overline{\ell} \not\subseteq \overline{S}_M$.

Write $u = [u_1 : u_2 : u_3 : u_4 : u_5]$, $v = [v_1 : v_2 : v_3 : v_4 : v_5]$, and set $u' = (\overline{u}_1, \overline{u}_2, \overline{u}_3)$, $v' = (\overline{v}_1, \overline{v}_2, \overline{v}_3)$. We proceed by distinguishing the following cases:

Case 1. Suppose that u' and v' are linearly independent. Then we can consider the line ℓ': $su' + tv'$. Reducing F modulo p, we get that $\ell' \cdot C_p = \phi(P_1) + \phi(P_2) + \phi(P_3)$, which completes the proof in this case.

Case 2. Suppose that u' and v' are linearly dependent. Then, there are α, $\beta \in \mathbb{F}_p$, not both zero, such that $\alpha u' + \beta v' = 0$. Let

$$R = [0 : 0 : 0 : \alpha\overline{u}_4 + \beta\overline{v}_4 : \alpha\overline{u}_5 + \beta\overline{v}_5] \in \overline{\ell}(\mathbb{F}_p) \cap \overline{S}_M(\mathbb{F}_p).$$

We observe $R = [0 : 0 : 0 : x : y]$, for some $x, y \in \mathbb{F}_p$, not both zero, as we have a good parametrisation of ℓ. This means that for $i = 1, 2, 3$, we have $R \neq \overline{P}_i$, because if $\overline{P}_i = R$ then $P_i \in S_M^{bd}(\mathbb{Q}_p)$ which is empty by the previous lemma. Hence, $\overline{\ell}$ and $\overline{S}_M$ meet at, at least, four points counting multiplicity, thus $\overline{\ell} \subseteq \overline{S}_M$. This forces $a \equiv 0 \pmod{p}$, which is a contradiction.

□

Now we will consider the case that $\overline{\ell} \subseteq \overline{S}_M$. It is worth mentioning that the following lemma does not need to distinguish between the case that ℓ is contained on S_M or not.

Lemma 2.7.5. *Let p be a prime divisor of M and P_1, P_2, P_3 be three points in $S_M(\mathbb{Q}_p)$ such that $P_1, P_2, P_3 \in \ell(\mathbb{Q}_p)$ and $\overline{\ell} \subseteq \overline{S}_M$. Then $\phi(P_1) = \phi(P_3) = \phi(P_3)$.*

Proof. Consider $su + tv$, a good parametrisation of ℓ. Thus we can write $P_i = \lambda_i u + \mu_i v$ where λ_i, $\mu_i \in \mathbb{Z}_p$ are coprime. Write $u = [u_1 : u_2 : u_3 : u_4 : u_5]$, $v = [v_1 : v_2 : v_3 : v_4 : v_5]$, $u' = [u_1 : u_2 : u_3]$ and $v' = [v_1 : v_2 : v_3]$. As $\overline{\ell} \subseteq \overline{S}_M$ we have that $\overline{F}(s\overline{u} + t\overline{v}) \equiv 0$.

On the other hand, we have that $\overline{F}(x, y, z, t, w) = x^3 + y^3 + z^3$, therefore, if $\overline{u}'$, $\overline{v}'$ are linearly independent, we would have the line $s\overline{u}' + t\overline{v}'$ contained in the irreducible curve $\overline{C}$, which is a contradiction. Thus, $\overline{u}'$, $\overline{v}'$ are linearly dependent, so $\phi(P_1) = \phi(P_3) = \phi(P_3)$. □

Chapter 3

The Mordell-Weil rank of cubic threefolds

3.1 Main Theorem

In this chapter we shall prove that there exists, conditionally on Colliot-Thélène's conjecture (Conjecture 1.7.5 in this thesis, see also [16]), a family of cubic threefolds S_M, whose Mordell-Weil rank has no upper bound. The idea is finding a family of the form:

$$F = C(x, y, z) + M \cdot f(x, y, z, t, w) = 0 \tag{3.1}$$

The idea comes from Siksek's paper [16]. We need

$$C \equiv 0 \pmod{p} \tag{3.2}$$

to be an elliptic curve such that p is a prime of bad reduction of F, i.e. a prime divisor of M, such that $\dim_{\mathbb{F}_3} \mathrm{Pic}^0(\mathrm{C})/3\mathrm{Pic}^0(\mathrm{C}) = 2$. Furthermore we

need

$$f \equiv 0 \pmod{p} \tag{3.3}$$

to have no non-trivial solutions. We will give an example where, as the number of prime divisors of M grows, the minimum number of Mordell-Weil generators will grow as well, proving the unboundedness. Therefore, we see that we need a positive density of primes such that (3.2) and (3.3) are both satisfied at the same time.

Proposition 3.1.1. *Let $\psi : S_M(\mathbb{Q}_p) \to \mathrm{Pic}^0(\mathrm{C_p})$ be given by $\psi(P) = \phi(P) - \overline{\mathcal{O}}$. Then ψ induces a well-defined surjective homomorphism $\overline{\psi}$.*

$$\overline{\psi} : H_{S_M}(\mathbb{Q}_p) \to \frac{\mathrm{Pic}^0(\mathrm{C_p})}{3\mathrm{Pic}^0(\mathrm{C_p})}, \qquad \overline{\psi}([P]) = \psi(P) \pmod{3\mathrm{Pic}^0(\mathrm{C_p})}.$$

Proof. Recall that by Lemma 2.7.3 we have that $S_M(\mathbb{Q}_p) = S_M^{gd}$. Therefore if we consider the map $\phi : S_M(\mathbb{Q}_p) \to C(\mathbb{F}_p)$, then $\phi \mid_{S_M^{gd}} = \phi$. By Hensel's lemma, we have that the map $\phi : S_M^{gd} \to C(\mathbb{F}_p)$ is surjective, thus if $\overline{\psi}$ is well-defined, then it is a surjective homomorphism. Therefore, it suffices to show that if $P, Q, R \in S_M(\mathbb{Q}_p)$ are collinear, then $\psi(P) + \psi(Q) + \psi(R) \in 3\mathrm{Pic}^0(\mathrm{C_p})$.

If P, Q and R are collinear, we have by lemmas 2.7.4 and 2.7.5 that either $\phi(P) + \phi(Q) + \phi(R) \sim 3\overline{\mathcal{O}}$ or $\phi(P) = \phi(Q) = \phi(R)$. Therefore in any case $\psi(P) + \psi(Q) + \psi(R) \in 3\mathrm{Pic}^0(\mathrm{C_p})$, which concludes the proof. □

We are now ready to prove the unboundedness of the Mordell–Weil rank for the family $\{S_M\}$. The proof is conditional on Conjecture 1.7.5, which is concerned with weak approximation on surfaces. We could replace it with a stronger conjecture about threefolds, but there is no need to; we will simply reduce the problem to the case of surfaces.

We recall from [16] the following proposition and its proof:

Proposition 3.1.2 (Siksek)**.** *Let $p_1, \ldots, p_s$ ($s \geqslant 1$) be distinct primes $\equiv 1 \pmod 3$, $M = \prod p_i$, and $\Sigma = \{3\}$. Let $S = S'_M/\mathbb{Q}$ be the cubic surface described by*

$$S'_M : x^3 + y^3 + z^3 + Mw^3 = 0. \tag{3.4}$$

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

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

is surjective.

Proof. We follow the proof given in [16]. All the results we need for this proof are due to Colliot-Thélène, Kanevsky and Sansuc [1], though Jahnel's Habilitation summarizes these results in one convenient theorem [9, Chapter III, Theorem 6.4]. Indeed, we know that: [1]

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

(ii) The image of

$$\langle\ ,\ \rangle : \mathrm{Br}(S) \times S(\mathbb{A}_\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

[1] The computation of $\mathrm{Br}(S)/\mathrm{Br}_0(S)$ in our situation is rather simple if we consider S as defined over $\mathbb{Q}(\zeta)$ where ζ is the primitive cube root of unity. For now let S be a smooth cubic surface over a number field K and let L be the field of definition of the 27 lines on S. Then L/K is a Galois extension. By [19, Lemma 5], the quotient $\mathrm{Br}(S)/\mathrm{Br}_0(S) \cong (\mathbb{Z}/3\mathbb{Z})^2$ if and only if $\mathrm{Gal}(L/K)$ is cyclic of order 3. Now let S be the diagonal cubic surface $x^3 + y^3 + z^3 + Mw^3 = 0$ where $M \in K\backslash\{0\}$. Then $L = K(\zeta, \sqrt[3]{M})$. The Galois group $\mathrm{Gal}(L/K)$ is cyclic of order 3 if and only if M is a non-cube in K and $\zeta \in K$.

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

(iii) The map

$$S(\mathbb{Q}_p) \to \frac{1}{3}\mathbb{Z}/\mathbb{Z}, \qquad P \mapsto \mathrm{inv}_p(A, P)$$

is surjective for all $p \mid M$.

