The Picard Group and Cubic Surfaces

by

William Fuller

MA4K9 Dissertation

Submitted to The University of Warwick

Mathematics Institute

April, 2024

Contents

Introduction

In this project I explore a a certain type of interesting variant on particular geometric objects, namely the **Picard group**. It turns out that there is a fascinating connection between the integer points on particular types of **cubic surfaces** and its associated Picard groups.

The geometric objects that we consider form the central objects of study in the field of **algebraic geometry**, namely those of **algebraic varieties**. After giving some context to the study of integral points on cubic surfaces in section 1 and why one might care about such a topic, in the subsequent chapter we give a brief outline of some of the fundamental concepts that are encountered in what one might call **classical algebraic geometry**. The primary focus of this area concerns studying particular **algebraic sets** equipped with certain 'natural' topologies.

In the following section, we introduce certain modern ideas in algebraic geometry such as that of a **sheaf**. This will enable us to see how algebraic geometry is studied today; the focus not being solely on topological spaces but additionally on **regular functions** on these spaces. It will be in this section where I define the Picard group for a particular 'nice' class of varieties, namely **non-singular varieties**.

In the latter part of this thesis, I explore the link between cubic surfaces and their associated Picard groups, studying in particular a special type of cubic surface called the **Fermat cubic**. On multiple occasions, I use the computer algebra system **SageMath** to help me do so.

1 Background

1.1 Diophantine Equations

Diophantine equations, namely the concern of finding integer solutions to special types of polynomial equations, typically those with integer coefficients, have been studied since antiquity. Indeed, the Pythagorean triples $(3, 4, 5)$, $(5, 12, 13)$, that is integer solutions to the polynomial equation $x^2 + y^2 = z^2$, were first known to the Babylons nearly 4000 years ago [6]. Taking us to the modern era, the famous **Fermat's last theorem** states that there are no positive integer solutions to the Diophantine equations $x^n + y^n = z^n$. Andrew Wiles proved only as recently as 1995 that the assertion does in fact hold, that was only after many unsuccessful attempts to prove it dating as far back as the 17th century. The moral of this story is then that one cannot be fooled into thinking that a simple to understand proposition involving equally simple Diophantine equations will also be equally easy to solve.

One particular example of where this will be the case and which will be a primary concern of this project will be that of polynomials in three variables of degree 3 in integer coefficients. More concisely, these will be polynomials $f \in \mathbb{Z}[x, y, z]$ with $\max\{i + j +$

$k \mid x^i y^j z^k$ a monomial of $f\} = 3$, and typically f is additionally assumed to be irreducible. Some corresponding Diophantine equations are then $f(x, y, z) = a$ where a is an integer.

One can easily think of examples of Diophantine equations of this form off the top of their heads, namely:

1. $x^3 + y^3 + z^3 = a, \ \ a \in \mathbb{Z}$;
2. $x^2 + y^2 + z^2 - xyz = a, \ \ a \in \mathbb{Z}$;
3. $x^2 + y^2 + z^2 + 2xyz = a, \ \ a \in \mathbb{Z}$;
4. $x^2 z + y^2 z - 2xy = 0$.

The first family of equations corresponds to the sum of three cubes problem [3], with $a = 1$ corresponding to the aforementioned Fermat cubic which will be the cubic surface will be primarily focus on in this thesis. The second family are called **Markoff surfaces**, another example of cubic surface having been studied extensively due to their various symmetric properties, as seen in [7].

With such polynomials, we can view the integer solutions in a wider picture. For example, we may concern ourselves not only about solutions in the integers, but also the rational, real or complex solutions. By desirable properties of the field $\mathbb{C}$[1], often it's preferable to focus on the latter. Moreover, one can view the complex solutions to a Diophantine equation $f(x, y, z) = 0$ of the above form as a subset of $\mathbb{C}^3$,

$$S = \{(x, y, z) \in \mathbb{C}^3 \mid f(x, y, z) = 0\}.$$

In the theory of **manifolds**, S is a 2-dimensional (complex) manifold [10] and so such a set is reasonably called a **cubic surface**[2], and similarly for when the field is $\mathbb{Q}$, $\mathbb{R}$ or arbitrary. Moreover, S is an example of an **algebraic set** which we define in the next section. Before doing that, let's take a look further at why one might be interested in cubic surfaces, and not just any arbitrary Diophantine equation, in particular.

1.2 Affine Cubic Forms

This subsection closely follows that of [7, Section 1]. Here we place the context of cubic surfaces in the wider context. An **affine form** in n-variables is a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ whose leading homogeneous term f_0 is non-degenerate[3] and the polynomials $f - a$ are irreducible over $\mathbb{C}$ for all $a \in \mathbb{C}$. An **affine cubic form** in n-variables is then just an affine

[1] For example $\mathbb{C}$ is **algebraically closed**, meaning that every polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$, the equivalent statements are false for $\mathbb{R}$ and $\mathbb{Q}$. This often makes the theory nicer for $\mathbb{C}$, for example the irreducible polynomials of $\mathbb{C}[x]$, simply correspond to linear polynomials whereas in $\mathbb{R}[x]$ or $\mathbb{Q}[x]$, the irreducible polynomials are more complicated.

[2] The set S and the cubic polynomial f which define such a set are often interchangeably called the cubic surface. Moreover we also interchangeably use the terms integer solutions and integral points for either scenario.

[3] This means f_0 includes all n-variables can't be reduced to a polynomial of fewer than n-variables by a linear change of coordinates.

form in n-variables of degree 3. For an affine cubic form f and for an infinite field k of characteristic zero[4], we define the set

$$V_{k,f} = \{\underline{x} \in k^n \mid f(\underline{x}) = a\}$$

and the subset $V_{a,f}(\mathbb{Z})$ consisting of the integral points. Some immediate questions regarding $V_{a,f}(\mathbb{Z})$ then follow: for which $a \in \mathbb{Z}$ is the set $V_{a,f}(\mathbb{Z})$ non-empty? If so, is $V_{a,f}(\mathbb{Z})$ infinite? **Zariski-dense**[5] in $V_{a,f}$? It turns out that for affine cubic forms in 3 variables that even the initial question is an extremely difficult one to answer and almost nothing is known, even for the simplest affine cubic forms one can think of.

However, in the 'super-critical' case of affine cubic forms in 2 or less variables and the 'sub-critical' case of 4 or more variables, more is known in general. For the case where we have one variable, the question of whether or not $V_{a,f}(\mathbb{Z})$ is easily dealt with by the rational root theorem. Things are more interesting in the case of 2 variables, although the questions regarding the nature of the $V_{a,f}$ is aptly dealt with by **Siegel's theorem on integral points**, which imply that $V_{a,f}(\mathbb{Z})$ is finite for every a and moreover that $V_{a,f}$ is non-empty for only a few **admissible**[6] a.

For the sub-critical case, it was proved by Roger Heath-Brown and Tim Browning in [5] that if f is an affine cubic form in $n \geq 10$ variables such that f_0 is non-singular[7], then for all but finitely many admissible k, $V_{a,f}(\mathbb{Z})$ is Zariski-dense (and hence infinite). Furthermore, it's conjectured that for $n \geq 4$, $f = f_0$ non-singular, then $V_{a,f}(\mathbb{Z})$ is also Zariski-dense for all but finitely many admissible a.

The previous conjecture does not hold in general for when $n = 3$. For example, for the non-singular cubic form $f(x, y, z) = x^2 + y^2 + z^2 + 2xyz$, if for example $c = 2^{2b}$ for some positive integer b, then we have only finitely many solutions, see [15] for more details. As we have no such analogous results for the case when $n = 3$ it proves especially fruitful to look at specific examples. This leads us on to the next subsection.

1.3 Sums of Three Cubes

An example of a affine cubic form that has been studied intensely is the sum of three cubes polynomial

$$f = x^3 + y^3 + z^3. \tag{1}$$

[4] The characteristic of a ring is the smallest number of copies of 1 the identity element that sum to give 0, and if no such number exists then a ring is said to have characteristic zero. We have this assumption to ensure that the integers are a subring.

[5] It'll be clear what this means in the next section. For now, it's worth knowing that this is stronger than $V_{a,f}$ being infinite.

[6] This just means all the integers which aren't ruled out by **local congruence obstructions**, which essentially means there can't be solutions by considering the equation $f(\underline{\mathrm{x}}) = a \bmod m$.

[7] We'll get on to what it means for a variety to be non-singular in section 3, and essentially a polynomial is defined to be non-singular if its corresponding variety is.

If $a \equiv 4, 5 \mod 9$, since cubes can only take the values $0, \pm 1 \mod 9$, we can deduce that $V_{a,f}(\mathbb{Z})$ is empty for such a. However for a not of this form i.e. k is admissible, it is an open problem as to whether or not $V_{a,f}(\mathbb{Z}) \neq \emptyset$ for all such a.

There have been further conjectures regarding the distribution of the integral points corresponding to each integer a, namely the one by Heath-Brown [9] asserts that for each non-cube integer a, we have an asymptotic formula for the number integral points within the box $[-B, B]^3$ that satisfy the equation $f(x, y, z) = a$. More precisely, for fixed $a > 0$, $N(B) = \{(x, y, z) \in \mathbb{Z}^3 \mid F(x, y, z) = a, \max(|x|, |y|, |z|) \leq B\}$, we have

$$N(B) \sim \frac{1}{9} \frac{\Gamma(\frac{1}{3})^2}{\Gamma(\frac{2}{3})} \prod_{p\ prime} \sigma_p^{(a)} \log B \tag{2}$$

where

$$\sigma_p^{(a)} = \lim_{l \to \infty} \frac{\#\{(x, y, z) \in (\mathbb{Z}/p^l\mathbb{Z})^3 \mid f(x, y, z) = 0 \mod p^l\}}{p^{2l}}$$

and Γ corresponds to the Gamma function. In particular, the conjecture is not only that $V_{a,f}(\mathbb{Z}) \neq \emptyset$ for all admissible a but in fact $V_{a,f}(\mathbb{Z})$ is infinite.

Heuristically then, because of the log term, we expect the number of solutions to grow very slowly. This prediction has been supported by extensive computer searches: beginning in 1954, a search conducted by Miller and Woollett [13] found solutions for all but 9 of the 69 admissible $a < 100$ in the region $\{(x, y, z) \in \mathbb{Z}^3 \mid \max\left(|x|, |y|, |z|\right) \leq 3164\}$. Moreover, it wasn't until as recently as 2019 that the first solution was found for $a = 42$ by Booker and Sutherland [3],

$$(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42$$

the last admissible $a < 100$ for which a solution, until that point, had yet to be found.

1.4 The Fermat Cubic

Heath-Brown's conjecture concerns that of integral solutions to $x^3 + y^3 + z^3 = a$ where a is not a cube number. One may also want to study what happens when this is not the case e.g. for the Fermat cubic. Something that we encounter in this case (and hence for all cubes a[8]) is that of parametric solutions. For example, in 1936 K. Mahler discovered the degree 4 parametrisation

$$r(t) = (9t^4, -9t^4 + 3t, -9t^3 + 1), \tag{3}$$

That is, $(9t^4)^3 + (-9t^4 + 3t)^3 + (-9t^3 + 1)^3 = 1$ for any t and so we see by varying $t \in \mathbb{Z}$, since we have polynomials with integer coefficients, we generate infinitely many integer solutions to the equation $x^3 + y^3 + z^3 = 1$.

[8] We have $x^3 + y^3 + z^3 = 1$ if and only if $(bx)^3 + (by)^3 + (bz)^3 = b^3$, and so the integer solutions for $a = b^3$ correspond to those for $a = 1$ multiplied by a factor of b.

Furthermore in 1956, Lehmer [11] in fact discovered an infinite family of parametrisations, given by recurrence relations in x, y and z, with initial conditions given by (3): Let $(x_k(t), y_k(t), z_k(t))$, $k \geq 0$ be a 3-tuple of recurrence relations with initial conditions

$$\begin{aligned}(x_0(t), y_0(t), z_0(t)) &= (9t^4, 3t - 9t^4, 1 - 9t^3),\\ (x_1(t), y_1(t), z_1(t)) &= (9t^4, -3t - 9t^4, 1 + 9t^3),\end{aligned} \tag{4}$$

and recurrences given by

$$\begin{aligned}x_{n+1}(t) &= 2(216t^6 - 1)x_n(t) - x_{n-1}(t) - 108t^4,\\ y_{n+1}(t) &= 2(216t^6 - 1)y_n(t) - y_{n-1}(t) - 108t^4,\\ z_{n+1}(t) &= 2(216t^6 - 1)z_n(t) - z_{n-1}(t) + 216t^4 + 4,\end{aligned} \tag{5}$$

then we have $(x_k(t))^3 + (y_k(t))^3 + (z_k(t))^3 = 1$ for all $k \geq 0$.

The problem with parametrisations such as the ones above is that most solutions found from a computer search will be of this form, for example for $x^3 + y^3 + z^3 = 1$, of the approximately 100,000 solutions found in the region $\min\big(|x|, |y|, |z|\big) \leq 10^{15}$, only around 3500 do not lie on the quartic parametrisation (3). This is since degree n parametrisations, that is a parmetrisation with two of its coordinates degree n polynomials[9], contribute roughly $B^{\frac{1}{n}}$ to the counting function $N(B)$, which grows much faster than any power of $\log B$, the rate at which the solutions are predicted to grow by in (**??**).

1.5 The Overarching Problem

In general, we want to understand the nature of integral points on cubic surfaces. As for the sum of three cubes, a concrete way of doing so is by giving a prediction for the asymptotic behaviour for the number of integral points $N(B)$ within a given bound B as in (2). It's then natural to ask if we can give any sensible predictions for various other types of cubic surfaces.

Before going on to state any current predictions, it's worth mentioning the well-known **Manin's conjecture**. Very crudely, this concerns the behaviour of rational points of a special type of smooth (non-singular) variety called a Fano variety defined over a number field k. For such a variety V, an associated height function which counts $N(B)$ which counts the rational points of a certain height is conjectured to be asymptotic (as $B \to \infty$) to a function in B of the form

$$cB^a (\log B)^{b-1}$$

where c is a known constant, a and b geometric invariants of V, where, in particular, b is related to the rank of the Picard group of V.

