Finding Rational Solutions on a Nonsingular Cubic Surface in P^3

Nathaniel Josephs
Advisor: Christopher Rasmussen

A thesis in Mathematics submitted to the faculty of Wesleyan University in partial fulfillment of the requirements for the degree of Master of Arts

Wesleyan University

Middletown, Connecticut

Spring, 2015

Acknowledgments

I would foremost like to thank my advisor Christopher J. Rasmussen. I have benefited greatly as a mathematician from his guidance and patience. His trust in my ability helped me through times of struggle, while his demand for precision challenged me in times of success. My sincerest thanks go out to Professor Rasmussen, without whom this project would not exist.

I also want to thank my committee members David Pollack and Cameron Hill, as well as everyone in the Wesleyan Mathematics Department. In particular, I want to thank the other first year students Nick, Ryan, Josh, Freda, and Noelle, whose conversations I enjoyed, mathematical and otherwise.

A special thanks to my family who have supported me throughout the completion of my degrees. Their love and support did not go unnoticed. I hope I made you all proud.

Last, but not least, I must thank Amy. You have pushed me from day 1 to be better and I accept the challenge. Thank you.

Abstract

The purpose of this thesis is to present a strategy for parametrizing the rational points on nonsingular, homogeneous cubic surfaces. The particular Diophantine equation we will consider is $X^3 + Y^3 + YZ^2 + W^3 = 0$. The strategy will be to find a family of singular cubic curves on our hypersurface with which to sweep through rational solutions, not unlike the standard parametrization of the circle. We enumerate the 27 lines on the surface in order to search for a rational point. The tangent plane is known to intersect a nonsingular cubic surface in a singular cubic curve. We present a 2-parameter set of solutions and discuss its possible incompleteness. Throughout, we provide an introduction to the necessary algebraic geometry, as well as presenting, in detail, our parametrization. We end with an explanation of how our process can be generalized for similar equations vis-a-vis a computer algebra package, such as SAGE.

Contents

1 Overview

The goal of this paper is to find the rational solutions to the equation

$$X^3 + Y^3 + YZ^2 + W^3 = 0.$$

This is known as a *Diophantine equation*. In the language of algebraic geometry, this polynomial defines a cubic surface. Throughout, we let

$$S = \mathbf{V}(X^3 + Y^3 + YZ^2 + W^3) \subseteq \mathbb{P}^3(\mathbb{C}).$$

If we want to parametrize a cubic surface, where should we start? Blindly scraping at the abyss of ingenuity may yield clever bits and pieces of a solution to any mathematical problem, but this approach denies the service of what is already known. Indeed, we will economize our mental energy by extending a classic approach to similar problems. In this case, we will consider the well-known strategy of finding all the rational points on a circle. Given a rational point on the unit circle, we can 'sweep' through all other rational points by parametrizing the line through our given rational point and any other rational point. Studying this example will reveal what we may borrow for our solution and what will require adjustment.

In general, it is much easier to find rational points on varieties with a rational singular point. Since S is nonsingular, we will not be able to immediately employ the sweeping strategy. Instead, we will find a singular subvariety of S. The intersection of S with a plane generically results in a curve. We can force a singularity on this curve by reverse-engineering a plane whose intersection with S is singular. This process will reveal a line contained on our singular curve. With one line in hand, we will be able to find the other 26 lines on S.

In particular, we will identify 2 skew lines on S, l and $\bar{l}$. By parametrizing points

on l and $\bar{l}$, we can define the family of lines passing through l and $\bar{l}$. Such lines will intersect our surface at a third, nontrivial point. With luck, we can force this third point to be rational by choosing particular coordinates for our parametrization of the points on l and $\bar{l}$. This rational point P lies on S and does not lie on any line on S. Obtaining P will allow us to employ the strategy from the parametrization of the unit circle.