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

$$\mathrm{inv}_3(A, P_3) = -\sum_{v \neq 3} \mathrm{inv}_v(A, P_v).$$

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 $\mathrm{Br}(S)/\mathrm{Br}_0(S)$ we know that $\mathcal{P}' \in S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(S)}$. 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. □

Theorem 3.1.3. *Let $p_1, p_2, \ldots, p_s$ be s distinct primes all satisfying* (2.6) *and let $M = \prod_{i=1}^{s} p_i$. Then the cubic threefold:*

$$S_M : x^3 + y^3 + z^3 + M(t^3 + w^3 + t^2 w) = 0$$

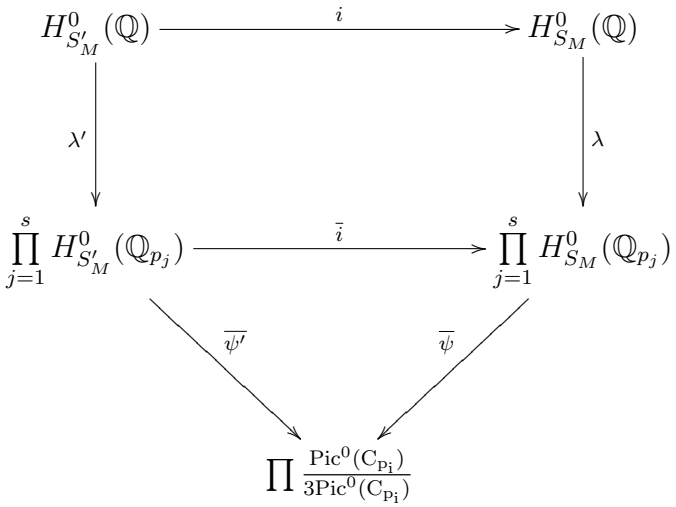
has rank at least 2^s.

Proof. Consider the cubic surface:

$$S'_M : x^3 + y^3 + z^3 + Mt^3 = 0.$$

and the map $\chi : S'_M \hookrightarrow S_M$, with $\chi([a : b : c : d]) = [a : b : c : d : 0]$. By Proposition 2.3.1, this map induces a group homomorphism i, which makes

the following diagram commutative:



Here $\overline{\psi}$ is as in Proposition 3.1.1. The homomorphism $\overline{\psi'}$ is surjective (this is Proposition 15.1 of [16], and the proof is very similar to the proof of Proposition 3.1.1 above). By Proposition 3.1.2, the homomorphism λ' is surjective. Hence $\overline{\psi'} \circ \lambda'$ is surjective. Since $\overline{\psi} \circ \lambda \circ i = \overline{\psi'} \circ \lambda'$, it follows that $\overline{\psi} \circ \lambda$ is also surjective. It is also easy to see that $3H^0_{S_M}(\mathbb{Q}) \subseteq Ker(\overline{\psi})$. Thus,

$$H^0_{S_M}(\mathbb{Q}) \to \frac{H^0_{S_M}(\mathbb{Q})}{3H^0_{S_M}(\mathbb{Q})} \to \prod_{i=1}^{s} \frac{\mathrm{Pic}^0(\mathrm{C}_{\mathrm{p_i}})}{3\mathrm{Pic}^0(\mathrm{C}_{\mathrm{p_i}})}$$

are two homomorphisms, whose composition is a surjective homomorphism, and thus

$$r(S_M, \mathbb{Q}) \geqslant \dim_{\mathbb{F}_3} \frac{H^0_{S_M}(\mathbb{Q})}{3H^0_{S_M}(\mathbb{Q})} \geqslant \dim_{\mathbb{F}_3} \prod_{i=1}^{s} \frac{\mathrm{Pic}^0(\mathrm{C}_{\mathrm{p_i}})}{3\mathrm{Pic}^0(\mathrm{C}_{\mathrm{p_i}})} = 2^s.$$

Here we have used Lemma 2.2.9 and Lemma 2.7.2. There is one final detail, which is that to apply Lemma 2.2.9 we need to show that S_M has a $\mathbb{Q}$-ternary point. Let $P_0 = (1 : -1 : 0 : 0 : 0)$, and let ℓ be the line given by $x + y = w =$

$t = 0$. Then $\ell \cdot S = 3P_0$ showing that P_0 is $\mathbb{Q}$-ternary. $\square$

It is worth noting that fourfolds are the highest dimensional varieties that Siksek's trick can work directly. Consider a family of varieties of the form (3.1). In that family, f cannot have more than 3 variables, as we need the equation (3.3) to have no non-zero solutions; if it had more than 3, by Chevalley-Waring's Theorem (Theorem 1.6.1) it would have a non-trivial solution. Even if these variables are not different than the variables in C, F will have at most 6 variables, therefore its dimension cannot be greater than 4.

Question 1. *Can we find a family of fourfolds of the form*

$$F = c(x, y, z) + M \cdot f(t, w, v) = 0$$

such that Siksek's trick will work?

Chapter 4

The Mordell-Weil rank in higher dimensions

4.1 Setup

Suppose that S is a cubic hypersurface and A is a point in it. Recall that $\langle A \rangle_{MW}$ is the set of points we can obtain from A via secant and tangent operations. In order to find $\langle A \rangle_{MW}$ the first thing we have to check is the set $\mathcal{B}$, which contains the points B such that there exists a K-line $\ell \not\subseteq S$ such that $\ell \cdot S = A + A + B$. This line ℓ is tangent to S at A, and so it is contained in the tangent plane $T_A S$. This means that all such B live inside $T_A S$, and more specifically

$$\{A\} \subseteq \mathcal{B} \subseteq (T_A S \cap S)(K).$$

One may see that the case of $\mathcal{B} = \{P\}$ is inherently different to the others, as it leads to $\langle A \rangle_{MW} = \{A\}$. This observation is the idea behind the definition of lonely points.

4.2 Lonely Points

Definition 4.2.1. Let S be a cubic hypersurface. A point $A \in S(\overline{K})$ is called a **lonely** point if for all points $B \in (T_A S \cap S)(\overline{K})$ we have that $\ell_{A,B} \subseteq S$, where $\ell_{A,B}$ is the line joining A and B.

The following two lemmas show that lonely points are a genuine generalisation of the Eckardt points of cubic surfaces.

Lemma 4.2.2. *Let S be a smooth cubic surface, and $P \in S$. Then P is an Eckardt point if and only if it is lonely.*

Proof. If $\dim S = 2$ then $S \cap T_P S$ is a plane cubic curve that might be degenerate, i.e. a union of a line and a conic, or a union of three lines. If P is an Eckardt point then $S \cap T_P S$ is the union of three lines passing through P, and so P is clearly lonely.

Conversely suppose P is lonely. Let C be an irreducible component of $S \cap T_P S$. Choose $Q \in C(\overline{K})$ that does not belong to any other component. Then $\ell_{P,Q} \subset S \cap T_P S$, and so $\ell_{P,Q} = C$. Therefore, all the components of $S \cap T_P S$ are lines passing through P. As $S \cap T_P S$ is a plane cubic curve there must be exactly three of them, and so P is Eckardt. □

Lemma 4.2.3. *Suppose that $S \subseteq \mathbb{P}^n$ is a cubic hypersurface, with $n \geqslant 3$ and $A \in S$, a lonely point. Let Π be a 2-dimensional linear subvariety of $T_A S$ containing A, and suppose $\Pi \not\subset S$. Then $\Pi \cap S$ is a union of three lines passing through A.*

Proof. As $\Pi \not\subset S$, and Π is 2-dimensional, we see that $S \cap \Pi$ is a plane cubic curve. Again let C be an irreducible component of $S \cap \Pi$, and let $B \in C(\overline{K})$ not contained in any other component. As $\Pi \subset T_A S$ we have $B \in (S \cap T_A S)(\overline{K})$.

Since A is lonely, we have $\ell_{A,B} \subset S$ and so $\ell_{A,B} \subset S \cap \Pi$. In other words, $\ell_{A,B}$ is an irreducible component of $S \cap \Pi$ which intersects C in B. This shows that $C = \ell_{A,B}$ is a line passing through A. As $S \cap \Pi$ is cubic, it consists of three lines passing through A. □

The main problem with the definition of lonely points is that it is purely geometric, and sometimes we would need to treat them as solutions to polynomial equations. In order to find such a characterisation of lonely points it would be easier to choose a standardised set of coordinates for the point in question. The following definition will serve as such.

Definition 4.2.4. Let f be a homogeneous cubic polynomial with coefficients in K and let $S : f = 0$. Let $S_{ns}(K)$ be the set of all non-singular K-points in S. Suppose that $A \in S_{ns}(K)$. We can apply a linear transformation, so that $A \mapsto [1 : \overrightarrow{0}]$ and $T_A S \mapsto \{x_n = 0\}$. After that transformation we have that S is isomorphic to

$$S_A \ : \ f_A = 0,$$

where

$$f_A = x_0^2 x_n + x_0 x_n l_A(x_1, \ldots, x_n) + x_0 q_A(x_1, \ldots, x_{n-1}) + c_A(x_1, \ldots, x_n). \quad (4.1)$$

We call f_A an **A-normal form** of f.

It is worth noting that the A-normal form of a cubic polynomial is unique up to a non-singular change of variables $x_1, \ldots, x_{n-1}$. Another observation about the A-normal form is that it needs $T_A S$ to be a hyperplane, therefore it has no meaning for singular points. Its main purpose is to facilitate the following algebraic characterisation of lonely points.