By the work of Tim Browning and Florian Wilsch, we have a similar prediction as was given in [20] for integral points on a smooth variety, again subject to other 'niceness'

[9] We will see why parametrisations on the Fermat cubic must be of this form later in section 4.

conditions. Here, although we're concerned about the integer solutions to the equation $f = 0$ for $f \in \mathbb{Z}[x, y, z]$ (irreducible) of degree 3, we also want to consider the rational solutions which we denote by the set U. Moreover, we also want to consider a modified counting function $N'(B)$ which excludes any integral points which lie on parametrisations of the form that we encountered in the previous section (we will go into more detail about these in section 4). Then we have the heuristic,

$$N'(B) \sim c(\log(B))^{\rho_U + b} \tag{6}$$

as $B \to \infty$, where b and c are again geometric invariants of our surface, and ρ_U is the rank of the Picard group of the variety U.

We shall explore this asymptotic formula later in section 4 and make sense of some of the terms introduced in subsection 3.3. For now, lets move on to the fundamentals of algebraic geometry.

2 Classical Algebraic Geometry

In this section we will give a summary of the fundamental aspects of classical algebraic geometry. The content will be in a large part similar to that appearing in Chapter 2 of [14].

2.1 Affine Algebraic Sets

To begin, let k an algebraically closed field of characteristic zero (e.g. $\mathbb{C}$). An **affine algebraic set** of k^n is a subset $X \subset k^n$ such that X is the common zero set of a collection of polynomials $S \subset k[x_1, \ldots, x_n]$, that is:

$$X = V(S) = \left\{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \quad \forall f \in S\right\}.$$

We have our first elementary result for algebraic sets, namely that 'applying V'[10] is inclusion reversing:

$$S \subset S' \implies V(S) \supset V(S'). \tag{7}$$

Instead of thinking in terms arbitrary subsets of $k[x_1, \ldots, x_n]$, we can think in terms of ideals. The reasoning for this is that for an ideal $\mathfrak{a}$ of $k[x_1, \ldots, x_n]$ that is generated by a set $S \subset k[x_1, \ldots, x_n]$ we have that [14, p.37]

$$V(\mathfrak{a}) = V(S). \tag{8}$$

It turns out that the algebraic subsets of k^n form the closed subsets of a topology

[10] we can make precise the statement 'applying V' by thinking of it as a function from the power set of $k[x_1, \ldots, x_n]$ to the power set of k^n given by $S \mapsto V(S)$.

known as the **Zariski topology**. We deduce this from the following relations [14, Prop 2.10.]:

Proposition 2.1.

(a) $\emptyset = V(1)$, $k^n = V(0)$;

(b) $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ *for all ideals* $\mathfrak{a}, \mathfrak{b} \subset k[x_1, \ldots, x_n]$;

(c) $V(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} V(\mathfrak{a}_i)$ *for every family of ideals* $(\mathfrak{a}_i)_{i \in I}$.

Remark 2.1. When k^n is considered as a topological space with the Zariski topology we denote it by $\mathbb{A}^n$ as the unchanged notation is typically reserved for when k^n is a vector space.

Although open sets in the Zariski topology are also open in the Euclidean topology, the converse is not true - the Zariski topology is coarser. On the whole they are quite different, for the Euclidean topology we have that it is Hausdorff, meanwhile for the Zariski topology the open sets are dense in $\mathbb{A}^n$ and so can't possibly be Hausdorff.[11]

2.2 Algebraic Fundamentals

The power of algebraic geometry lies in the translating problems of Geometry to ones of Algebra. As affine algebraic sets are common zero loci of polynomials in the commutative ring $k[x_1, \ldots, x_n]$, we can study properties of such rings in isolation and relate them back to properties of the corresponding geometric objects, the theorem which relates such objects is that of **Hilbert's Nullstellensatz** which we'll state later on.

In the study of (commutative) ring theory, the unlike group theory where we often study a group by looking at subgroups of it, for rings the more 'natural' subobject to consider is not subrings in general but a special type of subring, namely **ideals**. The three types we primarily care about are as follows:

- **maximal ideals** - these are ideals $\mathfrak{m} \subset R$ such that if we have $\mathfrak{m} \subset I \subset R$ then $I = \mathfrak{m}$ or $I = R$.
- **prime ideals** - these are ideals $\mathfrak{p} \subset R$ such that if $ab \in \mathfrak{p}$ then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. These generalise the notion of prime numbers, indeed the prime ideals of $\mathbb{Z}$ are the zero ideal (0) and (p) where $p \in \mathbb{N}$ is prime.
- **radical ideals** - these are ideals $I \subset R$ which are equal to their **radicals** $\sqrt{I}$ that is the ideal defined as

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}.$$

[11] This follows from the topological fact that the intersection of two **open** dense sets is also dense, the assumption that the sets are open being key here e.g. $\mathbb{Q}$ and $\mathbb{R} \backslash \mathbb{Q}$ are both dense in $\mathbb{R}$ (with respect to the Euclidean topology) but their intersection is empty.

Definition 2.1. A ring R is said to be **Noetherian** if every ideal is finitely generated.

It turns out that a ring being Noetherian is equivalent to it satisfying the **ascending chain condition**: every chain of ideals

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

eventually terminates, that is there exists a k such that $I_k = I_{k+1} = \ldots$. The following theorem allows us to deduce that every algebraic set is the common zero loci of finitely many polynomials.

Theorem 2.1 (Hilbert's Basis Theorem)**.** *The ring $k[x_1, \ldots, x_n]$ is Noetherian.*

For a proof of the theorem, see [1, p. 81] - it essentially follows from induction on the fact that if R is noetherian then $R[x]$ is also.

As we saw in (8), for an affine algebraic set $V(S) \subset \mathbb{A}^n$ where S is a subset of $k[x_1, \ldots, x_n]$, $V(S) = V(I)$ where I is the ideal generated by S. Then the above theorem says that I is finitely generated i.e $I = \langle f_1, \ldots, f_r \rangle$ for some $f_1, \ldots, f_r \in I$ and hence $V(S) = V(f_1, \ldots, f_r)$.

Another result first proved by Hilbert which is of fundamental importance to the subject of algebraic geometry is the following:

Theorem 2.2 (Weak Nullstellensatz)**.** *If $\mathfrak{a} \subsetneq k[x_1, \ldots, x_n]$ is a proper ideal then $V(\mathfrak{a}) \neq \emptyset$.*

In other words if I is a proper ideal, then there is a point $p \in \mathbb{A}^n$ such that $f(p) = 0$ for all polynomials in I. For a proof, see [1, Cor 7.10.].

Just as we have V('algebraic object') gives us a geometric set, we also have the analogous operation I where I('geometric set') gives us an algebraic object: for an affine algebraic set $W \subset \mathbb{A}^n$ we define $I(W)$ to be the set

$$I(W) = \left\{ f \in k[x_1, \ldots, x_n] \mid f(p) = 0 \quad \forall p \in W \right\}.$$

This turns out to be a radical ideal of $k[x_1, \ldots, x_n]$. Moreover, we have the following relation [17, p. 19]:

$$V(I(W)) = W. \tag{9}$$

Theorem 2.3 (Nullstellensatz)**.** *Let $\mathfrak{a} \subset k[x_1, \ldots, x_n]$ be an ideal. Then*

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

In particular if $\mathfrak{a}$ is a radical ideal then $I(V(\mathfrak{a})) = \mathfrak{a}$. Combining this with (9) we get a 1-1 correspondence between the radical ideals of $k[x_1, \ldots, x_n]$ and the algebraic subsets of $\mathbb{A}^n$.

Moreover, another consequence of the (weak) Nullstellensatz is that maximal ideals of $k[x_1, \ldots, x_n]$ are precisely the ideals of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ with the a_i's in

k and clearly $V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$, giving us a 1-1 correspondence between maximal ideals of $k[x_1, \ldots, x_n]$ and points of $\mathbb{A}^n$.

Definition 2.2. A topological space is said to be **irreducible** if it can't be written as a union of two proper closed subsets.

In other words, if $X = A \cup B$ is an irreducible topological space with A and B closed then either $X = A$ or $X = B$. It's a standard topological exercise to prove that all irreducible topological spaces are connected. In Algebraic Geometry, the topological notion of irreducibility will be to the Zariski topology what connectedness is to the Euclidean topology; irreducible algebraic sets will form the 'building blocks' for arbitrary algebraic sets like the connected components do for say, topological manifolds[12].

Similar to the two correspondences above, there exists another, namely there's a 1-1 correspondence between prime ideals of $k[x_1, \ldots, x_n]$ and irreducible algebraic subsets of $\mathbb{A}^n$ which involves showing that for an irreducible algebraic set $V \subset \mathbb{A}^n$ the radical ideal $I(V)$ is also prime and moreover for a prime ideal $\mathfrak{a} \subset k[x_1, \ldots, x_n]$, $V(a)$ is irreducible [14, prop 2.27.]. Hence in summary we have:

$$\begin{aligned} \text{radical ideals of } k[x_1, \ldots, x_n] &\longleftrightarrow \text{algebraic subsets of } \mathbb{A}^n \\ \text{prime ideals of } k[x_1, \ldots, x_n] &\longleftrightarrow \text{irreducible algebraic subsets of } \mathbb{A}^n \\ \text{maximal ideals of } k[x_1, \ldots, x_n] &\longleftrightarrow \text{points of } \mathbb{A}^n. \end{aligned} \tag{10}$$

Moreover with such a notion of irreducibility, we can give a sensible definition for the **dimension** of an algebraic set. Namely, for an algebraic set $V \subset \mathbb{A}^n$ equipped with the subspace topology, the **dimension** of V denoted $\dim(V)$, is the maximal length of the chains

$$V_0 \subset V_1 \subset \ldots \subset V_d$$

where the V_i's are distinct non-empty irreducible algebraic subsets of V.

2.3 Coordinate Ring

For an affine algebraic set $V \subset \mathbb{A}^n$ the **coordinate ring** of V is defined as

$$k[V] := \frac{k[x_1, \ldots, x_n]}{I(V)},$$

the elements of $k[V]$ are called **regular functions**. By definition, these are equivalence classes of polynomials in $k[x_1, \ldots, x_n]$ which coincide on V, but we can also think as the elements more generally as functions on V, and sometimes we may want to represent an equivalence class by a function that isn't a polynomial. For example, on the affine algebraic

[12] We later explore the connection between manifolds and their equivalent object in algebraic geometry in 3.3.

set $V = V(xy-1) \subset \mathbb{A}^2$, the function $V \to k$, $(x,y) \mapsto \frac{1}{x}$ (which is well-defined as V doesn't contain the y-axis) coincides with the polynomial function y.

Via the quotient map $\pi : k[x_1,\dots,x_n] \to k[V]$, we have a bijection between radical, prime and maximal ideals of $k[V]$ and radical, prime and maximal ideals of $k[x_1,\dots,x_n]$ containing $I(V)$ respectively, giving us an analogous correspondence to that of (10) between ideals of the coordinate ring $k[V]$ and algebraic subsets of V by simply replacing $k[x_1,\dots,x_n]$ with $k[V]$ and $\mathbb{A}^n$ with V. This is consistent with (10) since for the affine algebraic set $V = \mathbb{A}^n$ as $k[\mathbb{A}^n] = k[x_1,\dots,x_n]$.

2.4 Projective Algebraic Sets

Another set we consider is that of projective space $\mathbb{P}^n$. Often it's preferable to work in projective space rather than affine space, there being numerous reasons for doing so. One reason being that projective space $\mathbb{P}^n$ can be viewed as a natural compactification[13] of $\mathbb{A}^n$ i.e. points 'added at infinity' in a particular way.

We denote the set of lines through the origin in k^n by $\mathbb{P}^n$, that is

$$\mathbb{P}^n = \left(k^{n+1} - \{0\}\right) / \sim$$

where $\sim$ is the equivalence relation given by $x \sim y \in k^n$ if and only if $x = \lambda y$ for some $\lambda \in k^\times$. We call such a set **projective $n-$space**, often omitting the n variable.

Elements of $\mathbb{P}^n$ are written in the form $[a_0 : \dots : a_n]$; this is the equivalence class containing the point $(x_0,\dots,x_n)$ in k^n. This is convenient since similarly to affine algebraic sets, we're provided with global coordinates which can be used to explicitly describe subsets of $\mathbb{P}^n$.

We have an immediate connection between the sets $\mathbb{P}^n$ and $\mathbb{A}^n$: for each $0 \leq i \leq n$ define the subset $U_i \subset \mathbb{P}^n$ by

$$U_i = \{[a_0 : \dots : a_i : \dots : a_n] \in \mathbb{P}^n \mid a_i \neq 0\}^{14}.$$

Then we easily see that the complement, $\mathbb{P}^n \backslash U_i$ is in bijection with $\mathbb{P}^{n-1}$ and that $\mathbb{P}^n = \bigcup_i U_i$.

Moreover, for each i we have a bijection[15] $u_i : U_i \to \mathbb{A}^n$ given by

$$[a_0 : \dots : a_n] \mapsto \left(\frac{a_0}{a_i}, \dots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i}\right). \tag{11}$$

[13] An example of another compactification is that of adding a single point ∞ to the complex plane $\mathbb{C}$ and from which we can define a topological space $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$ that is homeomorphic to the (compact) 2-sphere.

[14] This is well-defined as $a_i \neq 0$ if and only if $\lambda a_i \neq 0$ for $\lambda \neq 0$

[15] This bijection is made clear from the fact that $[a_0 : \dots : a_n]$ and $[\frac{a_0}{a_i} : \dots : \frac{a_{i-1}}{a_i} : 1 : \frac{a_{i+1}}{a_i} : \dots : \frac{a_n}{a_i}]$ are the same elements in U_i and so our map is simply 'removing the 1' from our latter representation and inverse equivalent to 'adding 1'.