Having found P, we will intersect S with $T_P S$, the tangent plane at P, creating a nondegenerate singular cubic curve. We will then apply the sweeping strategy a first time, to obtain a family of rational points on S. Each of these points also has a tangent plane whose intersection with S is a nondegenerate singular cubic curve. This family will be specified by a first parameter t. We will then repeat the sweeping strategy by introducing a second parameter u, which parametrizes the points on the family of nondegenerate singular cubic curves, giving a final solution in two parameters, as desired. This 2 parameter solution matches our intuition for an object of dimension two.

As a practical mater, this solution only lies in the open subvariety of S where $Z \neq 0$. Therefore we must recover the rational points on the relatively small subvariety for $Z = 0$. We do so by identifying $S \cap \mathbf{V}(Z)$ as an elliptic curve. We finish by discussing the completeness of our solution and arguing that what we have found is, at least, a dense set of rational solutions in the Zariski topology. Be that as it may, our strategy only produces a family of rational points, so although dense in $S(\mathbb{Q})$, our parametrization may still miss rational points on the surface.

Before we begin the project of finding the rational points on S, we study the rudiments of algebraic geometry, following the texts of Cox, Little, O'Shea [2], as well as Miles Reid [4]. We begin our study by introducing varieties, coordinate rings, and the correspondence between varieties and ideals. This connection between

geometry and algebra is fundamental. For instance, after we establish the ideal-variety correspondence, we extend it to projective space. We then describe the different maps between varieties and consider how these maps interact with ring homomorphisms. All of this allows us to make precise the notions of singularity and dimension, so that our intuition regarding the sweeping strategy can be properly applied to S. We also state the algorithms underlying SAGE, Software for Algebra and Geometry Experimentation [5], which we will use for our computations.

Sections 2 and 3 detail ideals and varieties in affine and projective space, respectively. Section 4 considers polynomial and rational functions, and section 5 outlines the computational tools used in the parametrization. Section 6 covers miscellaneous topics including the notions of dimension and singularity. Finally, Section 7 presents our parametrization of S in detail, concluding with a 2 parameter family of rational points on S. We include in the appendix the SAGE code used throughout to obtain our parametrization.

2 Ideals and Varieties in Affine Space

Our introduction to ideals and varieties revolves around Hilbert's Basis Theorem, a fundamental algebraic result that contributes to the foundations of algebraic geometry. This result, in conjunction with our definition of affine varieties, the objects of algebraic geometry, leads to another of Hilbert's major contributions– The Nullstellensatz. Our discussion culminates with the important correspondence between ideals and varieties.

2.1 Background Algebra

To begin, we recall a particular type of ring. For our purposes, we will work exclusively over the complex numbers, $\mathbb{C}$.

Definition 2.1. A ring R is **Noetherian** if every ideal in R is finitely generated.

Example 2.2. All fields are Noetherian since, in particular, they are principal ideal domains.

Such rings have a remarkable property, namely that their polynomial rings are also Noetherian. This is Hilbert's Basis Theorem. Here, we present a purely algebraic proof following [4] Theorem 3.3. Later, we present an alternate proof using Groebner bases. For our present demonstration, we must first recall the following fact about Noetherian rings.

Proposition 2.3. *A ring is Noetherian if and only if it satisfies the ascending chain condition for ideals.*

Proof. Suppose R is a Noetherian ring and consider a chain of ascending ideals $\{I_n\}$. That is, $I_1 \subseteq I_2 \subseteq \cdots$ with $I_i \subseteq R$. Then $\bigcup I_n$ is an ideal and since R is Noetherian, $\bigcup I_n$ is finitely generated, say $\bigcup I_n = (a_1, \ldots, a_k)$. Each $a_i \in I_{n_i}$ for

some n_i. Let $N = \max\{n \mid a_i \in I_n \text{ for some } i\}$ with respect to inclusion. Then $\bigcup I_{n_i} = (a_1, \ldots, a_k) \subseteq I_N$. Since the opposite containmemt is obvious, it follows that $\bigcup I_n = I_N$. Thus our chain terminates (at N) and R satisfies the ascending chain condition.