Proposition 4.2.5. *A point $P \in S(\overline{K})$ is a lonely point if and only if there is any (and thus all) P-normal form of f with $q_P \equiv 0$.*

Proof. Let $P \in S(\overline{K})$, and let $Q \in (S \cap T_P S)(\overline{K})$. We shall use the identity (Taylor's expansion):

$$f_P(sP + tQ) = s^3 f_P(P) + s^2 t\, Q \cdot \nabla f_P(P) + st^2\, P \cdot \nabla f_P(Q) + t^3 f_P(Q).$$

Then $\ell_{P,Q} \subset S$ is equivalent to $f_P(sP+tQ) \equiv 0$, and consecutively is equivalent to

$$f_P(P) \;=\; Q \cdot \nabla f_P(P) \;=\; P \cdot \nabla f_P(Q) \;=\; f_P(Q) = 0.$$

As P, Q are points on S, we have $f_P(P) = f_P(Q) = 0$. Moreover, $Q \cdot \nabla f_P(P) = 0$ as $Q \in T_P S$. In our new coordinates:

$$P = [1 : \overrightarrow{0}], \qquad Q = [\alpha_0 : \alpha_1 : \cdots : \alpha_{n-1} : 0].$$

Thus,

$$P \cdot (\nabla f_P(Q)) = \frac{\partial f_P}{\partial x_0}(Q) = q_P(\alpha_1 \ldots, \alpha_{n-1}).$$

Therefore, P is lonely if and only if for all $Q = [\alpha_0 : \cdots : \alpha_{n-1} : 0] \in S(\overline{K}) \cap T_P S$ we have $q_P(\alpha_1, \ldots, \alpha_{n-1}) = 0$. It follows that if $q_P \equiv 0$ then P is lonely.

Suppose that $q_P \not\equiv 0$. Then there are $\alpha_1, \ldots, \alpha_{n-1} \in \overline{K}$ such that $q_P(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Let

$$\alpha_0 = \frac{-c_P(\alpha_1, \ldots, \alpha_{n-1}, 0)}{q_P(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})}, \tag{4.2}$$

and $Q = [\alpha_0 : \cdots : \alpha_{n-1} : 0]$. Clearly $Q \in (S \cap T_P S)(\overline{K})$, and so P is not lonely. □

Let $A \in S$, and consider the set

$$W_A = \{B \in T_A S \cap S \mid l_{A,B} \not\subseteq S\}.$$

Then A is non lonely if and only if $W_A(\overline{K}) \neq \varnothing$. An interesting question that arises is whether it suffices to look for a point in $W_A(K)$ in order to prove that A is non lonely. A first application of the previous proposition is Lemma 4.2.7 below, which gives an affirmative answer to the question. We shall first need a version of Lemma 1.8.4 that is valid over finite fields, but with a more restrictive hypothesis.

Lemma 4.2.6. *Let K be any field. Let $q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a non-zero homogeneous quadratic polynomial. Then there are $a_1, \ldots, a_n \in K$ such that $q(a_1, \ldots, a_n) \neq 0$.*

Proof. We prove this by induction on n. If $n = 1$ then $q = \alpha x_1^2$ where $\alpha \neq 0$. Then $q(1) \neq 0$.

Suppose $n > 1$. We can write

$$q = g(x_1, \ldots, x_{n-1}) + h(x_1, \ldots, x_{n-1})x_n + \alpha x_n^2,$$

where g is homogeneous quadratic, and h is homogeneous linear. If $g \not\equiv 0$, then by the inductive hypothesis there are $a_1, \ldots, a_{n-1} \in K$ such that $g(a_1, \ldots, a_{n-1}) \neq 0$. We complete the proof in this case by taking $a_n = 0$. So we may suppose $g \equiv 0$. If $\alpha \neq 0$, then we can take $a_1 = \cdots = a_{n-1} = 0$ and $a_n = 1$, so we may suppose $\alpha = 0$. Since $q \not\equiv 0$, we now have $h \not\equiv 0$. By linear

algebra, the set

$$\{(a_1, \ldots, a_{n-1}) \in K^{n-1} \ : \ h(a_1, \ldots, a_{n-1}) = 0\}$$

is a subspace of K^{n-1} of codimension 1, and there are vectors $(a_1, \ldots, a_{n-1}) \in K^{n-1}$ outside this subspace. Now for such a vector, let $a_n = 0$ and we get $q(a_1, \ldots, a_n) \neq 0$. □

The above lemma is not true for $K = \mathbb{F}_2$ if q is allowed to be inhomogeneous. For example, take $q = x_1^2 - x_1$.

Lemma 4.2.7. *Let S be a cubic hypersurface defined over K, and $P \in S(K)$ a non-lonely point. Then, there exists a point $Q \in (T_P S \cap S)(K)$ with $Q \neq P$ such that $\ell_{P,Q} \not\subseteq S$.*

Proof. Suppose $P \in S(K)$ is non-lonely. By Proposition 4.2.5 we have $q_P \not\equiv 0$. We follow the proof of Proposition 4.2.5 for the case when $q_P \not\equiv 0$, by slightly modifying the last part of the proof. By Lemma 4.2.6 we can choose $\alpha_1, \ldots, \alpha_{n-1} \in K$ so that $q_P(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$ and let $\alpha_0 \in K$ be given by (4.2). Then $Q = [\alpha_0 : \cdots : \alpha_{n-1} : 0] \in (S \cap T_P S)(K)$ and from the first part of the proof of Proposition 4.2.5 we have $\ell_{P,Q} \not\subseteq S$. □

An interesting fact about Eckardt points is that any line in a cubic surface can contain up to 5 of them if the characteristic of the field is 2, otherwise this number drops to 2. We would like to generalise this observation. There are two ways to prove such a lemma; first, using Bertini's Theorem (Theorem 1.8.2), or using the characterisation of lonely points and doing the calculations.

We will first need a lemma that finds the upper bound for the number of points in a line that have the same tangent space.

Lemma 4.2.8. *Let $S \subseteq \mathbb{P}^n$ be a smooth hypersurface, with $n \geqslant 3$, defined over a field K (of any characteristic). Let $\ell \subseteq S$ be a line. Then at most two $\overline{K}$-points in ℓ have the same tangent space.*

Proof. Let $A, B \in \ell(\overline{K})$ with the same tangent space. By a suitable linear change of variables (defined over $\overline{K}$), we can suppose that

$$A = [1 : 0 : \cdots : 0], \qquad B = [0 : 1 : 0 : \cdots : 0],$$

and the common tangent hyperplane is

$$T_A S = T_B S \ : \ x_n = 0.$$

Then ℓ is given by

$$\ell \ : \ x_2 = x_3 = \cdots = x_n = 0.$$

We conclude that f (the defining polynomial for S) takes the form:

$$\begin{aligned} f(x_0, \ldots, x_n) \ &= \ (x_0^2 + \delta x_1^2)x_n + x_0 x_1(\alpha x_n + h(x_2, \ldots, x_n)) \\ &\quad + x_0 q_0(x_2, \ldots, x_n) + x_1 q_1(x_2, \ldots, x_n) + c(x_2, \ldots, x_n). \end{aligned}$$

where h is homogeneous linear, q_0 and q_1 are homogeneous quadratic, and c homogeneous cubic. Now we carry out a further linear change of variable in the variables $x_2, \ldots, x_{n-1}$ that does not affect x_0, x_1, x_n but replaces $h(x_2, \ldots, x_n)$

by βx_{n-1} where $\beta = 0$ if $h \equiv 0$ and $\beta = 1$ otherwise. Thus

$$\begin{aligned} f(x_0, \ldots, x_n) &= (x_0^2 + \delta x_1^2)x_n + x_0 x_1(\alpha x_n + \beta x_{n-1}) + x_0 q_0(x_2, \ldots, x_n) \\ &\quad + x_1 q_1(x_2, \ldots, x_n) + c(x_2, \ldots, x_n). \end{aligned}$$

Now suppose $C \in \ell(\overline{K})$, and so $C = [x : y : 0 : \cdots : 0]$ for appropriate x, $y \in \overline{K}$. So then,

$$(\nabla f)(C) = (0, 0, \ldots, 0, \beta xy, x^2 + \delta y^2 + \alpha xy).$$

First we show that $\beta \neq 0$. Suppose $\beta = 0$. Choose x, $y \in \overline{K}$, neither of which are zero, so that $x^2 + \delta y^2 + \alpha xy = 0$. Then $(\nabla f)(C) = 0$ which shows C to be singular on the smooth surface S, giving a contradiction. Hence $\beta \neq 0$. Now the tangent hyperplane at C is

$$T_C S \ : \ \beta xy x_{n-1} + (x^2 + \delta y^2 + \alpha xy)x_n = 0.$$

Suppose now that $T_C S = T_A S$ which is given by $x_n = 0$. It follows that $\beta xy = 0$ and so $C = A$ or B. □

We have now built the tools needed to find the maximum number of lonely points in a line.

Proposition 4.2.9. *Let $S \subset \mathbb{P}^n$ be a cubic hypersurface defined over $\overline{K}$, with $n \geqslant 3$. Let ℓ be a line contained in S. If* $\mathrm{char(K)} = 2$*, there are at most* 5 *lonely points in ℓ, otherwise there are at most* 2*.*

Proof. We shall proof this by induction on $n \geqslant 3$. If $n = 3$, then the lonely points are Eckardt points, and so the lemma follows from Lemma 4.2.2.

Suppose $n \geqslant 4$. By Corollary 1.8.7, there is some hyperplane H (defined over the infinite field $\overline{K}$) containing ℓ such that $S' = H \cap S$ is smooth. Any point on ℓ that is lonely for S is also lonely for S'. The lemma follows by induction. □

The following proposition shows that lonely points can exist in cubic hypersurfaces of any dimension.