Hence, since $\mathbb{P}^n = U_0 \cup (\mathbb{P}^n \backslash U_0)$, the former in bijection with $\mathbb{A}^n$ and the latter in bijection with $\mathbb{P}^{n-1}$, we get $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$ and so the points added to $\mathbb{A}^n$ 'at infinity' to produce $\mathbb{P}^n$ as hinted at in the first paragraph of this section correspond to the set $\mathbb{P}^{n-1}$ (such a statement will be made more precise once we give $\mathbb{P}^n$ a suitable topology).

Given a **homogeneous** polynomial $f \in k[x_0, \ldots, x_n]$ of degree d, we get that the algebraic subset $V(f)$ of $\mathbb{A}^{n+1}$ descends to a well defined subset of $\mathbb{P}^n$ since $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in k$ and so the zero loci of f consists of lines through the origin. In exactly the same way, for an arbitrary collection of homogeneous polynomials, $\{f_i\}_{i \in I}$, $V(\{f_i\}_{i \in I})$ is a well-defined subset of $\mathbb{P}^n$. We call such a subset a **projective algebraic set**.

As we had for algebraic sets, instead of considering the common zero loci of a collection of polynomials in $k[x_0, \ldots, x_n]$, we instead often consider ideals of $k[x_0, \ldots, x_n]$, since as we saw, the common zero locus of a collection of polynomials and the ideal generated by such polynomials are the same. We do the same for projective algebraic sets, but this time we care about **homogeneous ideals**[16] which correspond precisely to ideals generated by homogeneous polynomials. We also have the same relations for projective sets as we have in Prop. 2.1 for algebraic sets, from which we can similarly define a topology on $\mathbb{P}^n$ that have as their closed sets projective algebraic sets and which we also call the **Zariski topology** on $\mathbb{P}^n$.

The subsets U_i as given above are in fact Zariski-open in $\mathbb{P}^n$ ($U_i = \mathbb{P}^n \backslash V(x_i)$) and fortunately for us the subspace topology on any $U_i \subset \mathbb{P}^n$ coincides with the Zariski topology on $\mathbb{A}^n$ (see [17, ex 3.2.2]). As a result the collection $\{U_i\}_{0 \leq i \leq n}$ is often called an **affine chart** of $\mathbb{P}^n$, in analogy to those for manifolds. Along these lines, for an affine algebraic set $V \subset \mathbb{A}^n$ and $\mathbb{A}^n$ identified as a subset of $\mathbb{P}^n$, The **projective closure** of V, denoted by $\overline{V}$, is then the Zariski-closure of V in $\mathbb{P}^n$.

and the projective closure of $\mathbb{A}^n$ is $\mathbb{P}^n$.

We also have the same associated algebraic structures as for affine algebraic sets. Namely for a projective algebraic set $V \subset \mathbb{P}^n$ we have the associated ideal $I(V)$ consisting of all polynomials in $k[x_0, \ldots, x_n]$ that vanish identically on V which we call the **homogeneous ideal** of the projective set V.

Likewise, we define the **homogeneous coordinate ring** of a projective set V to be the ring

$$k[V]_{hom} = \frac{k[x_0, \ldots, x_n]}{I(V)}$$

but in this case we can't think of the elements of this ring as regular functions on $V \subset \mathbb{P}^n$; for $V = \mathbb{P}^n$ in particular, the only regular functions on $\mathbb{P}^n$ are the constant functions.

[16] In various commutative algebra textbooks e.g. [1], these are called **graded** ideals which are ideals such that if a polynomial f is in the ideal then so are all the homogeneous components f_d, where d the degree of f_d.

3 The Picard Group

In the previous section we introduced the notion of an algebraic set. However, we have not yet defined what it means for any two such geometric objects to be isomorphic or 'essentially the same thing'. In classical algebraic geometry, for affine algebraic sets for example, a morphism between $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ is a restriction of a **polynomial map** $f : \mathbb{A}^n \to \mathbb{A}^m$ i.e. $f(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$ where the g_i's are polynomials in $k[x_1, \ldots, x_n]$. An isomorphism is then just a bijective morphism whose inverse is also a morphism and two sets are isomorphic if there exists an isomorphism between them. The issue with this is that the definition requires that we give explicit embeddings for V and W. One way around this is by taking the more modern approach to algebraic geometry, namely studying such geometric objects is done by studying certain types of functions on them. This brings us on to our first definition.

3.1 Sheaves

Note that throughout this section unless specified we will assume our underlying field k to be algebraically closed.

Definition 3.1. Let V a topological space and suppose that for every open subset $U \subset V$ we have a set $\mathcal{O}_V(U)$ consisting of functions $U \to k$. We say that $\mathcal{O}_V$ is a **sheaf** of k-algebras if the following hold for every open subset U:

(a) $\mathcal{O}_V(U)$ is a k-subalgebra of the k-algebra consisting of all functions $U \to k$;

(b) If $f \in \mathcal{O}_V(U)$ then $f|_{U'} \in \mathcal{O}_V(U')$ for every open subset U' of U;

(c) For a function $f : U \to k$, if we have an open cover $U = \bigcup_{i \in I} U_i$ and $f|_{U_i} \in \mathcal{O}_V(U_i)$ for all $i \in I$ then $f \in \mathcal{O}_V(U)$.

Moreover if we have a sheaf $\mathcal{O}_V$ of k-algebras then the sets $\mathcal{O}_V(U)$ are called **sections** of $\mathcal{O}_V$ over U and is interchangeably denoted by $\Gamma(U, \mathcal{O}_V)$.

The properties (b) and (c) of a sheaf are typically called the **locality** and **gluing** properties respectively. The definition at first can seem pretty abstract and it's not immediately clear what a sheaf for particular topological spaces may look like, although one has likely encountered many in their mathematical study:

Examples 3.1.

- For any topological space V and for each open subset U of V we have $\mathcal{O}_V(U)$ consists all functions $U \to k$. Then $\mathcal{O}_V$ is trivially a sheaf of k-algebras.
- For any topological space V if $\mathcal{O}_V(U)$ consists of all real-valued continuous functions on $\mathbb{R}$(equipped with the standard topology), then we have a sheaf of $\mathbb{R}$-algebras:

for (a), the constant functions are continuous; the sum and product of continuous functions are also continuous. For (b), it follows from the fact that restrictions of continuous maps are continuous. (c) follows from the fact that a function $f : U \to \mathbb{R}$ is continuous if and only if it's locally continuous[17], and gluing a compatible family of continuous functions clearly results in a locally continuous and hence a continuous function.

- For $V = \mathbb{C}^n$, $U \subset \mathbb{C}^n$ open and $\mathcal{O}_{\mathbb{C}^n}(U)$ consisting of all analytic functions $f : U \to \mathbb{C}$ then $\mathcal{O}_{\mathbb{C}^n}$ is a sheaf of $\mathbb{C}$-algebras for similar reasons as for continuous functions: differentiability is a local property, that is in order to know differentiability at a point x we only need to know what values a function takes in a small open neighbourhood of x rather than what's happening on the whole space.

- (**non-example**) Let $V = \mathbb{R}$ and let $\mathcal{O}_V(U)$ consist of all bounded real functions $f : U \to \mathbb{R}$. Such sets do not necessarily form a sheaf: for $U = \mathbb{R}$ we have an open cover $\mathbb{R} = \cup_{n \in Z}(n, n+2)$ then the identity function $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x$ restricts to bounded functions on the open cover but is itself not bounded; boundedness of a function is a global property rather than a local one i.e. it is not defined pointwise.

Moreover, we can construct new sheaves from old: let $\mathcal{O}_V$ be a sheaf of k-algebras and $U \subset V$ open, then one can easily verify that $\mathcal{O}_U := \mathcal{O}_V|_U$ which is the collection of sections $\mathcal{O}_V(U')$ of $\mathcal{O}_V$ for $U' \subset U$ open, is also a sheaf. Now, let us introduce some preliminary definitions regarding sheaves.

Definition 3.2. Let V a topological space and $\mathcal{O}_V$ an associated sheaf of k-algebras. Then we call the pair $(V, \mathcal{O}_V)$ a $k-$**ringed space**.

Definition 3.3. Let $(V, \mathcal{O}_V)$ a k-ringed space and let $p \in V$. A **germ** of a function at p is an equivalence class of pairs (f, U) with $f \in \mathcal{O}_V(U)$, U an open neighbourhood of p where $(f, U) \sim (f', U')$ if and only if f and g agree on some smaller open neighbourhood V of p with $V \subset U \cap U'$. The germs of functions at p form a k-algebra[18] denoted by $\mathcal{O}_{V,p}$ which we call the **stalk** of the sheaf $\mathcal{O}_V$ at p.

Remark 3.1. In the language of **category theory**, the definition of the stalk of $\mathcal{O}_V$ at p corresponds to the **direct limit** over the sections $\mathcal{O}_V(U)$ with U an open neighbourhood of p. For a more precise definition, see [8, §2.1].

Having now introduced the general terminology, we now focus on when our topological space is an affine algebraic set. As such sets are defined by polynomials, we ought to want

[17] A function $f : X \to Y$ is **locally continuous** if every $x \in X$ has an open neighbourhood $U \subset X$ for which $f|_U$ is continuous. It's then a standard exercise in topology to show that this is equivalent to a function being continuous.

[18] Addition and multiplication in $\mathcal{O}_{v,p}$ is defined by $(f, U) + (g, V) := (f + g, U \cap V), (f, U) \cdot (g, V) = (fg, U \cap V)$. One can easily verify that such operations are well-defined i.e. the sum and product are independent of the chosen representatives for a given germ and that it is indeed a k-algebra.

to consider functions of a similar flavour. Such an appropriate class consists of what we called **regular** functions which we define below.

Definition 3.4. Let V an affine algebraic set and $U \subset V$ open. A function $f : U \to k$ is called **regular** at a point $p \in U$ if there exists an open neighbourhood $U' \subset U$ of p for which $f(x) = \frac{g(x)}{h(x)}$ for all $x \in U'$ with $g, h \in k[V]$ and $h(p) \neq 0$. We say that a function $f : U \to k$ is regular if it's regular at all points of U.

In other words a regular function looks on U locally like an element of the **function field** $k(V)$ which is defined to be just the field of fractions of the coordinate ring $k[V]$.

Proposition 3.1. *Let $\mathcal{O}_V(U)$ be the set consisting of regular functions $U \to k$ on an affine algebraic set V. Then $\mathcal{O}_V$ is a sheaf of k-algebras.*

Proof. We need to check that $\mathcal{O}_V$ satisfies the properties in Def. 3.1. But similar to the sheaf of continuous functions, regularity is a local property i.e. it's defined pointwise and so (b) and (c) are immediate.

To check (a), it's clear that constant functions are regular: a and $\frac{a}{1}$ agree as functions on all of U. for f, f' regular on U and a point $p \in U$ we have $f = \frac{g}{h}$, $f' = \frac{g'}{h'}$ for some $f, f', g, g' \in k[V]$, h, h' non-zero on some open neighbourhood $U' \subset U$ of p. Then $f + f' = \frac{gh' + g'h}{hh'}$ on U' and similarly $ff' = \frac{gg'}{hh'}$ on U' that is both are quotients of functions in the coordinate ring $k[V]$ with non-zero denominator i.e. $f + f'$ and ff' are both regular at p and hence regular on U. □

For $h \in k[V]$ we have the subset

$$D(h) = \{p \in V \mid h(p) \neq 0\}$$

of V. Such a set is open since it's the complement of the closed set $V(h) \subset V$, and as a consequence of Hilbert's basis theorem, any open set of V can be written as a finite union of sets of this form.

Lemma 3.1. *Let $g, h \in K[V]$ with $h \neq 0$ and let $m \in \mathbb{N}$. The function $\varphi : D(h) \to k$ given by $p \mapsto \frac{g(p)}{h(p)^m}$ is the zero function if and only if $gh = 0$ in $k[V]$.*

Proof. If φ is the zero function then g is zero on $D(h)$, h zero on the complement of $D(h)$ by definition, and so gh is zero on all of V. The other direction is similar: if $gh = 0$ on V then when $h \neq 0$ we must have $g = 0$, and so again by definition, φ is zero on $D(h)$. □

By the above lemma we have that for $h \neq 0$ in $k[V]$, the k-algebra homomorphism $k[V]_h \to \mathcal{O}_V(D(h))$ which maps g/h^m to the function $p \mapsto \frac{g(p)}{h(p)^m}$ is well-defined and injective. It turns out that this map is also an isomorphism, [14, p. 61]. Moreover, in particular, when $D(h) = V$ e.g. $h = 1$, then $\mathcal{O}_V(V) \simeq k[V]$, which is consistent with calling elements of $k[V]$ regular functions.

Corollary 3.1. *For all $p \in V$ we have an isomorphism $\mathcal{O}_{V,p} \to k[V]_{m_p}$ where $\mathfrak{m}_p$ is the maximal ideal of $k[V]$ corresponding to the point $p \in V$ as mentioned in subsection 2.3.*

Proof. [14, Cor. 3.12] The proof of this fact is most straightforward to see with our alternate definition of $\mathcal{O}_{V,p}$ as mentioned in Remark 3.1. As the $D(h)$'s form a basis of V, this is the same as the direct limit over the $D(h)$'s for which $h(p) \neq 0$. Moreover, we also have $k[V]_{m_p} \simeq \varinjlim k[V]_h$ where the direct limit varies over $h \notin m_p$. Combining this with the previous corollary, altogether we get

$$\mathcal{O}_{V,p} = \varinjlim_{h \notin \mathfrak{m}_p} \mathcal{O}_V(D(h)) \simeq \varinjlim_{h \notin \mathfrak{m}_p} k[V]_h \simeq k[V]_{m_p}$$

as required. □

3.2 Affine Algebraic Varieties

Definition 3.5. Let $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ be k-ringed spaces. A **morphism of k-ringed spaces** from $(V, \mathcal{O}_V)$ to $(W, \mathcal{O}_W)$ is a continuous map $\varphi : V \to W$ such that if $f \in \mathcal{O}_W(U')$ then $f \circ \varphi \in \mathcal{O}_V(\varphi^{-1}(U'))$ for all $U' \subset W$ open. Hence for every pair of open subsets $U \subset V$ and $U' \subset W$ with $\varphi(U) \subset U'$ we get a homomorphism of k-algebras $\mathcal{O}_W(U') \to \mathcal{O}_V(U)$, $f \mapsto f \circ \varphi$ with such homomorphisms being compatible with restrictions to smaller open subsets of U'. A morphism is an **isomorphism** if φ has an inverse which is also a morphism of k-ringed spaces.