Conversely, suppose this condition is satisfied. Let $I \subseteq R$ be an ideal. We will use this ideal to build an ascending chain of ideals. We may assume that I is not the zero ideal, since $\{0\}$ is clearly finitely generated; so there is some $0 \neq x_1 \in I$. Let $I_1 = (x_1)$ with $I_1 \subseteq I$. If $I_1 \subsetneq I$, choose $x_2 \in I \setminus I_1$. Let $I_2 = (x_1, x_2)$ with $I_1 \subsetneq I_2 \subseteq I$. Repeating this process, we obtain an ascending chain of ideals, which terminates by assumption. That is, there is some $N \in \mathbb{N}$ with $I_N = I_{N+1} = \cdots = I$. Thus I is finitely generated, namely by the generators of I_N, contradicting our assumption. It follows that every ring satisfying the ascending chain condition is Noetherian. □

Theorem 2.4 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is also Noetherian.*

Proof. Let R be a Noetherian ring and suppose $I \subseteq R[x]$ is an ideal. We will build a finite generating set of I by considering the set of leading coefficients of the polynomials in I. We may assume I is nonzero, otherwise we are done. Let $I_n = \{a_n \in R \mid \exists f = a_n x^n + \cdots + a_0 \in I\} \cup \{0\} \subseteq R$, the set of leading coefficients of degree n polynomials in I together with 0. We claim that I_n is an ideal. First, I_n is nonempty since $0 \in I_n$. Next, if $a_n, b_n \in I_n$, then there exist some $f, g \in I$ with $f = a_n x^n + \cdots + a_0$ and $g = b_n x^n + \cdots + b_0$. Then $f - g \in I$ since I is an ideal. Hence, $a_n - b_n \in I_n$. Note that if $a_n = b_n$, then certainly $a_n - b_n = 0 \in I_n$. Next, let $a_n \in I_n$ and $r \in R$. Then, again, there is some $f \in I$ with $f = a_n x^n + \cdots + a_0$. By absorption, $r \cdot f \in I$, as we may view r simply as a constant polynomial in $R[x]$. Thus $ra_n \in I_n$ and I_n is indeed an ideal. Furthermore, we claim that $I_n \subseteq I_{n+1}$. To

see this, let $a \in I_n$. Then, there is some polynomial $f \in I$ with $f = a_n x^n + \cdots + a_0$. Since I is an ideal, $x \cdot f = a_n x^{n+1} + \cdots + a_0 x \in I$, hence $a_n \in I_{n+1}$. Since R is Noetherian and $I_n \subseteq R$, the ascending chain conditions guarantees that our chain of ideals terminates. That is, $I_N = I_{N+1} = \cdots$ for some $N \in \mathbb{N}$. Since I_d is finitely generated, let $I_d = (a_{d,1}, \ldots, a_{d,m})$ and let $f_{d,k}$ be the polynomial of degree d and leading coefficient $a_{d,k}$. We claim that I is equal to J, the ideal generated by these polynomials. That is, $J = (f_{d,k} \mid 0 \leq d \leq N, 1 \leq k \leq m) = I$. Clearly $J \subseteq I$.

For the sake of contradiction, suppose we did not have equality. Then there exists a polynomial of minimal degree in $I \setminus J$, say g. Let $\deg(g) = d$. If the leading term of g is bx^d, then $b \in I_d = (a_{d,1}, \ldots, a_{d,m})$, so $b = \sum_{i=1}^m r_i a_{d,i}$ with $r_i \in R$. We have two cases to consider. First, suppose $d \geq N$. We will construct a polynomial in J whose leading term is the same as g and consider their difference. First, note that $\sum_{i=1}^m r_i f_{N,i} \in J$, since this is a linear combination of polynomials in J. Moreover, the leading coefficient is $\sum_{i=1}^m r_i a_{d,i} = b$ and the degree is N. Next, we multiply this polynomial by x to a sufficiently large degree such that the leading term is exactly that of g. That is, $g' = x^{d-N} \sum_{i=1}^m r_i f_{N,i} \in J$. Hence g and g' both have leading term bx^d so that $\deg(g - g') < d$. But $g - g' \in I \setminus J$, contradicting the minimality of g.