Proposition 4.2.10. *Let K be a field with* $\mathrm{char(K)} \neq 3$. *For all $n \geqslant 2$ there exists a non singular cubic hypersurface in $\mathbb{P}^n$ that has at least one lonely point.*

Proof. Consider the hypersurface given by

$$f(x_0, x_1, \ldots, x_n) = x_0^2 x_n + x_0 x_n \sum_{i=1}^{n-1} x_i + \sum_{i=1}^{n} x_i^3.$$

It is easy, but tedious, to check that

$$f = \frac{\partial f}{\partial x_0} = \cdots = \frac{\partial f}{\partial x_n} = 0$$

have a common solution if and only if $\mathrm{char(K)} = 3$. Then, by proposition 4.2.5, we conclude that the point $A = [1 : 0 : \cdots : 0]$ is lonely. □

4.3 Some Geometry

Lemma 4.3.1. *Let S be a cubic hypersurface. Let A be a smooth point in S and let $\Pi \subset S$ be a linear subvariety containing A. Then $\Pi \subset T_A S$.*

Proof. We work in affine coordinates. We can suppose that $A = (0, 0, \ldots, 0) \in$

$\mathbb{A}^n$, and $T_A S$ is given $x_n = 0$. Then S has the equation

$$x_n + q(x_1, \ldots, x_n) + c(x_1, \ldots, x_n) = 0 \tag{4.3}$$

where q and c are homogeneous, respectively linear and quadratic. Now Π, as it is a linear subvariety containing A, is a subspace of $\mathbb{A}^n$. Let $B \in \Pi$ with $B \neq A$. Then the line joining A and B is given parametrically by tB. This is contained in Π which is contained in S. Thus the polynomial

$$x_n(B)t + q(B)t^2 + c(B)t^3$$

vanishes identically. In particular, $x_n(B) = 0$, so $B \in T_A S$. This proves that $\Pi \subset T_A S$. □

Lemma 4.3.2. *Let S be a cubic hypersurface. Let A be a smooth point in S and let Π be a linear variety containing A such that $\Pi \not\subset S$. Then $S \cap \Pi$ is singular at A if and only if $\Pi \subset T_A S$.*

Proof. We start as in the proof of Lemma 4.3.1, so we can suppose that $A = (0, \ldots, 0)$, that T_A is given by $x_n = 0$ and that S is given by (4.3). Suppose that $\Pi \subset T_A S$. Now Π is a vector subspace of $\mathbb{A}^n$, that is contained in $x_n = 0$. We can suppose by carrying a further linear transformation that Π is given by

$$\Pi \ : \ x_r = x_{r+1} = \cdots = x_n = 0.$$

Then

$$S \cap \Pi \ : \ \begin{cases} x_r = 0, \\ x_{r+1} = 0 \\ \vdots \\ x_n = 0, \\ q(x_1, x_2, \ldots, x_{r-1}, 0, \ldots, 0) + c(x_1, x_2, \ldots, x_{r-1}, 0, \ldots, 0) = 0. \end{cases}$$

As the final equation does not contain linear terms, we see that $S \cap \Pi$ is singular at $A = (0, \ldots, 0)$.

Conversely, suppose that $\Pi \not\subset T_A S$. Then there is a linear change of coordinates that does not affect the plane $T_A S \ : \ x_n = 0$ that takes Π to

$$\Pi \ : \ x_1 = x_2 = \cdots = x_s = 0$$

for some $s < n$. Hence

$$S \cap \Pi \ : \ \begin{cases} x_1 = 0, \\ x_2 = 0 \\ \vdots \\ x_s = 0, \\ x_n + q(0, \ldots, 0, x_{s+1}, \ldots, x_n) + c(0, \ldots, 0, x_{s+1}, \ldots, x_n) = 0. \end{cases}$$

As the final equation does contain a non-zero linear term, we see that $S \cap \Pi$ is nonsingular at $A = (0, \ldots, 0)$. □

The following lemma can be generalised for some non finite fields like $\mathbb{Q}_p$ and $\mathbb{Q}$, just by changing the lower bound of the dimension. We shall give

only the finite field case, as this is the only case we will use.

Lemma 4.3.3. *Let $S \subseteq \mathbb{P}^n$ be a non singular cubic hypersurface over a finite field K, with $n \geqslant 6$. Let $A \in S(K)$ be a non lonely point and $B \in (T_A S \cap S)(K)$ be a lonely point. Then the set*

$$(T_A S \cap T_B S \cap S)(K)$$

contains at least two points.

Proof. If $A \in T_B S$ there is nothing to prove. Therefore we may assume that $A \notin T_B S$. Without loss of generality we may assume that $A = [1 : 0 : \cdots : 0]$, $T_A S = \{[x_0 : x_1 : \cdots : x_n] \mid x_n = 0\}$, $B = [0 : 0 : \cdots : 0 : 1]$ and $T_B S = \{[x_0 : x_1 : \cdots : x_n] \mid x_{n-1} = 0\}$. Therefore, S is given by the zero locus of a function of the form

$$\begin{aligned} f =& x_0^2 x_n + x_0 x_n \ell_1(x_1, x_2, \ldots, x_{n-2}) + x_0 q(x_1, x_2, \ldots, x_{n-2}) + x_n^2 x_{n-1} \\ &+ x_n x_{n-1} \ell_2(x_1, x_2, \ldots, x_{n-2}) + c(x_1, x_2, \ldots, x_{n-2}) \end{aligned}$$

A point $P = [0 : x_1 : \cdots : x_{n-2} : 0 : 0]$ lives in $(T_A S \cap T_B S \cap S)(K)$ if and only if $c(x_1, x_2, \ldots, x_{n-2}) = 0$. By the Chevalley-Warning theorem (Theorem 1.6.1) we have that as $n - 2 > 3$, then c cannot have only the trivial solution. □

4.4 Point Generation

We are now ready to work towards a criterion for the minimum number of points needed to generate all the points of a smooth cubic hypersurface.

Lemma 4.4.1. *Let S be a smooth cubic hypersurface over a field K. Let $A \in S(K)$, and $B \in (T_A S \cap S)(K)$, with $B \neq A$. Let $\ell_{A,B}$ be the line joining A and B. Suppose $\ell_{A,B} \not\subset S$. Then $B \in \langle A \rangle_{MW}$.*

Proof. Clearly $\ell_{A,B} \subset T_A S$, and so is tangent to S at A. Thus $\ell_{A,B} \cdot S = A + A + B$. It follows that $B \in \langle A \rangle_{MW}$. □

We will need a version of Lemma 4.2.6 with a slightly stronger conclusion, but also slightly stronger hypothesis.

Lemma 4.4.2. *Suppose $\#K \geqslant 3$. Let $q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a non-zero homogeneous quadratic polynomial. Then there are $a_1, \ldots, a_n \in K$ with $a_n \neq 0$ and $q(a_1, \ldots, a_n) \neq 0$.*

Proof. If $K = \mathbb{F}_3$, we shall show that the polynomial $f(x_1, x_2, \ldots, x_{n-1}, 1)$ is not identically zero. For $n > 5$, this is an immediate consequence of Theorem 1.6.1. There are $3^{10} - 1$ non-zero homogeneous quadratic polynomials, in less than 4 variables. We can easily check all of them using a computer algebra program. Therefore, we may assume that $\#K \geqslant 4$. In this case we will do it by induction on n. If $n = 1$ then $q = \alpha x_1^2$ where $\alpha \neq 0$, and so $q(1) \neq 0$.

Suppose $n > 1$. We can write

$$q = g(x_1, \ldots, x_{n-1}) + h(x_1, \ldots, x_{n-1}) x_n + \alpha x_n^2$$

where g is a homogeneous quadratic polynomial or the zero polynomial, and h is a homogeneous linear polynomial or the zero polynomial.

First suppose that g is not the zero polynomial. Then, by the inductive hypothesis we can choose $a_1, \ldots, a_{n-1} \in K$ such that $g(a_1, \ldots, a_{n-1}) \neq 0$.

Then the equation

$$g(a_1, \ldots, a_{n-1}) + h(a_1, \ldots, a_{n-1})x_n + \alpha x_n^2 = 0$$

has at most two solutions in K. As $\#K \geqslant 4$, we can choose $a_n \in K$ to be different from 0 and the two solutions.

Now assume that g is the zero polynomial. Then h can be assumed that is not the zero polynomial as is we would the case of $n = 1$. In that case we can choose $x_n = 1$ and $a_1, \ldots, a_{n-1} \in K$ such that $h(a_1, \ldots, a_{n-1}) \neq \alpha$, which concludes the proof. □

Next we will prove a lemma that will do all the heavy lifting in terms of algebraic calculations. This will allow us to concentrate on the geometry of the problem afterwards.