Remark 3.2. A possibly more succinct definition which appears in [8, §II.2] is that a morphism of k-ringed space is the pair $(\varphi, \varphi^\sharp)$ where $\varphi^\sharp : \mathcal{O}_W \to \varphi_*\mathcal{O}_V$ is a **morphism of sheaves**, where $\varphi_*\mathcal{O}_V$ is the sheaf consisting of sections $\mathcal{O}_V(\varphi^{-1}(U))$ of $\mathcal{O}_V$ for $U \subset W$ open. The latter part of our definition essentially describes what a morphism of sheaves is.

Definition 3.6. An **affine algebraic variety** over k is a k-ringed space isomorphic to a k-ringed space of the form $(V, \mathcal{O}_V)$ where $V \subset \mathbb{A}^n$ is an affine algebraic set and $\mathcal{O}_V$ the sheaf of regular functions on V. For $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ affine algebraic varieties, a map $(V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$ is called a **regular map** (or a **morphism of affine algebraic varieties**) if it is a morphism of k-ringed spaces. Moreover, it's an **isomorphism** if it has an inverse which is also a regular map.

Remark 3.3. Typically we shorten 'affine algebraic varieties' to 'affine varieties'. Moreover, as for a topological space where we denote it by just the underlying set X as opposed to the pairing (X, τ) for τ is a topology on X, we usually just write V for the affine variety.

3.3 Algebraic Varieties

So far, it's not clear where projective sets come into the picture. Here we introduce a class of algebraic structures called **algebraic varieties** where the relationship between them and affine algebraic varieties will be analogous to the relationship between topological manifolds and $\mathbb{R}^n$. In fact, in the language that we have introduced, manifolds can in fact be viewed as $\mathbb{R}$-ringed spaces: a topological manifold can be defined to be a $\mathbb{R}$-ringed space $(V, \mathcal{O}_V)$ for which V is Hausdorff and for each point in V there exists an open neighbourhood U for which $(U, \mathcal{O}_V|_U)$ is isomorphic to the $\mathbb{R}$-ringed space consisting of an open subset of $\mathbb{R}^n$ and the corresponding sheaf of continuous functions. For the standard definition of a manifold which also includes the assumption of V being second countable[19], see [10, §5].

Typically the topological spaces we'll be dealing with won't be Hausdorff: indeed, any non-empty open subsets of an algebraic set are dense, the overlap is also dense[20] and hence non-empty, and so we'll need to introduce an analogous 'separation' condition. We'll define an algebraic variety to be the structure below satisfying such a condition. The content of this section follows section 5 of [14].

Definition 3.7. An **algebraic prevariety** over k is a k-ringed space $(V, \mathcal{O}_V)$ such that V is quasi-compact[21] and for every point p of V there is an open neighbourhood U of p for which $(U, \mathcal{O}_V|_U)$ is isomorphic to a k-ringed space consisting of an affine algebraic set and the associated sheaf of regular functions.

Hence, for V above, as it is quasi-compact, this means that a k-ringed space $(V, \mathcal{O}_V)$ is an algebraic prevariety if it has a finite open cover $V = \bigcup V_i$ where $(V_i, \mathcal{O}_V|_{V_i})$ is an affine algebraic variety for each i. Moreover, observe that our definition doesn't depend on our ringed space being embedded in an ambient space in any particular way, unlike for our definitions of affine or projective algebraic sets.

Definition 3.8. Let $(V, \mathcal{O}_V)$ an algebraic prevariety and U an open subset of V. The elements of $\mathcal{O}_V(U)$ when treated as functions $U \to k$ are called **regular**.

Definition 3.9. Let $(V, \mathcal{O}_V)$, $(W, \mathcal{O}_W)$ be algebraic prevarieties. A map $\varphi : (V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$ is said to be **regular** if it is a morphism of k-ringed spaces.

In other words, a continuous map $\varphi : V \to W$ is a regular map if the induced map on sheaves, $\varphi^\sharp : \mathcal{O}_W \to \varphi_* \mathcal{O}_V$, maps a regular functions $f \in \mathcal{O}_W(U)$ for some $UsubsetW$ open to a regular function $f \circ \varphi \in \mathcal{O}_V(\varphi^{-1}(U))$. Below we give the lemma that motivates what our separation axiom should look like.

Lemma 3.2. *Let $\varphi_1, \varphi_2 : V \to W$ be regular maps of affine algebraic varieties. Then φ_1 and φ_2 agree on a closed subset of V.*

[19] This just means the topological space has a countable basis.

[20] The assumption that the sets are open is necessary here e.g. $\mathbb{Q}$ and $\mathbb{R}\backslash\mathbb{Q}$ are both dense in $\mathbb{R}$ but their intersection is trivial.

[21] In algebraic geometry, a quasi-compact topological space means compact in the usual sense, while the term compact is reserved for the additional property of the space being Hausdorff.

Proof. Let $x_1, \dots, x_n$ be generators for the coordinate ring $k[W]$ $(= \mathcal{O}_W(W))$ of W. As W is an affine algebraic variety, by definition we have a regular map $f : W \to \mathbb{A}^n$, $p \mapsto (x_1(p), \dots, x_n(p))$ which identifies W with a closed subset of $\mathbb{A}^n$ for some n. Moreover, as f is regular, we have that $x_i \circ \varphi_1$ and $x_i \circ \varphi_2$ are regular functions on V for all i and the points of V for which φ_1 and φ_2 agree is given by $\bigcap_{i=1}^n V(x_i \circ \varphi_1 - x_i \circ \varphi_2)$ which is a finite union of closed sets of V and hence closed. □

Definition 3.10. Let V be an algebraic prevariety. We say that V is **separated** if it satisfies the following separation axiom: for every pair of regular maps $\varphi_1, \varphi_2 : X \to V$ where X is an affine algebraic variety, the set $\big\{x \in X \mid \varphi_1(x) = \varphi_2(x)\big\}$ is closed. We then call a separated algebraic prevariety an **algebraic variety**.

With this definition it should be clear that an affine algebraic variety is indeed an algebraic variety: An algebraic prevariety is just a compact k-ringed space which is locally isomorphic to an affine algebraic variety and trivially so are affine algebraic varieties. Lemma 3.2 shows that affine varieties are separated.

Remark 3.4. We also have an equivalent formulation of the above definition as given in [14, § 5(h)]: An algebraic prevariety V is separated if and only if the diagonal

$$\Delta_V = \{(v, v) \mid v \in V\}$$

is closed in $V \times V$. This is motivated by the topological fact that a topological space X is Hausdorff if and only if the diagonal Δ_X is closed in $X \times X$ with respect to the **product topology**. We have avoided such a definition since we have not defined what the product of prevarieties must be. It's not simply the case of it being the product of sets equipped with the product topology. For example, for the set $\mathbb{A}^2$, the Zariski topology on $\mathbb{A}^2$ is not the same as the product topology on $\mathbb{A}^1 \times \mathbb{A}^1$, the latter is Hausdorff while the former is not. For a more detailed exposition, see [14, § 5(g)].

As seen in (11) at the end of section 1, projective space $\mathbb{P}^n$ has a finite open cover of sets that are in bijection with $\mathbb{A}^n$. In the next section, we show that these maps are also homeomorphisms and that we can use this to endow $\mathbb{P}^n$ with a ringed space structure to make it an algebraic variety.

3.4 $\mathbb{P}^n$ is an Algebraic Variety

Before we get on to showing that $\mathbb{P}^n$ has the structure of an algebraic variety, we need to introduce some terminology which will enable us to define what it means to be a **projective variety**, as seen in [14, Section 5(c)]. Moreover, we'll also introduce a way of constructing an algebraic prevariety by patching together prevarieties and checking compatibility on the overlap [14, Section 5(f)].

Definition 3.11. Let $(V, \mathcal{O}_V)$ an algebraic variety over k and let U an open subset of V. Then U is a (finite) union of open affine varieties and hence $(U, \mathcal{O}_V|_U)$ forms an algebraic variety[22] which we call an **open subvariety** of V.

For an algebraic variety $(V, \mathcal{O}_V)$ and $W \subset V$ closed, we can also endow W with a ringed space structure from the structure of V. For this, let $\mathcal{O}_W(U)$ with $U \subset V$ open be the k-algebra consisting of functions f on U such that for every $p \in U$ there is a germ (f', U') of $(V, \mathcal{O}_V)$ for which $f|_{U \cap U'} = f'|_{U \cap U'}$. The fact that this is a ringed space then follows from the locality of our definition of $\mathcal{O}_W$. To then show that it's a variety involves showing that for each open affine variety $U \subset V$, the ringed space $(U \cap Z, \mathcal{O}_{U \cap Z})$ is an affine algebraic variety, more details are given in [14, p. 103].

Definition 3.12. Let $(V, \mathcal{O}_V)$ an algebraic variety and let $W \subset V$ beclosed. Then the algebraic variety $(W, \mathcal{O}_W)$ with $\mathcal{O}_W$ as above is called a **closed subvariety** of V.

Later in this subsection we will show that $\mathbb{P}^n$ is an algebraic variety, a **projective variety** is then defined to be just a closed subvariety of $\mathbb{P}^n$. As promised, we also give the necessary criterion in order to produce a prevariety by 'patching' together subsets which are prevarieties [14, prop 5.15.].

Proposition 3.2. *Let V a set and $V = \bigcup V_i$ a finite union of ringed spaces $(V_i, \mathcal{O}_{V_i})$. Suppose that the following compatibility condition holds:*

If every i and j $V_i \cap V_j$ is open in both V_i and V_j and $\mathcal{O}_{V_i}|_{V_i \cap V_j} = \mathcal{O}_{V_j}|_{V_i \cap V_j}$ then V has the unique ringed space structure $(V, \mathcal{O}_V)$ such that

(a) each inclusion $V_i \hookrightarrow V$ is a homeomorphism onto an open subset of V

(b) $\mathcal{O}_V|_{V_i} = \mathcal{O}_{V_i}$ for every i.

Moreover if each V_i is an algebraic prevariety then so is V and a regular map $\varphi : V \to W$ between prevarieties corresponds to giving a family of regular maps $\varphi_i : V_i \to W$ such that $\varphi_i|_{V_i \cap V_j} = \varphi_j|_{V_i \cap V_j}$ for every i and j.

Proof. Recall that a ringed space is a topological space equipped with a sheaf of k-algebras. So far V is just a set so we also need to equip it with a topology. It turns out that the unique topology on V satisfying the conditions is one where a subset $U \subset V$ is open if and only if $U \cap V_i$ is open in V_i for all i. Indeed, by (a) for $U \cap V_i$ open in V_i for each i, then since the maps are homeomorphisms $U \cap V_i$ is open in an open subset of V and hence open in V for all i and so must $U = \bigcup U \cap V_i$.

Similarly, for $U \subset V$ open, we define $\mathcal{O}_V(U)$ to be the set of functions $f : U \to k$ for which $f|_{U \cap V_i} \in \mathcal{O}_{V_i}(U \cap V_i)$ for every i. Then showing that this is a sheaf directly follows from the fact that $\mathcal{O}_{V_i}$ are all sheaves and so satisfy the locality and gluing axioms

[22] This follows from the fact that any subspace of a separated space is separated.

respectively, and likewise to the uniqueness of the induced topology, (b) ensures that our sheaf is necessarily this one.

For the last paragraph, if each V_i is an algebraic prevariety then quasi-compactness of V follows from the topology on V and quasi-compactness of each of the V_i and each V_i is a union of finitely many affine algebraic varieties means V is also and hence an algebraic prevariety.

Finally, for the correspondence between a regular map $\varphi : V \to W$ and a family of regular maps $\varphi_i : V_i \to W$, the forward direction is clearly the case. For the backwards direction then, continuity of φ follows from the continuity on each φ_i and the topology on V. Regularity holds since if $f \in \mathcal{O}_W(U')$ for $U' \subset W$ open then by regularity of the φ_i's $f \circ \varphi|_{V_i} \in \mathcal{O}_{V_i}(\varphi|_{V_i}^{-1}(U'))$ for all i which implies $f \circ \varphi|_{\varphi^{-1} \cap V_i} \in \mathcal{O}_{V_i}(V_i \cap \varphi^{-1}(U'))$ for all i and so by definition of $\mathcal{O}_V$ $f \circ \varphi \in \mathcal{O}_V(\varphi^{-1}(U'))$ as required. □

Recall, at the end of section 2, I argued that for every $0 \leq i \leq n$ there is a bijection between the open subsets $U_i = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid x_i \neq 0\}$ of $\mathbb{P}^n$ and affine space $\mathbb{A}^n$ giving the correspondence

$$[x_0 : \dots : x_{i-1} : 1 : x_i : \dots x_n] \leftrightarrow (x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n).$$

We want to strengthen this assertion by showing that when each U_i is endowed with the subspace topology from $\mathbb{P}^n$ then these maps are in fact homeomorphisms.

Before we show this, like we have for the affine case where the open sets $D(f) = \mathbb{A}^n \backslash V(f)$ with $f \in k[x_1, \dots, x_n]$ form a basis of $\mathbb{A}^n$, the open sets $D(F)$, $F \in k[x_0, \dots, x_n]$ is homogeneous, form a basis of $\mathbb{P}^n$ in exactly the same way.