For our second case, suppose $d < N$. We make a similar construction as before, only without needing to adjust for the degree of our polynomial. So, let $g' = \sum_{i=1}^m r_i f_{d,i} \in J$. Then $g - g' \in I \setminus J$, but $\deg(g - g') < d$, again contradicting the minimality of g. We conclude that there is no such element in I and not J. Hence $I \subseteq J$ and equality is ensured. We conclude that $R[x]$ is Noetherian. □

A simple induction argument yields the following result, which we will use often:

Corollary 2.4.1. *If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is also Noetherian.*

2.2 Varieties and Ideals

We now introduce affine space, the geometric world of affine varieties. Keep in mind that $\mathbb{A}^n(k)$ is just k^n in the language of algebraic geometry. This allows us to define the central object of algebraic geometry, an affine variety, which is simply the vanishing set for some given polynomials.

Definition 2.5. Let k be a field and $n \in \mathbb{N}$. Then

$$\mathbb{A}^n(k) = \{(x_1, \ldots, x_n) : x_i \in k\},$$

the set of n-tuples of elements from k, is called the **affine space of dimension** n **over** k. Such an n-tuple is called a **point**.

Remark 2.6. We say $\mathbb{A}^1(k)$ is the affine line and $\mathbb{A}^2(k)$ is the affine plane.

Example 2.7. $\mathbb{A}(\mathbb{R})$ is the real line and $\mathbb{A}^2(\mathbb{R})$ is the real coordinate plane.

Definition 2.8. If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then an **affine variety**, $\mathbf{V}(f_1, \ldots, f_s)$, is the set of common zeros of $f_1, \ldots, f_s$ in $\mathbb{A}^n(k)$. A subset of a variety that is also a variety is called a **subvariety**. Note that this author does not require that a variety be irreducible.

Remark 2.9. Such objects can be visualized as the graphs of their polynomials, as the next example demonstrates. This forms the basis for the connection between algebra and geometry.

Example 2.10. In $\mathbb{A}^2(\mathbb{R})$, the variety $\mathbf{V}(x^2 + y^2 - 1)$ is the unit circle.

Example 2.11. $\mathbf{V}(0) = \mathbb{A}^n(k)$ and $\mathbf{V}(k[x_1, \ldots, x_n]) = \emptyset$.

Remark 2.12. Definition 2.8 naturally extends to varieties defined over infinite families of polynomials, as we see with Example 2.11, since $k[x_1, \ldots, x_n]$ contains infinitely many polynomials.

With Definition 2.8, we are prepared to define the topology of choice for algebraic geometers.

Definition 2.13. The **Zariski Topology** is given by the varieties of $\mathbb{A}^n(k)$, which are the closed sets of this topology.

We will return to the Zariski Topology later in the paper. Our first result about varieties discusses what happens when we take unions and intersections of varieties.

Proposition 2.14. *Finite unions and finite intersections of affine varieties are also affine varieties.*

Proof. Let V and W be varieties. Then $V = \mathbf{V}(f_1, \ldots, f_s)$ and $W = \mathbf{V}(g_1, \ldots, g_t)$ for some f_i, g_j. Then $V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$. This is clear since $p \in V \cap W$ just in case p vanishes on all f_i and g_j, which is equivalent to p belonging to $\mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$.

Next, we claim that $V \cup W = \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$. To see this, let $p \in V$. Then p vanishes simultaneously at every f_i, hence $V \subseteq \mathbf{V}(f_i g_k)$. Likewise, $W \subseteq \mathbf{V}(f_i g_k)$, so $V \cup W \subseteq \mathbf{V}(f_i g_j)$. Conversely, let $p \in \mathbf{V}(f_i g_k)$ and suppose $p \notin V$. Then p does not vanish for some f_i, but it does vanish on $f_i g_j$ for $1 \leq j \leq t$. Thus p vanishes for every g_j and $p \in W$ as desired. □

Before we explore the deep connection between ideals and varieties, we first introduce the ideal function, which turns a variety into an ideal, and justify the name of this function. In the next section, we will explore some of its basic properties.