Lemma 4.4.3. *Let $\#K \geqslant 3$. Let S be a smooth cubic hypersurface in $\mathbb{P}^n$ where $n \geqslant 3$. Let $\ell \subset S$ be a K-line. Let $A \in \ell(K)$ be a non-lonely point. Suppose $B \in \ell(K) \smallsetminus \{A\}$ satisfies $T_B S \neq T_A S$. There exists $C \in S(K)$ such that*

(i) $C \neq A, B$,

(ii) $C \notin \ell$,

(iii) $C \in T_A S$,

(iv) $C \notin T_B S$

(v) $\ell_{A,C} \not\subset S$, *where* $\ell_{A,C}$ *is the unique line jointing* A *and* C,

(vi) $\Pi_{A,B,C} \cap S = \ell \cup Q$, *where* $\Pi_{A,B,C}$ *is the unique* 2*-dimensional linear subvariety containing* A, B, C. *Here*

(a) *either Q is a conic defined over K and irreducible over $\overline{K}$, and $B \notin \ell \cap Q$,*

(b) *or there are K-lines ℓ_1, ℓ_2, so that $Q = \ell_1 \cup \ell_2$, the lines ℓ, ℓ_1, ℓ_2 are pairwise distinct, $\ell \cap \ell_1 = A$, $A \notin \ell_2$, and $B \notin \ell_1 \cup \ell_2$.*

Proof. By Lemma 4.3.1, we have that $\ell \subset T_A S$ and $\ell \subset T_B S$. In particular $T_A S$ and $T_B S$ are distinct hyperplanes, both containing A. Applying a linear transformation, we may suppose that

$$A = [1 : 0 : \cdots : 0], \qquad T_A S : \ x_n = 0, \qquad T_B S : \ x_{n-1} = 0.$$

The equation for S is now given in A-normal form by

$$f_A = x_0^2 x_n + x_0 x_n l_A(x_1, \ldots, x_n) + x_0 q_A(x_1, \ldots, x_{n-1}) + c_A(x_1, \ldots, x_n). \quad (4.4)$$

Here as before l_A, q_A and c_A are homogeneous of degree 1, 2, 3 respectively. By hypothesis, A is not lonely. Proposition 4.2.5 tells us that $q_A \not\equiv 0$. By Lemma 4.4.2, as $\#K \geqslant 3$, we have that there are $\gamma_1, \ldots, \gamma_{n-1} \in K$ with $\gamma_{n-1} \neq 0$ and $q_A(\gamma_1, \ldots, \gamma_{n-1}) \neq 0$. Let

$$\gamma_n = 0, \qquad \gamma_0 = \frac{-c_A(\gamma_1, \ldots, \gamma_n)}{q_A(\gamma_1, \ldots, \gamma_{n-1})}.$$

and $C = (\gamma_0 : \cdots : \gamma_n)$. It is straightforward to check from equation (4.4) that $C \in S(K)$. Moreover, since $T_A S$ is given by $x_n = 0$ and $\gamma_n = 0$ we have that $C \in T_A S$. This proves (iii). Also $T_B S$ is given by $x_{n-1} = 0$ and $\gamma_{n-1} \neq 0$ so $C \notin T_B S$. This proves (iv). It is clear that $C \neq A$. Moreover, as $C \notin T_B S$ we have $C \neq B$. This proves (i).

By Lemma 4.3.1, we have $\ell \subset T_B S$. As $C \notin T_B S$, we have $C \notin \ell$. This proves (ii).

Let $\ell_{A,C}$ be the line joining A and C. The parametric form for $\ell_{A,C}$ is given by

$$\ell_{A,C} \ : \ (s + t\gamma_0 : t\gamma_1 : t\gamma_2 : \cdots : t\gamma_{n-1} : 0).$$

Here we made use of the fact that $\gamma_n = 0$. Substituting this into the polynomial f_A we obtain

$$(s + t\gamma_0)t^2 q_A(\gamma_1, \ldots, \gamma_n) + t^3 c_A(\gamma_1, \ldots, \gamma_{n-1}, 0).$$

This expression is not identically zero as $q_A(\gamma_1, \ldots, \gamma_n) \neq 0$, so $\ell_{A,C} \not\subset S$, proving (v).

We now prove (vi). Let $\Pi_{A,B,C}$ be the 2-dimensional linear subvariety containing A, B, C. This must be unique as A, B, C do not lie on one line. First we show that $\Pi_{A,B,C} \not\subset S$. Suppose otherwise. Then by Lemma 4.3.1 we have $\Pi_{A,B,C} \subset T_B S$. Thus $C \in T_B S$ giving a contradiction. This proves $\Pi_{A,B,C} \not\subset S$. It follows, by Lemma 4.3.2, that $S \cap \Pi_{A,B,C}$ is a plane cubic curve that is singular at A, and this contains ℓ as a component. Thus $S \cap \Pi_{A,B,C} = \ell \cup Q$ where Q is possibly reducible conic.

Suppose first that Q is irreducible over $\overline{K}$. To complete the proof in this case (vi)(a) we want to show that $B \notin \ell \cap Q$. Suppose otherwise. Then B is a singular point of $S \cap \Pi_{A,B,C}$. Thus, by Lemma 4.3.2, $\Pi_{A,B,C} \subset T_B S$. This shows that $C \in T_B S$, giving a contradiction. Hence $B \notin \ell \cap Q$ as required by (vi)(a).

Suppose $Q = \ell_1 \cup \ell_2$ where ℓ_i are lines. These are either K-lines, or

they defined over a quadratic extension and are conjugate. Since $S \cap \Pi_{A,B,C} = \ell \cup \ell_1 \cup \ell_2$ is singular at A, the point A must belong to ℓ_1 or ℓ_2. Without loss of generality A belongs to ℓ_1.

Suppose that $\ell = \ell_1$ so that ℓ is a multiple component of $S \cap \Pi_{A,B,C}$. In this case the line $\ell_{B,C}$ joining B and C meets S at B with multiplicity at least 2, meaning that $C \in T_B S$ giving a contradiction. Hence $\ell \neq \ell_1$ and similarly $\ell \neq \ell_2$. Suppose $\ell_1 = \ell_2$. Recall that $A \in \ell_1$, and $C \in \ell_1 \cap \ell_2$. So $\ell_{A,C} = \ell_1 \subset S$ giving a contradiction. Hence $\ell_1 \neq \ell_2$.

Thus we have that ℓ, ℓ_1, ℓ_2 are pairwise distinct. Recall that $A \in \ell_1$, and $A \in \ell$. Thus $\ell \cap \ell_1 = A$. If ℓ_1 and ℓ_2 are Galois conjugates then $A \in \ell_2$. As C belongs to one of ℓ_1, ℓ_2 we have $\ell_{A,C} = \ell_1$ or $\ell_2 \subset S$, again giving a contradiction. Therefore ℓ_1, ℓ_2 are K-lines. Moreover the argument shows that $A \notin \ell_2$ Finally $B \in \ell$. We want to show that $B \notin \ell_1 \cup \ell_2$. Since $\ell \cap \ell_1 = A \neq B$, we know that $B \notin \ell_1$. If $B \in \ell_2$, then B is a singular point of $\Pi_{A,B,C} \cap S = \ell \cup \ell_1 \cup \ell_2$, and so $\Pi_{A,B,C} \cap T_B S$ again giving a contradiction. Thus $B \notin \ell_2$. This completes the proof. □

A first step is to find out how many points we need in order to generate all the points of a line that is contained in the cubic hypersurface. We will start by proving that if we have all of them but one, we are able to generate that last point from the previous ones.

Lemma 4.4.4. *Let $\#K \geqslant 5$. Let S be a smooth cubic hypersurface in $\mathbb{P}^n$, where $n \geqslant 3$. Let $\ell \subset S$ be a K-line. Let $B \in \ell(K)$, and write $L = \ell(K) \setminus \{B\}$. Then $\ell(K) \subseteq \langle L \rangle_{MW}$.*

Proof. We have $\#L = \#\ell(K) - 1 = \#K \geqslant 5$. Recall by Proposition 4.2.5 that ℓ contains at most 2 lonely points if char(K) $\neq 2$ and at most 5 lonely point

if char(K) = 2 (in which case $\#K \geqslant 8$). Moreover, by Lemma 4.2.8 there is at most one other point in ℓ that shares the same tangent hyperplane as B. Thus there is some $A \in L$ that is non-lonely, and satisfies $T_A S \neq T_B S$.

We apply Lemma 4.4.3 and distinguish three cases:

1. The first case we consider is (vi)(b). This is illustrated in Figure 4.1. Here the lines ℓ, ℓ_1, ℓ_2 are K-lines and thus so their intersections are

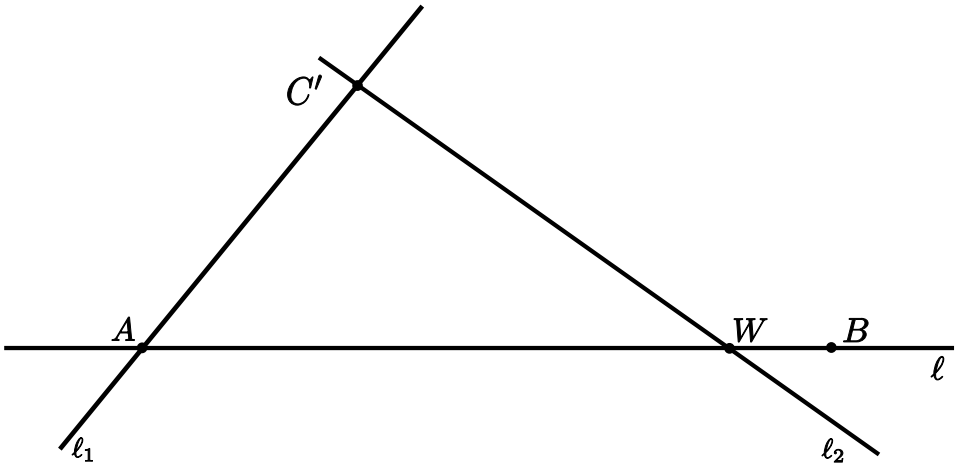


Figure 4.1:

K-points. If $D \in \ell_2(K) \setminus \{C', W\}$ then the K-line joining A and D is tangent to S at A, and so we have

$$\ell_2(K) \setminus \{C', W\} \subseteq \langle A \rangle_{MW}.$$

Similarly

$$\ell_1(K) \setminus \{A, C'\} \subseteq \langle W \rangle_{MW}.$$

Take a point $D \in \ell_2(K) \setminus \{C', W\}$. The line joining D and B meets $\ell_1(K)$ in some point $D' \in \ell_1(K) \setminus \{A, C'\}$. Thus $B \in \langle A, W \rangle_{MW}$. As A, $W \in L$, we have $B \in \langle L \rangle_{MW}$ as required.