Moreover, given $f \in k[x_1, \dots, x_n]$ a polynomial of degree d, we can **homogenize** f to obtain a homogeneous polynomial $f^* \in k[x_0, \dots, x_n]$ of degree d where

$$f^*(x_0, \dots, x_n) = x_0^d f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Similarly, we can **dehomogenize** (not necessarily uniquely) an $F \in k[x_0, \dots, x_n]$ to give us a polynomial $F_* \in k[x_1, \dots, x_n]$ where

$$F_*(x_1, \dots, x_n) = F(1, x_1, \dots, x_n).$$

Proposition 3.3. *For each i, let $u_i : U_i \to \mathbb{A}^n$ be the bijection as in (11). For $U_i \subset \mathbb{P}^n$ equipped with the subspace topology, $\mathbb{A}^n$ equipped with the Zariski topology, then this map is a homeomorphism.*

Proof. [14, prop 6.5.] By symmetry we only need to prove the proposition for $i = 0$. Moreover to show that a function is a homeomorphism, we only need to consider the image and preimage of basic open sets and show that they're open.

As mentioned above, the open subsets $D(F)$ form a basis of $\mathbb{P}^n$, $U_0 = D(x_0)$, and so the open sets $D(F(x_0,\dots,x_n)) \cap D(x_0)$ form a basis of U_0. But these sets correspond precisely to basic open subsets in $\mathbb{A}^n$ of the form $D(F(1,x_1,\dots,x_n)) = D(F_*(x_1,\dots,x_n))$ via the bijection u_0. Similarly, for any polynomial $f \in k[x_1,\dots,x_n]$, $D(f(x_1,\dots,x_n))$ corresponds to the open set $D(f^*(x_0,\dots,x_n)) \cap U_0$ of U_0 via u^{-1} and so we are done. □

In addition to the previous proposition, in order to prove that $\mathbb{P}^n$ is indeed an algebraic variety, we need the following lemma which we state without proof.

Lemma 3.3. *Let $U_{ij} = U_i \cap U_j$, then $\mathcal{O}_i|_{U_{ij}} = \mathcal{O}_j|_{U_{ij}}$, and when U_{ij} is endowed with this sheaf it is an affine algebraic variety. Moreover the k-algebra $\mathcal{O}_i(U_{ij})$ is generated by the functions $(f|_{U_{ij}})(g|_{U_{ij}})$ where $f \in \mathcal{O}_i(U_i)$, $g \in \mathcal{O}_j(U_j)$.*

Proof. See [14, p. 135]. □

Proposition 3.4. *$\mathbb{P}^n$ has a unique structure of an algebraic prevariety where each U_i is an open affine subvariety of $\mathbb{P}^n$ and each map u_i is an isomorphism of algebraic prevarieties. Moreover, $\mathbb{P}^n$ is separated and hence an algebraic variety.*

Proof. For each i, as we have a homeomorphism $u_i : U_i \to \mathbb{A}^n$ by Prop. 3.3, we can endow U_i with a sheaf $\mathcal{O}_i$ inherited from the sheaf of regular functions on $\mathcal{O}_{\mathbb{A}^n}$ where for $U \subset U_i$ open, $f \in \mathcal{O}_i(U)$ if and only if $f \circ u_i^{-1} \in \mathcal{O}_{\mathbb{A}^n}(u_i(U))$.

Moreover, by definition, this shows that u_i is an isomorphism of k-ringed spaces and hence U_i is an affine algebraic variety. Also, for the affine cover $\mathbb{P}^n = \cup U_i$, Lemma 3.3 shows that the set $\mathbb{P}^n$ satisfies the compatibility condition in Prop. 3.2 and hence is an algebraic prevariety with the unique ringed space structure $(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n})$ as given in the proposition.

To show $\mathbb{P}^n$ is separated, we also appeal to Lemma 3.3 to show that $\mathbb{P}^n$ satisfies condition (c) of Theorem 5.29 in [14].

□

3.5 Divisors

In this section we introduce the notion of a **prime divisor** on an **irreducible non-singular algebraic variety**. With such objects we will define the **Picard group** which will be the free groups of prime divisors modulo a particular equivalence. To begin, let us introduce some preliminary commutative algebra definitions.

Definition 3.13. Let R a Noetherian ring. The **height** $\operatorname{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ in R is the greatest length d of a chain of distinct prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_d = \mathfrak{p}.$$

The **Krull dimension** of R is then defined as the greatest length of such chains in R i.e.

$$\dim R = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \subset R \text{ a prime ideal}\}.$$

Definition 3.14. Let R be a ring. R is called a **local ring** if it has a unique maximal ideal $\mathfrak{m}$, and typically we denote such a ring by $(R, \mathfrak{m})$. Moreover, suppose that $(R, \mathfrak{m})$ is Noetherian, then we say that R is **regular** if the minimal number of generators of $\mathfrak{m}$ is equal to the Krull dimension $\dim R$ of R.

Recall that in Cor. 3.1 we showed that for an affine algebraic set V, $\mathcal{O}_{V,p}$ is isomorphic to the local ring $k[V]_{m_p}$ and hence also a local ring. The result is also true in general: for an algebraic variety V, the unique maximal ideal of $\mathcal{O}_{V,p}$ corresponds to the germs of regular functions which vanish at p. This gives rise to the following definition.

Definition 3.15. Let V be an irreducible algebraic variety. For a point $p \in V$ we say that V is **non-singular** at p if the stalk of p at V, $\mathcal{O}_{p,V}$, is regular. Moreover, we say that V is non-singular if V is non-singular at all points p of V.

Proposition 3.5. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension one. Then R is a principal ideal domain.*

In order to prove this proposition we will need to use the **Krull intersection theorem** from commutative algebra which asserts that for a Noetherian local ring $(R, \mathfrak{m})$, then $\cap_{n \geq 1} \mathfrak{m}^n = (0)$ [14, Theorem 1.8.].

Proof. [14, Prop 4.20] A principal ideal domain is an integral domain where every ideal is principal. We first show that every ideal of R is principal. By assumption, $\mathfrak{m}$ is a principal ideal and so let $\mathfrak{m} = (\pi)$. Moreover, let $\mathfrak{a}$ be a proper non-zero ideal. As R is Noetherian, $\mathfrak{a}$ is finitely generated, and so there exists a positive integer r for which $\mathfrak{a} \subset \mathfrak{m}^r$ but $\mathfrak{a} \not\subset \mathfrak{m}^{r+1}$[23]. Therefore, there is an element $a = c\pi^r \in \mathfrak{a}$ but $c \notin \mathfrak{m}^{r+1}$, and we must have $c \notin \mathfrak{m}$ and so c is a unit, giving us that $(\pi^r) = (a) \subset \mathfrak{a} \subset (\pi^r)$, hence $\mathfrak{a} = (\pi^r)$ as required.

To show that R is an integral domain, by assumption R has Krull dimension 1, and so we know there exists a prime ideal $\mathfrak{p}$ properly contained in $\mathfrak{m}$. This implies that $\pi \notin \mathfrak{p}$ and since $\mathfrak{p}$ is prime, $R/\mathfrak{p}$ is an integral domain, and so (the image of) π is not nilpotent in $R/\mathfrak{p}$ and hence also not nilpotent in R. As we saw in the previous paragraph, we can write elements non-zero elements of R in the form $u\pi^r$ where u is a unit and $r \in \mathbb{N}$ and so when we multiply two non-zero elements of R we get an element of this form and since π is not nilpotent the product is non-zero. □

Definition 3.16. Let K be a field. A **discrete valuation** on K is a function $\nu : K^\times \to \mathbb{Z}$ such that for all $x, y \in K^\times$,

(a) $\nu(xy) = \nu(x) + \nu(x)$;

(b) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

[23] This assertions follows from the fact that for any ring, every proper ideal is contained in some maximal ideal.

A **discrete valuation ring** is defined to be a local principal ideal domain which is also not a field i.e. it's a P.I.D whose unique maximal ideal is not the zero ideal. With such a ring R we can define a valuation on its field of fractions $\mathrm{Frac}(R)$: as we saw in the proof of the proposition above, any non-zero element of $(R, \mathfrak{m})$ can be written in the form $u\pi^r$ where u is a unit, π is a generator of $\mathfrak{m}$ which we call a **uniformiser** and $r \in \mathbb{N}$ and so every element of $\mathrm{Frac}(R)$ can be written as $v\pi^s$ with v a unit of R and $s \in \mathbb{Z}$. This gives rise to a discrete valuation $\nu : \mathrm{Frac}(R)^\times \to \mathbb{Z}$ where $\nu(v\pi^s) = s$ which one can easily check is well-defined[24].

Definition 3.17. Let V be a non-singular irreducible algebraic variety. A **prime divisor** Z on V is a closed irreducible subvariety of codimension 1. A **divisor** D is an element of $\mathrm{Div}X$, the free (abelian) group on the prime divisors i.e. $D = \sum n_i Z_i$ where the Z_i's are prime divisors, the n_i's are integers such that all but finitely many of them are zero. Moreover, if $n_i \geq 0$ for all i then we say that D is **effective**.

A **generic point** of a topological space is a point whose closure is the whole space. It's a fact that every irreducible closed subset Z of an irreducible variety V has a unique generic point $\eta \in Z$ [8, §2 Ex. 2.9]. Moreover, we have another fact that $\mathrm{codim}(Z, V) = \dim(\mathcal{O}_{\eta,V})$ where the right hand side is the Krull dimension, [19, Ex 11.1.I]. Hence for a prime divisor Z, $\mathrm{codim}(Z, V)$ equals to 1 and so by Prop. 3.5, $\mathcal{O}_{\eta,V}$ is a discrete valuation ring and hence we get a discrete valuation ν_Z on $k(V) = \mathrm{Frac}(\mathcal{O}_{\eta,V})$.

For $f \in k(V)^\times$, if $\nu_Z(f) > 0$ we say that f has a **zero of order** $\nu_Z(f)$ along Z and if $\nu_Z(f) < 0$ we say that f has a **pole of order** $-\nu_Z(f)$ along Z. As elements of $\mathrm{Frac}(\mathcal{O}_{\eta,V})$ take the form $v\pi^s$ where π is the uniformiser of the (unique) maximal ideal of $\mathcal{O}_{\eta,V}$ which consists of the germs of regular functions of $\mathcal{O}_V$ which vanish at η and v is a unit i.e. the corresponding function doesn't vanish at η. We see then that the terms are similar to those used for **complex functions** in complex analysis.

Proposition 3.6. *Let V be a non-singular irreducible variety and let $f \in k(V)^\times$. Then $\nu_Z(f) = 0$ for all but finitely many prime divisors $Z \subset V$.*

Proof. We shall prove the case when V is a non-singular irreducible affine variety. As $f \in k(V)^\times$ we can write $f = g/h$ where g, h are non-zero polynomials in $k[V]$. Moreover, for each prime divisor Z, the ν_Z's are group homomorphisms, Def. 3.16(a), hence $\nu_Z(f) = \nu_Z(g) - \nu_Z(h)$, and so without loss of generality we only need to prove the proposition for g. If $V(g)$ is empty then we are done, g doesn't vanish anywhere, so in particular doesn't vanish on any prime divisors giving us $\nu_Z(f) = 0$ for all divisors. If $V(g)$ is non-empty then by Theorem 3.42 of [14], $V(g)$ has pure codimension[25]1, and since we know that every affine variety can be written as a finite union of irreducible affine varieties these must also have codimension 1 i.e. they're prime divisors and so we are done. □

[24] One can easily verify that if an element $u\pi^r$ of $\mathrm{Frac}(R)^\times$ is written instead as $w\tau^t$ then $t = s$ and so we get the same valuation.

[25] This just means that every irreducible component has codimension 1.

Definition 3.18. Let V be an irreducible non-singular variety and let $f \in k(V)$. The divisor of f is defined as

$$\operatorname{div}(f) = \sum_{Z} \nu_Z(f) Z$$

where the sum taken over the prime divisors of V. From the previous proposition $\operatorname{div}(f)$ is indeed a divisor, and we call a divisor of such a form a **principal divisor**. Moreover two divisors are said to be **linearly equivalent** if they differ by a principal divisor, that is $D_1 \sim D_2$ if and only if $D_1 - D_2 = \operatorname{div}(f)$ for some $f \in k(V)$.

It turns out that the principal divisors form a subgroup $\operatorname{Prin} V$ of $\operatorname{Div} V$: as the ν_Z's are group homomorphisms(Def. 3.16(a)), as seen in the proof of the previous proposition, $\operatorname{div}(f) - \operatorname{div}(g) = \operatorname{div}(f/g)$ i.e. $\operatorname{Prin} V$ is closed under addition and inverses. The **Picard group** is then defined to be the quotient group

$$\operatorname{Pic} V = \frac{\operatorname{Div} V}{\operatorname{Prin} V}.$$

Remark 3.5. The group that we have defined here is usually called the **divisor class group**, denoted by Cl V. Meanwhile, as in [8], for example, the Picard group is defined for much more general geometric objects. For this what are called **Cartier divisors** are considered instead of **Weil divisors** which we have defined. However, for non-singular varieties, these two notions of divisors agree and so the corresponding groups are isomorphic [8, Prop. 6.11], hence what we have said is at least consistent.

In general, the Picard group is notoriously difficult to compute, even for the simplest cases we can think of, such as for affine n-space $\mathbb{A}^n$.

Proposition 3.7. *Pic* $\mathbb{A}^n = 0 \ \forall n \in \mathbb{N}$.

Spelling it out, to show that the Picard group of $\mathbb{A}^n$ is indeed equal to 0 requires showing that every divisor is an element of $\operatorname{Prin} \mathbb{A}^n$ i.e. it is a principal divisor, or equivalently that every prime divisor is a principal divisor. Again, this then becomes the question of showing that every prime divisor is defined by the zero loci of a single polynomial in $k[x_1, \ldots, x_n]$. Spelling it out again, a prime divisor is just an irreducible subvariety of $\mathbb{A}^n$ of codimension 1, which from our correspondence between irreducible varieties and prime ideals of $k[x_1, \ldots, x_n]$ as in (10) and our definition of the Krull dimension as in Def. 3.13, corresponds to a prime ideal of height 1. The proposition then follows from the more general fact in commutative algebra that in a unique factorisation domain (UFD), every prime ideal of height one is principal, as seen in [12].