Definition 2.15. If $X \subseteq \mathbb{A}^n(k)$,

$$\mathbf{I}(X) = \{f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in X\}.$$

In words, $\mathbf{I}(X)$ consists of all the polynomials vanishing at every point in X.

Remark 2.16. $\mathbf{I}(\mathbb{A}^n(k)) = \{0\}$ for any infinite field k, since nonzero polynomials have only finitely many roots.

Proposition 2.17. *Given $X \subseteq \mathbb{A}^n(k)$, $\boldsymbol{I}(X)$ is an ideal in the ring $k[x_1, \ldots, x_n]$.*

Proof. First, $0 \in \mathbf{I}(X)$ since the zero polynomial vanishes everywhere. Next, suppose $f, g \in \mathbf{I}(X)$. By definition, for any $p \in X$, $f(p) = g(p) = 0$. Thus $(f+g)(p) = f(p) + g(p) = 0$, so $f + g \in \mathbf{I}(X)$. Finally, if $f \in \mathbf{I}(X)$ and h is any polynomial in $k[x_1, \ldots, x_n]$, then $(fh)(p) = f(p)h(p) = 0$, so $fh \in \mathbf{I}(X)$. Thus $\mathbf{I}(X)$ is an ideal. □

Remark 2.18. We call $\mathbf{I}(X)$ the ideal of X.

2.3 Results From First Principles

We record below a series of results which follow purely from the definitions of ideals and varieties, following the propositions and excerises in [2] Chapter 4. The first several results explore the varieties of sums and products of ideals. The later results explain the inclusion reversing nature of the ideal and variety maps.

Proposition 2.19. *Let I and J be ideals. Then $\boldsymbol{V}(I + J) = \boldsymbol{V} \cap \boldsymbol{J}$.*

Proof. If $p \in \mathbf{V}(I + J)$, then p vanishes at all polynomials in $I + J$. Since $I \subseteq I + J$, it follows that $p \in \mathbf{V}(I)$. Likewise, $p \in \mathbf{V}(J)$. Thus $p \in \mathbf{V}(I) \cap \mathbf{V}(J)$ and $\mathbf{V}(I + J) \subseteq \mathbf{V}(I) \cap \mathbf{V}(J)$. Conversely, let $p \in \mathbf{V}(I) \cap \mathbf{V}(J)$. We want to show that for $f \in I + J$, $f(p) = 0$. So, let $f \in I + J$. Then $f = g + h$ for some $g \in I, h \in J$. By assumption, $g(p) = h(p) = 0$. Thus $f(p) = 0$, so $p \in \mathbf{V}(I + J)$ as desired, and equality follows. □

By induction, we obtain the following result.

Corollary 2.19.1. *If I_k is an ideal for $k \in \Omega$, then $\boldsymbol{V}(\sum_{k\in\Omega} I_k) = \bigcap_{k\in\Omega} \boldsymbol{V}(I_k)$.*

Proposition 2.20. *Let I and J be ideals. Then $\boldsymbol{V}(IJ) = \boldsymbol{V}(I) \cup \boldsymbol{V}(J)$.*

Proof. If $p \in \mathbf{V}(IJ)$, then $f(p)g(p) = 0$ for all $f \in I, g \in J$. Since we are working in a field, in particular a domain, either $f(p) = 0$ or $g(p) = 0$. In either case, $p \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Conversely, if $p \in \mathbf{V}(I) \cup \mathbf{V}(J)$, then either $f(p) = 0$ or $g(p) = 0$ for all $f \in I$ or $g \in J$. Thus $h(p) = f(p)g(p) = 0$ for all $h \in IJ$, and $p \in \mathbf{V}(IJ)$. □

Proposition 2.21. *Let I and J be ideals. If $I \subseteq J$, then $\boldsymbol{V}(I) \supseteq \boldsymbol{V}(J)$, i.e $\boldsymbol{V}$ is inclusion-reversing.*

Proof. Suppose $I \subseteq J$. If $p \in \mathbf{V}(J)$, p vanishes on all polynomials in J, so that p certainly vanishes on all polynomials in $I \subseteq J$. Thus $\mathbf{V}(I) \supseteq \mathbf{V}(J)$. □

The next result is our first application of the inclusion-reversing property of $\mathbf{V}$.