2. Q is irreducible and $|Q \cap S| = 2$ as illustrated in Figure 4.2. Note that

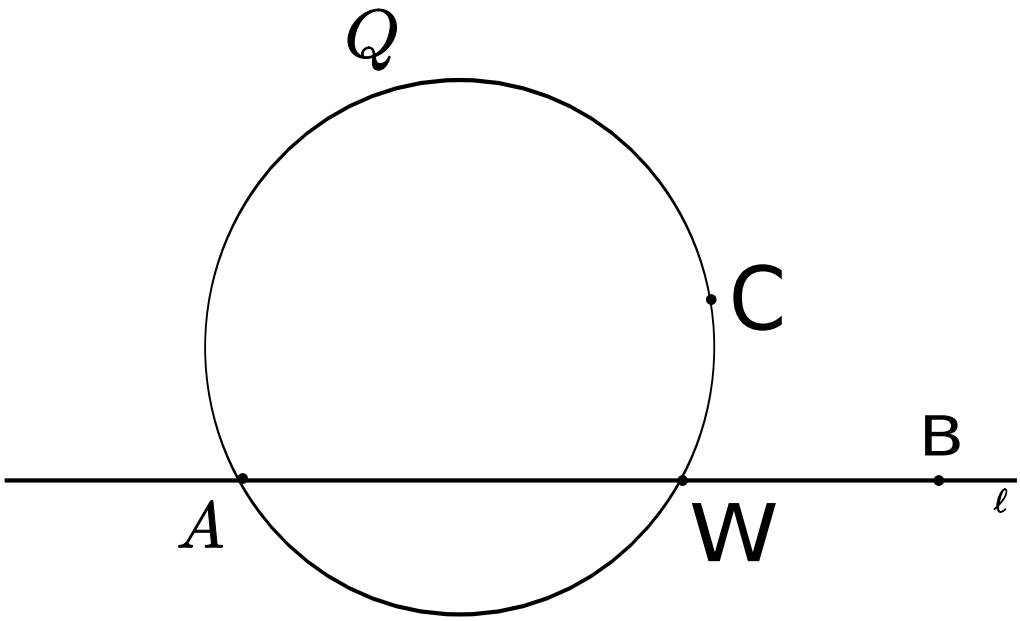


Figure 4.2:

W is a K-point as A is a K-point and $Q \cap \ell = \{A, W\}$. Now by the same argument as above,

$$Q(K) \setminus \{A\} \subseteq \langle A \rangle_{MW}.$$

Now the K-line joining B with C meets Q in some other K-point C' that is neither A nor W. Thus $B \in \langle A, W \rangle_{MW} \subseteq \langle L \rangle_{MW}$ as required.

3. Q is irreducible and $|Q \cap S| = 1$ as illustrated in Figure 4.3. Then $\langle A \rangle_{MW} \subseteq Q(K)$. Consider the K-line joining B and C. This meets Q in another K-point C'. In particular $C, C' \in \langle A \rangle_{MW}$. Thus $B \in \langle A \rangle_{MW} \subseteq \langle L \rangle_{MW}$ as required.

□

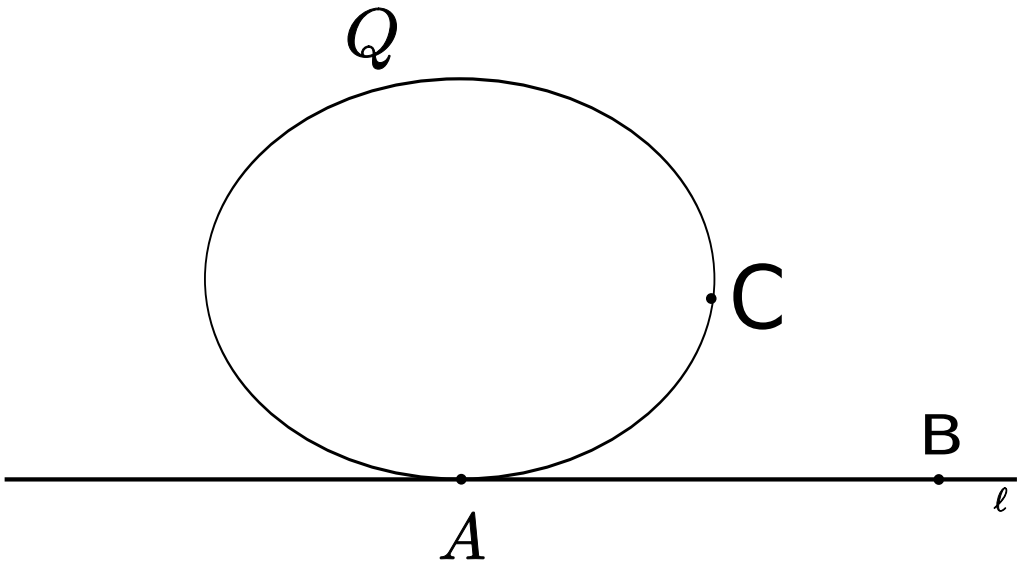


Figure 4.3:

Now we will continue relaxing the number of points that are needed by proving that we if we have generated all points in the line apart from two, then we can generate the remaining ones.

Lemma 4.4.5. *Let $\#K \geqslant 5$. Let S be a smooth cubic hypersurface in $\mathbb{P}^n$ where $n \geqslant 3$. Let $\ell \subset S$ be a K-line. Let $L \subseteq \ell(K)$, such that $|\ell(K) \smallsetminus L| = 2$. Then $\ell(K) \subseteq \langle L \rangle_{MW}$.*

Proof. Let $\ell(K) \smallsetminus L = \{B_1, B_2\}$. As in the proof of Lemma 4.4.4 we can find $A \in L$ which is non-lonely with $T_A S \neq T_{B_1} S$, and $A \neq B_2$. By Lemma 4.4.3 there exists $C \in S(K) \smallsetminus \ell(K)$ such that $C \in T_A S$, $C \notin T_{B_1} S$ and $\Pi_{A,B,C} \cap S = \ell \cup Q$, where Q is either an irreducible conic or the union of two K-lines. If $B' \notin Q$, then following exactly the proof of Lemma 4.4.4 we conclude that $\langle A \rangle_{MW} \supseteq \ell(K)$. If $B' \in Q$, then $B' = W$ where W is as in Figure 4.1 or Figure 4.2. we distinguish two cases.

1. The situation in Figure 4.2. As in the proof of Lemma 4.4.4, we have

$B \in \langle A \rangle_{MW}$. Thus $L \cup \{B\} \subset \langle L \rangle_{MW}$. But $|\ell(K) \setminus (L \cup \{B\})| = 1$. Applying Lemma 4.4.4, we have that $\ell(K) \subset \langle L \cup \{B\} \rangle_{MW} \subseteq \langle L \rangle_{MW}$.

2. The situation in Figure 4.1. As in the proof of Lemma 4.4.4, we have

$$\langle L \rangle_{MW} \supset \langle A \rangle_{MW} \supset \ell_2(K) \setminus \{C', W\}.$$

Let $D \in \ell(K)$ such that $D \neq A$, B, W. In particular $D \in L$. Let $D' \in \ell_2(K)$ such that $D' \neq A$, C'. In particular, $D' \in \langle A \rangle_{MW} \subseteq \langle L \rangle_{MW}$. The K-line joining D and D' meets ℓ_1 in a K-point $D'' \neq A$, C'. Thus $D'' \in \langle L \rangle_{MW}$. Now the line joining B and D'' meets ℓ_2 in a K-point that belongs to $\ell_2(K) \setminus \{C', W\}$. Thus $B \in \langle L \rangle_{MW}$. Hence $\langle L \rangle_{MW} = \langle L \cup \{B\} \rangle_{MW}$. Now we apply Lemma 4.4.4 to deduce $\ell(K) \subset \langle L \rangle_{MW}$.

□

We can now prove that any non-lonely point suffices to generate all the other points of a line that it belongs to. The non-loneliness is necessary, as a lonely point cannot generate anything by itself.

Proposition 4.4.6. *Let $\#K \geqslant 5$. Let S be a smooth cubic hypersurface in $\mathbb{P}^n$, where $n \geqslant 3$. Let $\ell \subset S$ be a K-line. Let $A \in \ell(K)$ be a non-lonely point. Then $\ell(K) \subseteq \langle A \rangle_{MW}$.*

Proof. Let $B \in \ell(K) \setminus \{A\}$ with $T_B S \neq T_A S$. We apply Lemma 4.4.3 and distinguish three cases:

1. The situation in Figure 4.1. As in the proof of Lemma 4.4.4, we have

$$\langle A \rangle_{MW} \supseteq \ell_2(K) \setminus \{C', W\}.$$

However, by Lemma 4.4.5 we know that

$$\ell_2(K) \subseteq \langle \ell_2(K) \smallsetminus \{C', W\} \rangle_{MW},$$

and in particular, $\langle A \rangle_{MW} \supseteq \ell_2(K)$. Thus

$$\langle A \rangle_{MW} \supseteq \langle W \rangle_{MW} \supseteq \ell_1(K) \smallsetminus \{C', A\}.$$

Now if $D \in \ell(K)$ and $D \neq A$, W, then joining D to some $D' \in \ell_1(K) \smallsetminus \{C', A\}$ by a K-line, we obtain as a third point of intersection some $D'' \in \ell_2(K) \smallsetminus \{C', W\}$. This shows that $\ell(K) \smallsetminus \{W\} \subseteq \langle A \rangle_{MW}$. Now Lemma 4.4.4 shows that $\ell(K) \subseteq \langle A \rangle_{MW}$.