3.6 The Picard Group of Cubic Surfaces

In this subsection we look at the Picard group for non-singular projective cubic surfaces (over algebraically closed fields). In affine 3-space, a line may be defined as (the image of) a parametrisation $\underline{r}(t) = \underline{a} + t\underline{b} = (a_1 + tb_1, a_2 + tb_2, a_b + tb_3)$ or equivalently as the intersection of two (non-parallel, non-disjoint) hyperplanes i.e. as a subvariety $V(a_1x + b_1y + c_1z + d_1, a_1x + b_1y + c_1z + d_2) \subset \mathbb{A}^3$ with not all coefficients equal to 0. We can similarly define **lines** in $\mathbb{P}^3$ by either of the two corresponding definitions, but this time we have a parametrisation given in projective coordinates and hyperplanes defined by homogeneous linear polynomials.

A celebrated theorem is that non-singular projective cubic surfaces contain exactly 27 lines [8, § II.V, Theorem 4.9]. One can use this fact to prove the following theorem.

Theorem 3.1. *Let V be a non-singular projective cubic surface. Then $Pic\, V = \mathbb{Z}^7$.*

In order to prove such a theorem, one considers a simpler subgroup $A(V)$ of Pic$V$ which turns out to be isomorphic[26] to Pic$V$. Such a subgroup is one which is generated by the 27 lines on our surface modulo the relations $L1 + L2 + L3 - L1' - L2' - L3'$ where $L1, L2, L3$ and $L1', L2', L3'$ are (possibly degenerate[27]) triangles in the usual sense i.e. 3 lines which intersect pairwise. One then uses various facts regarding the arrangement of the lines on the cubic surface such as

- Each line intersects exactly 10 of the 27 other lines;
- Each line forms part of exactly 5 triangles,

to prove that $A(V) \cong \mathbb{Z}^7$. Instead of arguing in such a combinatorial fashion, we prove the theorem in the case when V is the (projective) Fermat cubic surface,

$$V = V(x^3 + y^3 + z^3 + w^3). \tag{12}$$

By the symmetries of the defining equation of V, we can quite easily compute the lines explicitly, with which we can determine the triangles on our surface and hence the group $A(V)$. Below we compute such lines and also present an algorithm written in **SageMath** that is able to compute $A(V)$.

Proposition 3.8. *There are 27 lines on the Fermat cubic surface.*

Proof. For this proof we will the definition of a line in $\mathbb{P}^3$ as the intersection of two hyperplanes. That is, a line is a projective variety of the form $V(a_1x + b_1y + c_1z + d_1w, a_2x + b_2y + c_2z + d_2w)$ with not all coefficients in each equation equal to 0. Moreover, our line must lie on the Fermat surface, that is $x^3 + y^3 + z^3 + w^3 = 0$, therefore each coordinate on our line is determined by the other 3. Moreover, as we know from linear algebra, any linear (non-zero) combination of two linear equations preserves the set of solutions, which amounts to a change of coordinates, and so combining these two facts together, without

[26] The fact that these two subgroups are isomorphic is non-trivial; a more detailed exposition is given in [16, § 1].

[27] We allow for the case where three lines intersect at a point to be a triangle. In fact, such triangles are called **Eckhard points**

loss of generality, we can write a line in V in the form $V(z - a_1x - b_1y, w - a_2x - b_2y)$. Hence we get that a line lies in V if and only if

$$x^3 + y^3 + (a_2x + b_2y)^3 + (a_1x + b_1y)^3 = 0.$$

This is just a polynomial equation in $\mathbb{C}[x, y]$, and so expanding the left hand side and equating coefficients we get

$$\begin{aligned} 1 + a_1^3 + a_2^3 &= 0; && (x^3) \\ a_2^2b_2 + a_1^2b_1 &= 0; && (x^2y) \\ a_2b_2^2 + a_1b_1^2 &= 0; && (xy^2) \\ 1 + b_1^3 + b_2^3 &= 0. && (y^3) \end{aligned}$$

We want to show that at least one of these coefficients in 0, then the values of the other coordinates unravel nicely. Suppose not, then rearranging (x^2y), (xy^2) and multiplying them together we get $a_2^3b_2^3 = a_1^3b_1^3$ $(*)$, which we can rearrange to get $a_1^3 = \frac{a_2^3b_2^3}{b_1^3}$. Plugging this into (x^3) we get

$$\begin{aligned} 1 + a_2^3\left(\frac{b_2^3}{b_1^3} + 1\right) = 0 &\implies 1 + \frac{b_2^3}{b_1^3} = \frac{-1}{a_2^3} \\ &\implies b_1^3 + b_2^3 = \frac{-b_1^3}{a_2^3} \\ &\overset{(y^3)}{\implies} b_1^3 = a_2^3 \\ &\overset{(*)}{\implies} a_1^3 = b_2^3. \end{aligned}$$

This gives us $b_1 = \zeta^k a_2$ and $b_2 = \zeta^k a_1$ for some $0 \leq k, l \leq 2$ where $\zeta = \exp(2\pi i/3)$. Substituting both these equations into (x^2y) and factorising gives us $a_1a_2(\zeta^j a_2 + \zeta^i a_1) = 0$, and since by assumption the coefficients are non-zero we get $a_2 = -\zeta^{i-j}a_1$. From this we get that $a_1^3 + a_2^3 = 0$, contradicting (x^3).

Hence, without loss of generality, we can take $a_1 = 0$. By this assumption, from (x^3) we get $a_2^3 = -1$; $(*)$ still holds which gives $b_2 = 0$, and then from (y^3) we get $b_1^3 = -1$. As a result that $b_1 = -\zeta^i$ and $a_2 = -\zeta^j$ for some $0 \leq i, j \leq 2$. this gives us the 9 lines of the form

$$V(z + \zeta^i y, w + \zeta^j x) \qquad \text{for } 0 \leq i, j \leq 2.$$

Moreover, by symmetry of the defining equation of the Fermat surface we get 2 other families of 9 lines corresponding to permutations on the coordinates,

$$\begin{aligned} &V(x + \zeta^i y, w + \zeta^j z) && \text{for } 0 \leq i, j \leq 2. \\ &V(w + \zeta^i y, x + \zeta^j z) && \text{for } 0 \leq i, j \leq 2. \end{aligned}$$

One can then easily verify that all these lines are distinct e.g. by giving parametrisations in projective coordinates. One can also easily verify that we have no more families of lines e.g. if we consider the permutation that results in the family of lines $V(y+\zeta^i z, x+\zeta^j w)$, then these lines simply correspond to the first family of lines $V(z+\zeta^i y, w+\zeta^j x)$, which we see by multiplying the first equation by ζ^{3-i} and the second by ζ^{3-j}. □

We now present the code that enables us to compute $A(V)$ for the Fermat Surface.

```
from itertools import combinations
from itertools import chain
from collections import Counter

#Determine whether two tuples/lists are permutations of each other
def is_perm(items0, items1):
    return len(items0) == len(items1) and Counter(items0) == Counter(items1)

exp(2*\pi*i/3)
k = CyclotomicField(3) #Field Q[exp(2*\pi*i/3)]; using CC doesn't
                       #determine all intersections of lines below

a = k.gen() #Corresponds to exp(2*\pi*i/3)
P.<x,y,z,w> = ProjectiveSpace(3,k)

G = FreeGroup(27) #Free group generated by 27 lines

#Three family of 9 lines on Fermat surface from previous proposition
l_1 = [(x + y*a^i, w + z*a^j) for i in [0,1,2] for j in [0,1,2]]
l_2 = [(z + x*a^i, w + y*a^j) for i in [0,1,2] for j in [0,1,2]]
l_3 = [(z + y*a^i, w + x*a^j) for i in [0,1,2] for j in [0,1,2]]
lines = l_1 + l_2 + l_3
lines_x = list(G.generators()) #Symbolic representation of lines
                               #([x0, ..., x26]) - groups relations are
                               #given in terms of these symbols

#Flattened pairs of lines - necessary for computing P.subscheme below
itr = combinations(lines, 2)
list1 = []
for i in itr:
    flattened = [item for sublist in i for item in sublist]
    list1 += [flattened]

list_x = [x for x in combinations(lines_x, 2)] #Symbolic pairs of lines


#Determine whether two lines intersect or not
l = []
a_x = []
for i in range(len(list1)):
    X = P.subscheme(list1[i]) #P is our projective 3-space over k, computes
                              #a subvariety defined by equations in list
                              #of lines
    if X.dimension() == 0: #If two lines intersect it is at a point, which
                           #has dimension 0
        l += [[list1[i]]] #List of pairs of (actual) lines which intersect
        a_x += [list_x[i]] #List of pairs of (symbolic) lines which
                           #intersect

s_x = [(a_x[i][1], a_x[i][0]) for i in range(len(a_x))]
l_x = sorted(a_x + s_x) #List of pairs of (symbolic) lines which intersect
                        #and their transpositions e.g. both (x0, x1) and
                        #(x1, x0) are in this list - necessary for finding
                        # the triangles below

#List of triangles - we look for intersecting pairs of lines which form a
#triangle i.e we have the pairs (x_i, x_j), (x_j, x_k), (x_k, x_i) form
#the triangle (x_i, x_j, x_k)

tris = []
for i in range(len(l_x)):
    l1 = l_x[i]
    for j in range(i+1, len(l_x)):
        l2 = l_x[j]
        if l2[0] != l1[1]:
            continue
        for k in range(j+1, len(l_x)):
            l3 = l_x[k]  #l1, l2, l3 are in ascending order
            if l2[1] != l3[0]:
                continue
            if l3[1] == l1[0]:
                tri = tuple(set(l1+l2+l3)) #triangle (x_i, x_j, x_k)
                tris += [tri]
                break
print(‘The number of triangles we have computed is:’, len(tris))

#Relations on our free group G of 27 lines -  the first ensures the group
#is abelian and the second corresponds to the relation l1 + l2 + l3
# -l1’ -l2’ -l3’

abelian = [lines_x[i]*lines_x[j]*lines_x[i]^(-1)*lines_x[j]^(-1) for i in \
            range(len(lines_x)) for j in range(len(lines_x))]

tri_const = [tris[i][0]*tris[i][1]*tris[i][2]*tris[j][0]^(-1) \
             *tris[j][1]^(-1)*tris[j][2]^(-1) for i in range(len(tris)) \
             for j in range(len(tris))]
relations = abelian + tri_const

H = (G/ relations).simplified()
```

```

print('Our group is the', H)
```

The code then outputs the following:

```
- The number of triangles we have computed is: 45.
- Our group is the Finitely presented group < x2, x3, x8, x9, x17, x21, x24 | >.
```

Indeed, this gives us a group that is isomorphic to $\mathbb{Z}^7$, with the number of triangles in agreement with that in [2, p. 16]. Recall that in subsection 1.5, we gave a prediction for the asymptotic behaviour of the integral points on a smooth cubic surface of a bounded height, and that this formula involved the term ρ_U corresponding to the rank of the Picard group of the 'variety' $U = V(f) \subset \mathbb{A}^3_{\mathbb{Q}}$. Of course, we have only defined algebraic varieties over algebraically closed fields, for which $\mathbb{Q}$ is not. However, as is done in [8], one can define can define algebraic varieties over non-algebraically closed fields in the language of **schemes** [8, Section II.V].

Moreover, the Picard group for such varieties can be defined in the same way as we have done, as seen in [4]. Also, it turns out that for a variety defined over $\mathbb{Q}$, $V_{\mathbb{Q}}$, and the corresponding variety defined over $\mathbb{C}$, $V_{\mathbb{C}}$, then $\operatorname{Pic} V_Q$ is a subgroup of $\operatorname{Pic} V_{\mathbb{C}}$.

However, it's may not necessarily be true that these two groups are equal. For example, for the (projective) Fermat cubic, the lines $L_1 = V(x+\zeta y, w+z)$ and $L_2 = V(x+\zeta^2 y, w+z)$ in $V_{\mathbb{C}}$ are not lines in $V_{\mathbb{Q}}$ (and hence are not prime divisors), meanwhile their sum $L_1+L_2 = V(x^2+xy+y^2, z+w)$ is.

4 Finding Parametrisations

In order to test the heuristic as given in (6) for different examples of cubic surfaces, we want to find a way to remove parametric solutions from them. For the Fermat cubic, an infinite family of parametric equations are given by a recurrence relations as in (5). However, this is not always the case, for example for the cubic surface corresponding to the equation $x^3 + y^3 + z^3 = 2$, the only known parametric equation is $r(t) = (1 + 6t^3, 1 - 6t^3, -6t^2)$.

In this section then, I present an algorithm written in Sage that attempts to find some of the parametric equations on the Fermat cubic from scratch. This will be done by purely looking at a large data set of solutions, as provided by Andrew Sutherland [18], and trying to work out connections between the solutions. As the methods used will be mainly primitive i.e. they will not rely on any sophisticated tools from algebraic geometry, the ideas presented should generalise to other cubic surfaces.

4.1 Initial Analysis

To begin there are some immediate observations one can make about integral solutions of the equation $x^3 + y^3 + z^3 = 1$. One is that the equation is symmetric in x, y and z and so without loss of generality we'll only consider the specific permutation with $|x| \geq |y| \geq |z|$.

Moreover, if none of the values are 0 (otherwise we just get the solution $(1, 0, 0)$), from the equation we deduce that either one of the values is positive, the other two negative, or the other way round, and so our points are of the form $(+, -, -)$ or $(-, +, +)$ with the symbols representing the signs of the coordinates. Also one can immediately see that there are infinitely many integral solutions on the surface; $(t, -t, 1)$ for $t \in \mathbb{Z}$ are a trivial such family of solutions; these correspond to some of the lines seen in Prop. 3.8.