Proposition 2.22. *Let I and J be ideals. Then $\boldsymbol{V}(I \cap J) = \boldsymbol{V}(I) \cup \boldsymbol{V}(J)$.*

Proof. If $p \in \mathbf{V}(I) \cup \mathbf{V}(J)$, then either $f(p) = 0$ for all $f \in I$ or $g(p) = 0$ for all $g \in J$. Either way, $h(p) = 0$ for all $h \in I \cap J$, hence $p \in \mathbf{V}(I \cap J)$ and $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$. Conversely, since $IJ \subseteq I \cap J$, it follows that $\mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ)$. By Proposition 2.20, we have our desired equality. □

Next, we offer a counterpart to Proposition 2.21 regarding the inclusion-reversing property of $\mathbf{I}$.

Proposition 2.23. *If X and Y are subsets of $\mathbb{A}^n$ such that $X \subseteq Y$, then $\boldsymbol{I}(X) \supseteq \boldsymbol{I}(Y)$. Furthermore, if X and Y are varieties, then the converse is true.*

Proof. Let $f \in \mathbf{I}(Y)$. By definition, f vanishes for all points in Y, hence f vanishes for all points in X. Thus $f \in \mathbf{I}(X)$ and $\mathbf{I}(X) \supseteq \mathbf{I}(Y)$. Now suppose that X and Y are varieties with $\mathbf{I}(X) \supseteq \mathbf{I}(Y)$. Since Y is a variety, it is defined by polynomials $f_1, \ldots, f_s$. It follows that $f_1, \ldots, f_s \in \mathbf{I}(X)$. That is, these polynomials vanish on X. Since Y is the set of all zeroes of these polynomials, we have $X \subseteq Y$. □

Proposition 2.24. *If W is a variety, then $W = \boldsymbol{V}(\boldsymbol{I}(W))$.*

Proof. Suppose $f \in \mathbf{I}(W)$. By definition, f vanishes on W, so $W \subseteq \mathbf{V}(\mathbf{I}(W))$, as $\mathbf{V}(\mathbf{I}(W))$ contains all points where f vanishes. Conversely, if $f_1, \ldots, f_s$ are the polynomials defining W, then $f_1, \ldots, f_s \in \mathbf{I}(W)$ by definition. Hence $(f_1, \ldots, f_s) \subseteq \mathbf{I}(W)$. We showed above that $\mathbf{V}$ is inclusion-reversing, so $W = \mathbf{V}((f_1, \ldots, f_s)) \supseteq \mathbf{V}(\mathbf{I}(W))$, which establishes the other direction. □

While we would like the same to be true for ideals, namely that the ideal of a variety of and ideal is just the original ideal, this is not the case. One direction holds, but several problems can occur for the other direction. We consider when such problems occur in the examples after the proposition.

Proposition 2.25. *If J is an ideal, then $J \subseteq \boldsymbol{I}(\boldsymbol{V}(J))$, though equality need not occur.*

Proof. Let $f \in J$. Then $f(p) = 0$ for all $p \in \mathbf{V}(J)$. It follows that $f \in \mathbf{I}(\mathbf{V}(J))$. Hence $J \subseteq \mathbf{I}(\mathbf{V}(J))$. □

Example 2.26. Let $f = x^2 + 1 \in \mathbb{R}[x]$ and let $J = (f)$. Then $J \neq \mathbb{R}[x]$ since $1 \notin J$, but $\mathbf{V}(J) = \emptyset$ since the only roots of f are complex. Thus $\mathbf{I}(\mathbf{V}(J)) = \mathbf{I}(\emptyset) = \mathbb{R}[x]$ and $J \neq \mathbf{I}(\mathbf{V}(J))$.