2. The situation in Figure 4.2. As in the proof of Lemma 4.4.4 we have

$$Q(K) \smallsetminus \{W\} \subseteq \langle A \rangle_{MW}.$$

Let $D \in \ell(K)$, $D \neq A$, W. Fix $C \in Q(K) \smallsetminus \{A, W\}$. Then the K-line joining C with D meets S in a third K-point $C' \in Q(K) \smallsetminus \{A, W\}$. It follows that $D \in \langle A \rangle_{MW}$. Hence $\ell(K) \smallsetminus \{W\} \subseteq \langle A \rangle_{MW}$, we complete the proof by applying Lemma 4.4.4.

3. The situation in Figure 4.3. This is similar to the previous case but easier.

□

Proposition 4.4.7. *Let $\#K \geqslant 5$. Let S be a smooth cubic hypersurface in $\mathbb{P}^n$ where $n \geqslant 3$. Let $A \in S(K)$ be a non-lonely point. Then $(T_A S \cap S)(K) \subseteq \langle A \rangle_{MW}$.*

Proof. This follows from combining Lemma 4.4.1 and Proposition 4.4.6. □

The natural question that arises is whether we can have any kind of result in the case we have a lonely point.

Lemma 4.4.8. *Let $\#K \geqslant 5$. Suppose* $\mathrm{char}(\mathrm{K}) \neq 2$. *Let S be a smooth cubic hypersurface in $\mathbb{P}^n$ where $n \geqslant 3$. Let $B \in S(K)$ be a lonely point and $A \in S(K)$ non-lonely. Suppose $B \notin T_A S$. Then $\langle A, B\rangle_{MW} \supseteq (T_B S \cap S)(K)$.*

Proof. If $T_A S = T_B S$, then $(T_B S \cap S)(K) = (T_A S \cap S)(K) \subseteq \langle A\rangle_{MW}$, by Proposition 4.4.7. Thus we may suppose $T_A S \neq T_B S$.

Let $C \in (T_B S \cap S)(K)\backslash\{B\}$. We would like to show that $C \in \langle A, B\rangle_{MW}$. If $C \in T_A S$ then this follows from Proposition 4.4.7, so suppose $C \notin T_A S$.

Let ℓ be the K-line that joins B and C. We have that $\ell \not\subseteq T_A S$. As B is lonely, we know (by definition) that $\ell \subset S$. Since $B \in T_A S$, we have that $B \in \langle A\rangle_{MW}$.

Now let $D \in S(K)$ satisfy $T_A S \cap \ell = \{D\}$. Thus $D \in \langle A\rangle_{MW}$. If D is non-lonely, then $\ell(K) \subseteq \langle D\rangle_{MW} \subseteq \langle A\rangle_{MW}$ completing the proof. Thus we may suppose that D is lonely.

Let Π be the unique two dimensional linear variety that contains the point A and the line ℓ. If $\Pi \subset S$, then $\Pi \subset T_A S$ by Lemma 4.3.1 and so $C \in T_A S$, giving a contradiction. Hence we may suppose that $\Pi \not\subset S$. Next we consider $\Pi \cap S$. This is a plane cubic curve that contains ℓ as a component.

First suppose ℓ is a multiple component of $\Pi \cap S$. Now the line $\ell_{A,B}$ meets ℓ with multiplicity $\geqslant 2$ at B and so belongs to the tangent plane $T_B S$. As B is a lonely point, we have $\ell_{A,B} \subset S$. Similarly $\ell_{A,D} \subset S$. Now $\Pi \cap S$ has at least four components counting multiplicity, which is a contradiction.

Hence ℓ is a component of $\Pi \cap S$ of multiplicity 1. Suppose now that $\Pi \cap S$ has another multiple component, which must be a line ℓ_1 say. Then $A \in \ell_1$, and the line $\ell_{A,C}$ meets S with multiplicity $\geqslant 2$ at A. Thus $C \in \langle A \rangle_{MW}$ as required.

From now on, we may suppose that $\Pi \cap S$ does not have multiple components. We distinguish two cases:

(1) $\Pi \cap S = Q \cup \ell$, where Q is a plane conic that is irreducible over $\overline{K}$. Here $A \in Q(K) \setminus \ell(K)$. If $B \in Q \cap \ell$, then B is a singular point of $\Pi \cap S$, and the line connecting B and A would be a tangent at B, and as B is lonely, would be a component of $\Pi \cap S$ giving a contradiction. Thus $B \notin Q \cap \ell$. Similarly $D \notin Q \cap \ell$. Recall that $D \in \langle A, B \rangle_{MW}$. Consider the lines $\ell_{A,B}$ and $\ell_{A,D}$. These meet Q in K-points B', D' such that A, B', D' are pairwise distinct. Clearly D, $D' \in \langle A, B \rangle_{MW}$. Now the line joining B', D' meets ℓ in a K-point $R \neq B$, D. Then $R \in \langle A, B \rangle_{MW}$. As char(K) $\neq 2$, the line ℓ contains at most 2 lonely points, and the points B and D are lonely. Thus R is a non-lonely point. Hence by Lemma 4.4.6, we have $C \in \ell(K) \subseteq \langle R \rangle_{MW}$ as required.

(2) $\Pi \cap S = \ell \cup \ell_1 \cup \ell_2$. Here $A \in \ell_1$, and ℓ_1, ℓ_2 are either K-lines or Galois conjugate. In the second case $A \in \ell_2$ also, and so $\Pi \cap S$ is singular at A, implying that $\Pi \subset T_A S$, and so $C \in T_A S$ giving a contradiction. Hence we may suppose that ℓ_1, ℓ_2 are K-lines, and that moreover $A \notin \ell_2$. As A is non-lonely, $\ell_1(K) \subseteq \langle A \rangle_{MW}$. Let E, F, G be the K-points satisfying

$$\ell_1 \cap \ell_2 = \{E\}, \qquad \ell \cap \ell_1 = \{F\}, \qquad \ell \cap \ell_2 = \{G\}.$$

Then the $E \in \langle A \rangle_{MW}$. The lines joining E to K-points in ℓ are tangent to S at E,

$$\ell(K) \setminus \{F, G\} \subseteq \langle A \rangle_{MW}.$$

The set $\ell(K) \setminus \{F, G\}$ must contain a non-lonely point, H. So $\ell(K) \subseteq \langle H \rangle_{MW} \subseteq \langle A \rangle_{MW}$.

□

We will change the requirements, so that $B \in T_A S$, and therefore we will have the same result regardless of the position of B. The following lemma relies on Lemma 4.3.3, and therefore it inherits the same dimension requirements.

Proposition 4.4.9. *Let K be a finite field, with $\#K \geqslant 5$. Suppose* $\mathrm{char(K)} \neq 2$. *Let S be a smooth cubic hypersurface in $\mathbb{P}^n$ where $n \geqslant 5$. Let $B \in S(K)$ be a lonely point and $A \in S(K)$ non-lonely. Suppose $B \in T_A S$. Then $\langle A, B \rangle_{MW} \supseteq (T_B S \cap S)(K)$.*

Proof. We remark that since $B \in T_A S$, it follows that $B \in \langle A \rangle_{MW}$. If $T_A S = T_B S$, then $(T_B S \cap S)(K) = (T_A S \cap S)(K) \subseteq \langle A \rangle_{MW}$, by Proposition 4.4.7. Thus we may suppose $T_A S \neq T_B S$. Let $C \in (T_B S \cap S)(K) \setminus \{B\}$, we will show that $C \in \langle A, B \rangle_{MW}$. If $C \in T_A S$ then this follows from Proposition 4.4.7, so suppose $C \notin T_A S$.

Let ℓ be the K-line that joins B and C, so then $\ell \not\subseteq T_A S$. As B is lonely, we know (by definition) that $\ell \subset S$. By lemma 4.3.3 there exists a point $D \in (T_A S \cap T_B S \cap S)(K) \setminus \{B\}$. As ℓ contains more than two points and $\mathrm{char(K)} \neq 2$, without loss of generality we may assume that D is non-lonely and $T_B S \neq T_D S$. As $D \in T_B S$, we have that $\ell_{B,D} \subseteq S$, and as $B, D \in T_A S$, we have that $\ell_{B,D} \subseteq T_A S \subseteq \langle A \rangle_{MW}$.