As for parametrisations on $x^3 + y^3 + z^3 = 1$, suppose that we have one on our surface: $r(t) = (x(t), y(t), z(t))$ with $x(t)$, $y(t)$ and $z(t) \in \mathbb{Z}[t]$. Moreover suppose, without loss of generality, that $\deg x(t) \geq \deg y(t) \geq \deg z(t)$ with $\deg x(t) = d > 1$. By the defining equation we have $x(t)^3 + y(t)^3 + z(t)^3 = 1$, expanding out the LHS and considering the coefficient of t^{3d}, which is 0 by the RHS, gives us the equation in coefficients of $x(t), y(t)$ and $z(t)$ respectively:

$$a_d{}^3 + b_d{}^3 + c_d{}^3 = 0. \tag{13}$$

From Fermat's last theorem[28] for the case where $n = 3$ we can deduce that the only possible solutions are when $b_d = -a_d$, $c_d = 0$ i.e. parametrisations on our surface are of the form

$$(x(t), y(t), z(t)) = (a_d t^d + \ldots + a_0, -a_d t^d + \ldots + b_0, c_e t^e + \ldots + c_0) \tag{14}$$

with $e < d$.

Now the question is, assuming they exist, how do we find parametrisations on our surface? One way to do this is instead of looking at points in isolation, we look at pairs of points and try to deduce if it's likely that both pairs of points lie on a parametrisation.

First let us assume that we have two points (x_0, y_0, z_0), (x_1, y_1, z_1) on our surface and that they both lie on the same general parametric curve given in (14) in a consecutive order i.e. $(x_0, y_0, z_0) = (x(t_0), y(t_0), z(t_0))$, $(x_1, y_1, z_1) = (x(t_0 + 1), y(t_0 + 1), z(t_0 + 1))$. Then for $x_1 \neq 0$, sufficiently large $|t_0|$ we have the crude approximation,

$$\begin{aligned}\left|\frac{x_1}{x_0}\right| &= \left|\frac{a_d(t_0+1)^d + a_{n-1}(t_0+1)^{d-1} + \ldots a_0}{a_d t_d^d + a_{d-1}t^{d-1} + \ldots a_0}\right| \\ &\approx \left|\frac{a_d(t_0+1)^d}{a_d t_0^d}\right| \\ &= \left|1 + \frac{1}{t_0}\right|^d.\end{aligned}$$

In practice all we have to work with is our data set of points i.e. we only know what

[28] Fermat's last theorem states that there are no positive integer solutions to the equation $x^n + y^n = z^n$ for any $n \geq 3$. Similar to the previous deduction about the signs of the points; if none of the coefficients are zero we have two of the points with the same sign, one with the opposite sign, so we can rearrange (9) into an equation for which we can apply FLT to and deduce there are no possible solutions except when one of the coefficients is 0.

the value $r = \left|\frac{x_1}{x_0}\right|$ is. We can easily obtain a candidate value for t_0 by rearranging the approximation above to give

$$t_x = \frac{1}{r^{\frac{1}{d}} - 1} \approx t_0. \tag{15}$$

If we also consider the same for the y and z coordinates we get similiar approximations for t_0:

$$t_y = \frac{1}{s^{\frac{1}{d}} - 1} \approx t_0, \qquad t_z = \frac{1}{q^{\frac{1}{e}} - 1} \approx t_0 \tag{16}$$

where here $s = \left|\frac{y_1}{y_0}\right|$, $q = \left|\frac{z_1}{z_0}\right|$ and e the degree of the polynomial $z(t)$ as in (14).

Given any two pairs of points from our data set we can compute the left hand sides of 15 and 16. If these values are similar it then gives us some reason to believe that these two points are consecutive points on some parametric curve of the form in (14). This then begs the questions: What values of d and e should we consider? How might we use this information to actually compute parametrisations? For the former question I approach it with the use of **continued fractions** and the latter is tackled with **Lagrange Interpolation polynomials**.

4.2 Continued Fractions

In much the same way as every real number admits an (essentially unique) [29] decimal expansion and the decimal expansion up to a certain number of decimal places gives us an approximation for the real number, so we can have an (essentially unique) expression for any real number in a different way, which in some ways is even more natural and provides us with better approximations.

Take for example the fraction $r = \frac{337}{153}$. If we consider the integral part of this fraction, $\lfloor r \rfloor = 2$ we a very basic approximation for r with remainder $r_0 := r - \lfloor r \rfloor \in (0, 1)$. We can then rewrite r as $r = 2 + r_0 = 2 + \frac{1}{\frac{1}{r_0}}$. To justify writing r in this form, since $0 < r_0 < 1$ we can consider its reciprocal $\frac{1}{r_0} > 1$ and so approximate this by its floor function for which we get $\lfloor \frac{1}{r_0} \rfloor = \lfloor \frac{153}{31} \rfloor = 4$ giving us $r_1 = \frac{1}{r_0} - \lfloor \frac{1}{r_0} \rfloor$ and $r = 2 + \frac{1}{4+r_1}$. We can keep going like this: considering the reciprocal of r_1 and then approximating as we did for $\frac{1}{r_0}$ to obtain the next term to be

$$r = 2 + \frac{1}{4 + \frac{1}{1+r_2}}.$$

The process eventually terminates when we get a remainder r_k equal to 0, in this case this happens when $k = 4$, giving us what we call the **continued fraction** for $\frac{337}{153}$:

$$r = 2 + \frac{1}{4 + \frac{1}{1+\frac{1}{14+\frac{1}{2}}}}. \tag{17}$$

[29] e.g. $2 = 1.99999...$

The integers $2, 4, 1, 14, 2$ in the fraction, which are called **coefficients**, give us the compact expression of $[2; , 4, 1, 14, 2]$ for our continued fraction. Moreover truncating (17) gives what we call the **convergents** of the continued fraction, $\left[2, \frac{9}{4}, \frac{11}{5}, \frac{163}{74}, \frac{337}{153}\right]$.

In the example given, the real number we considered was rational and we obtained a finite expression for our continued fraction. It turns out in general that a real number having a finite continued fraction is equivalent to the number being rational. To see the non-trivial direction, for a rational number $n = \frac{p}{q}$ in lowest terms with either both positive or only p negative, by Euclid's lemma we have $p = a_1 q + r_1$ where $0 \leq r_1 < q$, $a_1 \in \mathbb{Z}$. So $n = a_1 + \frac{r_1}{q} = a_1 + \frac{1}{\frac{q}{r_1}}$. Similarly, we have $q = a_2 r_1 + r_2$, $0 < r_2 < r_1$, a_2 non-negative giving us $\frac{q}{r_1} = a_2 + \frac{r_2}{r_1}$ and now we have $n = a_1 + \frac{1}{a_2 + \frac{r_2}{r_1}}$. If we continue this process (this is essentially just Euclid's algorithm in disguise), we see that this is just the construction of the continued fraction of n and it will eventually terminate as the remainders are strictly decreasing.

One may now ask how we might use such a tool to obtain the degrees for the polynomials of any potential parametrisations. For this lets first consider we have a single point on a generic parametrisation as in 14 and suppose that we also know the leading coefficients, a_d and c_e. Then a simple approximation for large t follows from looking at a ratio of the x term and the z term:

$$\begin{aligned}\frac{\log(|\frac{x(t)}{a_d}|)}{\log(|\frac{z(t)}{c_e}|)} &\approx \frac{\log(|t^d|)}{\log(|t^e|)} \\ &= \frac{d}{e}.\end{aligned}$$

This is where continued fractions comes in. For any point in our data set we can compute the value on the left hand side of the approximation above. On a computer such a value will be a float type i.e. a number with finitely many decimal places, for which we can compute its finite continued fraction. We can then look at the convergents of the continued fraction and see if any of them provide particularly strong approximations. The fractions we will care about most will have small numerator and denominator; if they're too large then we won't have enough points on the corresponding parametrisation to do anything useful with.

To demonstrate such a method, we look at 5 points chosen at random from our data set. For such a task I will also be using SageMath, for its' built in features regarding continued fractions as well as Lagrange polynomials later on. The corresponding code is below.

```
## Continued fractions and convergents for 5 randomly chosen points ##
import random
import pickle

```

```python
# Data set for min(|x|, |y|, |z|) <= 10^15
with open('solutions','rb') as fp:
    sols = pickle.load(fp)

# Continued fraction for 5 random points of our data set
for i in random.choices(sols, k = 5):
    x = i[0]; z = i[2]
    r = RR(log(abs(x/9))/log(abs(z/9)))
    cont_frac = QQ(r).continued_fraction()
    convs = cont_frac.convergents()
    print('(x, y, z) =', i)
    print('continued fraction:', cont_frac)
    print('convergents:',convs)
    print()
```

The code then produces the following output:

```
(x, y, z) = [1082067890430355929, -1082067890430300066, -58110084873548]
continued fraction: [1; 2, 1, 120095990063213]
convergents: [1, 3/2, 4/3, 480383960252855/360287970189641]

(x, y, z) = [-16819982441035350, 16819982441015625, 2558172234376]
continued fraction: [1; 2, 1, 4501348952894]
convergents: [1, 3/2, 4/3, 18005395811579/13504046858684]

(x, y, z) = [-2225676096900066900, 2225676096900000000, 99806103000001]
continued fraction: [1; 2, 1, 158021039556859]
convergents: [1, 3/2, 4/3, 632084158227439/474063118670579]

(x, y, z) = [5382499495979802249, -5382499495979718822, -193552428925160]
continued fraction: [1; 2, 1, 428914250225761]
convergents: [1, 3/2, 4/3, 1715657000903047/1286742750677285]

(x, y, z) = [-1674016522074020079O, 1674016522074009000O, 453294482013001]
continued fraction: [1; 3]
convergents: [1, 4/3]
```

Such data is clearly signalling that there's a parametrisation of degree $4k$ and $3k$ (fraction is in its simplest form) for k some positive integer, which of course is consistent with the initial quartic parametrisation in (3). Forgetting for a moment that we actually know about such parametrisations, let us to try to find such a parametrisations of this form, and as mentioned previously, to do this we will use Lagrange Polynomials.

4.3 Lagrange Polynomials

Simply put, given $n+1$ points $\{(x_i, y_i)\}_{i=0}^{n}$ in $\mathbb{R}^2$ with the x_i's distinct, then there exists a unique polynomial of degree at most n that runs through all these points. Such a polynomial we call the Lagrange polynomial associated to these points. To see that such a polynomial exists, the problem can be formulated in terms of linear algebra. Supposing that the $n+1$ points lie on a degree at most n polynomial i.e. $p(x_i) = y_i$ for all $1 \leq i \leq n$, this can be written as

$$\begin{aligned}
a_0 + a_1x_0 + \dots a_n{x_0}^n &= y_0\\
a_0 + a_1x_1 + \dots a_n{x_1}^n &= y_1\\
&\vdots\\
a_0 + a_1x_n + \dots a_n{x_n}^n &= y_n
\end{aligned}$$

or equivalently in matrix form $A\underline{v} = \underline{y}$ with

$$A = \begin{pmatrix} 1 & x_0 & \dots & {x_0}^n \\ 1 & x_1 & \dots & {x_1}^n \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & \dots & {x_n}^n \end{pmatrix}, \qquad \underline{v} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}, \qquad \underline{y} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

A is called a **Vandermonde** matrix which can be shown to have determinant $\prod_{0\leq i<j\leq n}(x_j - x_i)$ and so in our case since the x_i's are distinct, the determinant is non-zero and hence A is invertible, giving us our unique solution for $\underline{v} = A^{-1}\underline{y}$ and corresponding polynomial with coefficients $a_0, \dots, a_n$.

The key idea for finding parametrisations then is this: If we pick $n+1$ points $\{(x_i, y_i, z_i)\}_{i=0}^n$ from our data set and assign them each a t-value t_i, then we can generate Lagrange polynomials $L_x(t), L_y(t), L_z(t)$ of degree at most n corresponding to the points $\{(t_i, x_i)\}_{i=0}^n$, $\{(t_i, y_i)\}_{i=0}^n$ and $\{(t_i, z_i)\}_{i=0}^n$ respectively. With this we can then check in Sage whether or not $r(t) = (L_x(t), L_y(t), L_z(t))$ gives us a valid parametrisation i.e. the polynomials have integer coefficients and that $r(t)$ actually lies on the surface: $(L_x(t))^3 + (L_y(t))^3 + (L_z(t))^3 = 1$. Hence in order to find a quartic parametrisation we ought to pick 5 points.

4.4 Algorithm for Finding Parametrisations

In order to compute a quartic parametrisation we need to then pick 5 points and allocate them particular t-values. As we're dealing with a very large data set ($\sim 100,000$ points) to do this in a random fashion would be extremely inefficient; there are upwards of 10^{23} possible combinations of points we could pick before deciding what t-values to choose!

Hence we want to find a way to sensibly pick our points and corresponding t-values. It turns out from the initial analysis at the start of this section it makes sense to try to find consecutive points on a parametrisation. Indeed, for points $p_0 = (x_0, y_0, z_0)$ and $p_1 = (x_1, y_1, z_1)$ we were able to find candidate t-values at least for the first point as in 15 and 16 and that if the points actually lie on a parametrisation we at least expected the values t_x, t_y and t_z to be similar e.g. they have equal nearest whole number. At which point then it'd be reasonable to assign $t_0 = t_x$ to p_0 and $t_0 + 1$ to p_1. To then find the other consecutive points we then apply the same reasoning but this time p_1 playing the role of p_0 for which we can find a consecutive point p_2 and so on. A summary of such an algorithm implementing these ideas is as follows:

■ **Finding candidate consecutive points:**

- Start out with a given point in our data set p_1, not known to be on a quartic parametrisation. We want to find a suitable candidate for its 'consecutive' point p_2.
- Without loss of generality, p_1 is a point of the form $(+, -, -)$[30], we pick p_2 to be the next point in the solution set of the same form.
- We can then compute t_x, t_y, t_z as in (15) and (16) for this pair of points.
- If p_1 and p_2 do indeed lie on the same quartic parametrisation then we expect the computed t-values to be similar e.g. they all round to the same integer. Otherwise we progress onto the next p_2.