Example 2.27. Consider the setup in Example 2.26, only suppose $f \in \mathbb{C}[x]$. Then $\mathbf{V}(J) = \{\pm i\}$. Thus $\mathbf{I}(\mathbf{V}(J)) = \mathbf{I}(\{\pm i\}) = (f)$, hence $\mathbf{I}(\mathbf{V}(J)) = J$.

Example 2.28. Let $f = x$ and $g = x^2$. Then $\mathbf{V}(f) = \{0\} = \mathbf{V}(g)$, but $(f) \neq (g)$. In fact, for $n \geq 1$, $\mathbf{V}(f) = \mathbf{V}(f^n)$.

2.4 The Nullstellensatz

To ensure equality in Proposition 2.25, we need to introduce the radical ideal. This will provide enough structure to prevent the problem in Example 2.28 above. In fact,

we are always afforded this solution by taking the radical of an ideal. Example 2.26 will be resolved when we confine ourselves to algebraically closed fields, as we saw with Example 2.27. Integrating these modifications into our previous proposition, we will finally attain Hilbert's Nullstellensatz. Literally translating as "zero-locus-theorem," the Nullstellensatz reveals exactly when a variety is non-empty. Recall that a locus is simply a set of points satisfying some specified conditions, which generalizes our notion of a variety.

Definition 2.29. Let R be a commutative ring. An ideal $I \subseteq R$ is **radical** if whenever $f^m \in I$ for some $m \in \mathbb{N}$, it follows that $f \in I$.

Example 2.30. $\langle x, y, z \rangle \subseteq \mathbb{C}[x, y, z]$ and $2\mathbb{Z} \subseteq \mathbb{Z}$ are both radical ideals.

Example 2.31. Neither $\langle x^3, y^6, z^9 \rangle \subseteq \mathbb{C}[x, y, z]$ nor $4\mathbb{Z} \subseteq \mathbb{Z}$ are radical ideals.

Our first result shows that taking the ideal of a variety gives us a radical ideal.

Proposition 2.32. *If V is a variety, then $\boldsymbol{I}(V)$ is radical.*

Proof. If $p \in V$ and $f^m \in \mathbf{I}(V)$, then $(f(p))^m = 0$, which implies $f(p) = 0$, hence $f \in \mathbf{I}(V)$. □

We can always produce a radical ideal given an ideal as follows.

Definition 2.33. Let $I \subseteq R$ be an ideal. Then the **radical** of I is

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

Proposition 2.34. *Let I be an ideal. Then $\sqrt{I}$ is a radical ideal containing I.*

Proof. Clearly $I \subseteq \sqrt{I}$, thus $\sqrt{I}$ is nonempty. Now suppose $f, g \in \sqrt{I}$. Thus $f^m, g^n \in I$ for some $m, n \in \mathbb{N}$. The Binomial Theorem shows that $(f+g)^{m+n} \in I$, hence $f + g \in \sqrt{I}$. Similarly, if $h \in k[x_1, \ldots, x_n]$, then $(hf)^m \in I$ by the absorption

properties of the ideal I. So $hf \in \sqrt{I}$. Thus $\sqrt{I}$ is an ideal. By definition, it is radical. $\square$

Proposition 2.35. *Let I and J be ideals. Then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*

Proof. If $f \in \sqrt{I \cap J}$, then $f^m \in I \cap J$, so $f^m \in I$ and $f^m \in J$. By definition, $f \in \sqrt{I}$ and $f \in \sqrt{J}$, and the forward direction is established. Conversely, if $f \in \sqrt{I} \cap \sqrt{J}$, then $f \in \sqrt{I}$ and $f \in \sqrt{J}$. Thus $f^m \in I$ and $f^n \in J$ for some $m, n \in \mathbb{N}$. Then $f^{m+n} \in I \cap J$, which implies $f \in \sqrt{I \cap J}$. $\square$

Next, we define the notion of an irreducible variety. We acknowledge that in the history, and in current use, some authors refer to this object simply as a variety, and instead call the set $\mathbf{V}(X)$ a vanishing set or an algebraic set.