Let Π be the unique two dimensional linear variety that contains ℓ and $\ell_{B,D}$. Then, as B is lonely we have that either $\Pi \cap S = \Pi$ or $\Pi \cap S = \ell \cup \ell_{B,D} \cup \ell_1$, for a line ℓ_1 in S that contains B. If $\Pi \cap S = \Pi$ then the result follows as

$$C \in \Pi \subseteq T_D S \subseteq \langle D \rangle_{MW} \subseteq \langle A \rangle_{MW} \subseteq \langle A, B \rangle_{MW}.$$

In the second case, it suffices to show that there is a non-lonely point $E \in \langle A \rangle_{MW}$ such that $B \notin T_E S$. To see that, let us assume for the moment that such a point does exist, then ℓ_1 meets $T_E S$ in a point $F \neq B$ and

$$F \in T_E S \subseteq \langle E \rangle_{MW} \subseteq \langle A \rangle_{MW}.$$

On the other hand there is $G \in \ell_{B,D}$ so that

$$\ell_{C,F} \cdot S = C + F + G,$$

hence $C \in \langle A, B \rangle_{MW}$. Therefore, it remains to prove that such a point E exists.

By Lemma 4.4.3, there exists a point F in $(T_D S \cap S)(K)$ such that $F \notin T_B S$. Let $\Pi' = \Pi_{B,D,F}$ and $\Pi' \cap S = \ell_{B,D} \cup Q$ for a conic Q.

(1) Suppose that Q is an irreducible conic. As $\#K \geqslant 9$, then the number of points in $Q(K) \setminus \ell_{B,D}(K)$ is at least 7. There are exactly two points in Q that have B in their tangent plane. Furthermore, at most 2 points in Q are lonely. Therefore, we can choose a non lonely point $E \in Q$ such that $E \in T_D S \subseteq \langle A \rangle_{MW}$ and $B \notin T_E S$.

(2) Suppose that $Q = \ell_2 \cup \ell_3$, with $D \in \ell_3$. Any point in $\ell_3 \setminus \{D, \ell_2 \cap \ell_3\}$ does

not contain B in its tangent plane, and as char(K) $\neq 2$, we have that ℓ_3 contains at most 2 lonely points. Hence, we can find a non lonely point $E \in \ell_3$, as required.

□

Proposition 4.4.10. *Let A be a non-lonely point and $B \in \langle A \rangle_{MW}$. Then $T_B S \subseteq \langle A \rangle_{MW}$.*

Proof. As $B \in \langle A \rangle_{MW}$ we have that $\langle B \rangle_{MW} \subseteq \langle A \rangle_{MW}$. If B is non-lonely, then clearly $T_B S \cap S(K) \subseteq \langle B \rangle_{MW}$. In the case that B is lonely, from Proposition 4.4.9 we get that $T_B S \cap S(K) \subseteq \langle A, B \rangle_{MW}$, and the result follows since $B \in \langle A \rangle_{MW}$. □

Theorem 4.4.11. *Let K be a finite field, with $\#K \geqslant 5$. Let A be a point in a smooth cubic hypersurface $S \subseteq \mathbb{P}^n$, where $n \geqslant 5$. If A is lonely, then $\langle A \rangle_{MW} = \{A\}$, else $\langle A \rangle_{MW} \supseteq T_A S \cap S(K)$.*

Proof. Suppose that A is lonely, and that $\langle A \rangle_{MW} \neq \{A\}$. Therefore, there exists a point $B \in \langle A \rangle_{MW} \backslash \{A\}$, and a line $\ell \not\subseteq S$, such that $S \cdot \ell = A + A + B$. Thus, by the definition of the tangent space, $\ell \subseteq T_A S$. As A is lonely, $\ell \subseteq S$, which is a contradiction. On the other hand, if A is non-lonely then the result follows from Proposition 4.4.10. □

Chapter 5

The Mordell-Weil rank over finite fields

In this chapter, we shall investigate the Mordell-Weil rank over finite fields.

5.1 The Mordell-Weil rank over $\mathbb{F}_q$

We shall consider cubic hypersurfaces over a finite field K, such that char(K) $\neq 2$. We have all the tools at hand to consider high dimensional hypersurfaces, therefore we will start with the following theorem.

Theorem 5.1.1. *Let $S \subseteq \mathbb{P}^n$ be a non-singular cubic hypersurface over a finite field K, such that $\#K \geqslant 5$ and* char(K) $\neq 2$. *Suppose that $n \geqslant 6$. Then, for any non-lonely point $A \in S$, we have that $\langle A \rangle_{MW} = S(K)$.*

Proof. Let A be a non-lonely point in S. We make an appropriate transformation so that $A = [1 : 0 : \cdots : 0]$ and $T_A S = \{[x_0 : x_1 : \cdots : x_n] \mid x_n = 0\}$. Let $B \in S$, such that $B \notin T_A S$, and make another transformation so that

$B = [0 : \cdot : 0 : 1]$. Then, an A-normal form for the equation describing S is the following:

$$\begin{aligned} f(x_0, x_1, \ldots, x_n) &= x_0^2 x_n + \alpha x_0 x_n^2 + x_0 x_n \ell_1(x_1, x_2, \ldots, x_{n-1}) \\ &\quad + x_0 q_1(x_1, x_2, \ldots, x_{n-1}) + x_n^2 \ell_2(x_1, x_2, \ldots, x_{n-1}) \\ &\quad + x_n q_2(x_1, x_2, \ldots, x_{n-1}) + c_2(x_1, x_2, \ldots, x_{n-1}) \end{aligned}$$

As A is non-lonely, $T_A S \cap S(K) \subseteq \langle A \rangle_{MW}$. Using Propositions 4.4.9 and 4.4.10, it suffices to show that there exists $C \in T_A S \cap S(K)$ such that $B \in T_C S$. In other words, that there exists $C = [x_0 : x_1 : \ldots : x_{n-1} : 0]$ such that:

$$\left.\begin{aligned} B \cdot (\nabla f)(C) = 0 \\ f(C) = 0 \end{aligned}\right\} \tag{5.1}$$

Equivalently, if the following system has a non-zero solution:

$$\left.\begin{aligned} x_0 q_1(x_1, x_2, \ldots, x_{n-1}) + c_2(x_1, x_2, \ldots, x_{n-1}) = 0 \\ x_0^2 + x_0 \ell_1(x_1, x_2, \ldots, x_{n-1}) + q_2(x_1, x_2, \ldots, x_{n-1}) = 0 \end{aligned}\right\} \tag{5.2}$$

The system (5.2) always has a non trivial solution. As $n \geqslant 6$, using the Chevalley-Warning Theorem (1.6.1), the system also has a non- trivial solution, which leads to the existence of such a point C. □

Corollary 5.1.2. *If $\mathbb{F}_q$ does not have characteristic 2 and $q \neq 3$, then any smooth cubic hypersurface in $\mathbb{P}^n$, $n \geqslant 6$ has Mordell-Weil rank 1 over $\mathbb{F}_q$.*

Proof. Using theorem 5.1.1, we have that any non-lonely point can generate

the whole hypersurface. It is evident that for two lonely points A and B,

$$A \in T_B S, \text{ if and only if } B \in T_A S.$$

Therefore, $\ell_{A,B}$ contains at least one more point, C, which we can by 4.2.9 must be non lonely. Hence, $\langle C \rangle_{MW} = S(K)$. $\square$

Index

Bibliography

[1] J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc, *Arithmtique des surfaces cubiques diagonales*, in Diophantine Approximation and Transcendence Theory, G. Wüstholz, ed., vol. 1290 of Lecture Notes in Mathematics, Springer Berlin Heidelberg, 1987, pp. 1–108.

[2] J. Cooley, *Generators for cubic surfaces with two skew lines over finite fields*, Archiv der Mathematik, 100 (2013), pp. 401–411.

[3] ——, *Cubic Surfaces over Finite Fields*, PhD thesis, University of Warwick, 2014.

[4] S. Galkin and E. Shinder, *The Fano variety of lines and rationality problem for a cubic hypersurface*, arXiv: 1405.5154v2, (2012).

[5] C. G. A. Harnack, *Über vieltheiligkeit der ebenen algebraischen curven*, Mathematische Annalen, 10 (1876), pp. 189–199.

[6] R. C. Hartshorne, *Algebraic Geometry*, vol. 52 of Graduate Texts in Mathematics, Springer-Verlag, 1977.

[7] D. R. Heath-Brown, *The density of zeros of forms for which weak approximation fails*, Mathematics of Computation, 59 (1992), pp. 613–623.

[8] K. Hulek, *Elementary Algebraic Geometry*, American Mathematical Society, 2003.

[9] J. Jahnel, *Brauer groups, Tamagawa measures, and rational points on algebraic varieties*, Habilitationsschrift, Mathematisches Institut, Göttingen, 2008.

[10] Y. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic*, North Holland, 1974.

[11] Y. I. Manin, *Mordell-Weil problem for cubic surfaces*, in Advances in mathematical sciences: CRM's 25 years, vol. 11, AMS, 1997, pp. 313–318.

[12] M. Reid, *Undergraduate Algebraic Geometry*, Cambridge University Press, 1988.

[13] A. Ricolfi, *Bertini's Theorem on Generic Smoothness*, ALGANT Master Thesis, Bordeaux, 2012.

[14] B. Segre, *A note on arithmetical properties of cubic surfaces*, Journal of the London Mathematical Society, 18 (1943), pp. 24–31.

[15] J.-P. Serre, *Local class field theory*, in Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 128–161.

[16] S. Siksek, *On the number of mordell-Weil generators for cubic surfaces*, Journal of Number Theory, 132 (2012), pp. 2610–2629.

[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2009.

[18] A. N. Skorobogatov, *Torsors and Rational Points*, vol. 144 of Cambridge Tracts in Mathematics, Cambridge University Press, 2001.

[19] P. Swinnerton-Dyer, *The Brauer group of cubic surfaces*, Math. Proc. Cambridge Philos. Soc., 113 (1993), pp. 449–460.