■ **Once we have such a pair:**

- These points are stored in a list in a dictionary containing all such lists of candidate consecutive points and their t-values.
- If there is a list with the point p_1 at the end of it we add p_2 with its corresponding t-value $t_x + 1$ to the end of that list.
- If not then we start a new list containing p_1 and p_2 along with corresponding t-values t_x and $t_x + 1$.
- Once a list has 5 points we're able to compute the Lagrange polynomials $L_x(t), L_y(t)$ and $L_z(t)$ from the data.
- We can then check if $r(t)$ is a quartic parametrisation or not; if so, great, otherwise we discard such a list.

Note that the above summary doesn't include all relevant details such as when to sensibly iterate our p_1 to the next point in the list, what range of values for p_2 to consider or how large the computed t-values should be to ensure accurate predictions. In the Sage code I present below, such problems are dealt with heuristically; such choices of variables were usually chosen for simplicity rather than on the basis of being the most optimal value:

[30] Each point in our data set is of the form $|x| \geq |y| \geq |z|$ and as a result the solutions are either of the form $(+, -, -)$ or $(-, +, +)$, the symbols denoting the signs of the entries. Moreover the solutions are ordered so that $|z|$ is increasing.

```
# Algorithm for finding quartic parametrisation
import sys

start = time.time()

my_dict = {} #Dicitonary to store lists of consecutive points
L = len(sols) #sols = list of solutions for B = 10^15
R = PolynomialRing(QQ,’t’)

for i in range(L):
    c1 = i; c2 = i+1
    x1, y1, z1 = sols[c1]; x2, y2, z2 = sols[c2] #consecutive points
    r_z = abs(z2/z1)^(1/3)

    while r_z <= 1.2: #ensures that t >= 5
        x1, y1, z1 = sols[c1]; x2, y2, z2 = sols[c2]
        r_z = RR((abs(z2/z1)^(1/3)))
        if abs(x1) >= abs(x2) or sign(x1) != sign(x2):
            c2+=1; continue

        r_x = RR((abs(x2/x1)^(1/4))); r_y = RR((abs(y2/y1)^(1/4)))
        r_z = RR((abs(z2/z1)^(1/3)))
        if r_x in ZZ or r_y in ZZ or r_z in ZZ:
            c2+=1; continue

        frac_x = QQ(frac(r_x)); frac_y = QQ(frac(r_y)); frac_z = QQ(frac(r_z))
        t_x = (1/frac_x).round(); t_y = (1/frac_y).round(); t_z = (1/frac_z).round()

        #Process of adding point(s) to list in dictionary:

        if t_z == t_x or t_z == t_y:

            list1 = [] #pairs of start and end points of lists of consec pts
            for i in my_dict.keys():
                list1 += [[i, my_dict[i][-1]]]
            list2 = [x[1] for x in list1] #list of all end points

            if not [t_z, sols[c1]] in list2:
                my_dict[(t_z, tuple(sols[c1]))] = [[t_z, sols[c1]], \
                [t_z + 1, sols[c2]]]

            elif [t_z, sols[c1]] in list2:
                index = list2.index([t_z, sols[c1]])
                key = list1[index][0]
                my_dict[key] += [[t_z + 1, sols[c2]]]

                #Computing Lagrange polys with 5 consecutive points:

                if len(my_dict[key]) == 5:
                    L_x(t) = R.lagrange_polynomial([(n[0],n[1][0]) \
                    for n in my_dict[key]])
                    L_y(t) = R.lagrange_polynomial([(n[0],n[1][1]) \
                    for n in my_dict[key]])
                    L_z(t) = R.lagrange_polynomial([(n[0],n[1][2]) \
                    for n in my_dict[key]])
                    c(t) = (L_x(t), L_y(t), L_z(t))

                    c_coeffs = L_x.coefficients() + L_y.coefficients() + L_z.coefficients()
                    if not all(x[0] in ZZ for x in c_coeffs):
                        my_dict.pop(key); c2+=1; continue

                    three_cubes = (L_x(t))^3 + (L_y(t))^3 + (L_z(t))^3
                    if three_cubes != 1:
                        my_dict.pop(key); c2+=1; continue
                    elif three_cubes == 1:
                        end = time.time()
                        print('- We have found a quartic:', c(t))
                        print('- The consecutive points and t-values used to find this parametrisation are:' \
                              , my_dict[key])

                        pts = [x[1] for x in my_dict[key]]
                        indexes = []
                        for i in pts:
                            a = sols.index(i)
                            indexes += [a]
                        print('- These points have corresponding entries in our list:', indexes)
                        sys.exit('found quartic parametrisation')

        c2+=1

    #Remove invalid entries from the dictionary:

    for i in my_dict.copy():
        if my_dict[i][-1][1] == sols[c1]:
            my_dict.pop(i, None)
```

The code then outputs the following:

```
- We have found the quartic parametrisation: (-9*t^4 - 3*t, 9*t^4, 9*t^3 + 1)
- The consecutive points and t-values used to find this parametrisation are:
  [[5, [-5640, 5625, 1126]], [6, [-11682, 11664, 1945]], [7, [-21630, 21609, 3088]],
  [8, [-36888, 36864, 4609]], [9, [-59076, 59049, 6562]]]
- These points have corresponding entries in our list: [22, 27, 31, 39, 43].
```

We see that such a method was able to find the parametrisation (3) with the minimal possible value of t that was allowed ($t = 5$). After removing all points from our data set that lie on this parametrisation, we're left with 3500 points for which we want to find any of the other parametrisations as given by Lehmer in (5). Adjusting the code by setting $d = 10$, $e = 9$, running over the set of non-quartic points, and ensuring that we have 11 points chosen before computing Lagrange polynomials we have the following output:

```
- We have found a degree-10 parametrisation:
  (3888*t^10 - 135*t^4, -3888*t^10 + 1296*t^7 - 81*t^4 - 3*t,
   -3888*t^9 + 648*t^6 + 9*t^3 + 1)
- The consecutive points and t-values used to find this parametrisation are:
  [[7, [1098263443977, -1097196650886, -156818584376]],
  [8, [4174707658752, -4171990634520, -521668652543]],
  [9, [13556616865353, -13550419554732, -1505946480902]],
  [10, [38879998650000, -38867040810030, -3887351990999]],
  [11, [100844704872153, -100819452661026, -9166552639100]],
  [12, [240734709303552, -240688275759396, -20059291075391]],
  [13, [535993812453177, -535912496544360, -41227165770218]],
  [14, [1124622093360528, -1124485485757242, -80325270732167]],
  [15, [2242016711915625, -2241795289100670, -149460400094624]],
  [16, [4274901199945728, -4274553321750576, -267170453876735]],
  [17, [7838184273670377, -7837652492790756, -461054022631406]]]
- These points have corresponding entries in our list:
  [1186, 1404, 1628, 1824, 2036, 2235, 2432, 2646, 2834, 3028, 3219].
```

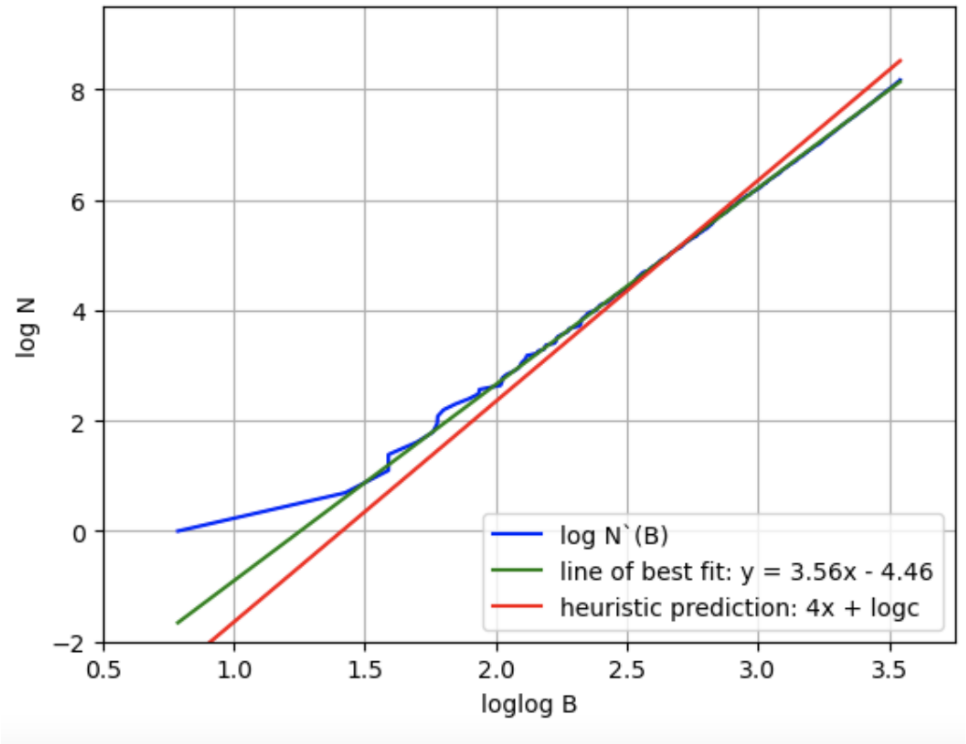
This matches up with the second term $(x_2(t), y_2(t), z_2(t)$ in (5). We also see that this is the extent of such an algorithm for this data set - any higher degree parametrisation wouldn't have enough points within our data set to work with[31]!

We now remove such points which lie on the two parametrisations that we have detected, from our data set. With this, we then count the number of remaining points, which will correspond to the modified counting function $N'(B)$ in (6) and compare it with the asymptotic prediction in the heuristic. For this, from (6), we use the fact that the rank of the Picard group of the variety $V(x^3 + y^3 + z^3 - 1) \subset \mathbb{A}^3_{\mathbb{Q}}$ is 3, $b = 1$ and $c \approx 0.0192$.

As we see in the figure below, the function $N'(B)$ asymptotically behaves like a constant times by $(\log B)^{3.56}$. As in [20], where all the parametrisations on the Fermat cubic were removed, we get in actuality that $N'(B)$ is closer to the prediction with the power of $\log B$ equal to 3.74.

There could be numerous reasons for these discrepancies: for example, it could be that our data set doesn't fully capture the long term behaviour of the actual modified counting function. However, to produce more data points, say to extend the x-axis of the graph to

[31] A degree n parametrisation will have roughly $B^{1/n}$ points in a data set with $max(x, y, z) \leq B$, so for $B = 10^{15}$ as we have, setting $n = 14$ for example we'll have less points than is needed to compute a Lagrange polynomial for corresponding degree!



4 for example, would be equivalent to searching for solutions of height up to $B = 10^{24}$! This would seem fairly futile: a more cost effective approach to this problem then seems to instead consider solutions to lots of examples of cubic surfaces for smaller heights, particularly those with lots of integral points.

5 Conclusion

In this project, we have seen a glimpse of the deep connection between between the geometric properties of cubic surfaces and the algebraic structures of their associated Picard groups. What's more, we have seen that when very little is known in general, as is the case for cubic surfaces, the use of computer software to construct algorithms to study specific examples proves very fruitful. In this project, I gave two algorithms to study the Picard group of the projective Fermat cubic surface and the parametrisations on the (affine) Fermat cubic, although as mentioned, there's no reason for these algorithms not to work for other examples of cubic surfaces.

Had I had more time for this project I would've like to test my algorithm for finding parametrisations on other examples of cubic surfaces. Moreover, I would've liked to compute the Picard group for the variety U given in subsection 1.5 for the heuristic, and gain a better understanding as to why the Picard group arises in such formulas at all.

Bibliography

References

[1] Michael Atiyah. *Introduction to commutative algebra.* CRC Press, 2018.

[2] Michel Bauer. Cubic surfaces and their invariants: Some memories of raymond stora. *Nuclear Physics B*, 912:374–425, 2016.

[3] Andrew R Booker and Andrew V Sutherland. On a question of Mordell. *Proceedings of the National Academy of Sciences*, 118(11):e2022377118, 2021.

[4] Martin Bright, Damiano Testa, and Ronald van Luijk. Geometry and arithmetic of surfaces, 2021.

[5] Timothy D Browning and DR Heath-Brown. Integral points on cubic hypersurfaces. *arXiv preprint math/0611086*, 2006.

[6] Bill Casselman. The babylonian tablet plimpton 322. `https://personal.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html`. Accessed: 31.03.2024.

[7] Amit Ghosh and Peter Sarnak. Integral points on Markoff type cubic surfaces. *Inventiones mathematicae*, 229(2):689–749, 2022.

[8] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[9] DR Heath-Brown. The density of zeros of forms for which weak approximation fails. *Mathematics of computation*, 59(200):613–623, 1992.

[10] John Lee. *Introduction to topological manifolds*, volume 202. Springer Science & Business Media, 2010.

[11] DH Lehmer. On the Diophantine equation x3+ y3+ z3= 1. *Journal of the London Mathematical Society*, 1(3):275–280, 1956.

[12] Hideyuki Matsumura. *Commutative algebra*, volume 120. WA Benjamin New York, 1970.

[13] Jeffrey CP Miller and Michael FC Woollett. Solutions of the Diophantine equation: x3+ y3+ z3= k. *Journal of the London Mathematical Society*, 1(1):101–110, 1955.

[14] James S Milne. *Algebraic geometry.* Allied Publishers, 2012.

[15] LJ Mordell. On the integer solutions of the equation x2+ y2+ z2+ 2xyz= n. *Journal of the London Mathematical Society*, 1(4):500–510, 1953.

[16] Miles Reid. Chapters on algebraic surfaces. *arXiv preprint alg-geom/9602006*, 1996.

[17] Karen Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves. *An invitation to algebraic geometry.* Springer Science & Business Media, 2004.

[18] Andrew Sutherland and Andrew Booker. Integer solutions on the fermat cubic surface [data set].

[19] Ravi Vakil. The rising sea: Foundations of algebraic geometry. *preprint*, 2017.

[20] Florian Wilsch and Tim Browning. Integral points on cubic surfaces via a hardy-littlewood heuristic. Conference presentation, December 2023. Oberseminar Number Theory, Göttingen Mathematical Institute.