Definition 2.36. A variety V is **irreducible** if whenever $V = V_0 \cup V_1$ with V_0, V_1 varieties, then either $V_0 = V$ or $V_1 = V$.

Here, we prove the Weak Nullstellensatz and the Nullstellensatz following Theorem's 1 and 2, respectively, in [2] Chapter 4, Section 1.

Theorem 2.37 (Weak Nullstellensatz)**.** *Let k be algebraically closed. If $\boldsymbol{V}(I) = \emptyset$, then $I = k[x_1, \ldots, x_n]$.*

Proof. We proceed by induction on n. When $n = 1$, $k[x]$ is a PID, so $I = (f)$ for some polynomial f. If $\mathbf{V}(I) = \emptyset$, then f has no roots in k. However, since k is algebraically closed, it follows that f is some non-zero constant, which is a unit in k, thus $1 \in I$. Hence $I = k[x]$.

Suppose the result is true for $n - 1$ variables. Let I be an ideal in $k[x_1, \ldots, x_n]$. By Hilbert's basis theorem, $I = (f_1, \ldots, f_s)$ for some polynomials $f_i \in k[x_1, \ldots, x_n]$. If f_1 is a nonzero constant, then again $1 \in I$ and we are done. Otherwise, take

f_1 to be some polynomial of positive degree N. Consider the following change of coordinates T:

$$x_1 = \widetilde{x_1}$$
$$x_i = \widetilde{x_i} + a_i\widetilde{x_1} \text{ for } 2 \leq i \leq n,$$

where $a_i \in k$ are fixed constants whose values we specify below. Using this substitution, we obtain

$$f_1(x_1, \ldots, x_n) = f_1(\widetilde{x_1}, \ldots, \widetilde{x_n} + a_n\widetilde{x_1}) = c(a_2, \ldots, a_n)\widetilde{x_1}^N + \mathcal{O}(\widetilde{x_1}),$$

where $\mathcal{O}(\widetilde{x_1})$ consists of terms of $\widetilde{x_1}$ of degree strictly less than N. We claim that $c(a_2, \ldots, a_n) \neq 0$. Notice that $f_1(1, 0, \ldots, 0) \neq 0$ if and only if $c(a_2, \ldots, a_n) \neq 0$. Now, if $f_1(1, 0, \ldots, 0) = 0$, then choose some a_i such that $f_1(a_2, \ldots, a_n) \neq 0$. We know that we can do this since f is a nonzero constant. Thus T replaces $(a_2, \ldots, a_n)$ with $(1, 0, \ldots, 0)$ as a vanishing point so that $c(a_2, \ldots, a_n) \neq 0$. Since $c(a_2, \ldots, a_n)$ is not the zero polynomial, and k is algebraically closed, hence infinite, let the a_i satisfy $c(a_2, \ldots, a_n) \neq 0$. Now, using this transformation, there exists an $\widetilde{f}$ for any f. We show that $\widetilde{I} := \{\widetilde{f} \mid f \in I\}$ is an ideal in $k[\widetilde{x_1}, \ldots, \widetilde{x_n}]$. First $0 \in \widetilde{I}$ because $0 \in I$ and the transformation sends 0 to 0. Next, if $\widetilde{f}, \widetilde{g} \in \widetilde{I}$, then $f, g \in I$, hence $f + g \in I$. So $\widetilde{f + g} \in \widetilde{I}$. A similar argument shows that if $\widetilde{f} \in \widetilde{I}$, then $\widetilde{fh} \in \widetilde{I}$ for all $\widetilde{h} \in k[\widetilde{x_1}, \ldots, \widetilde{x_n}]$. In fact, since T is an isomorphism, $\widetilde{I} = T(I)$ is an ideal.

Similarly, since $\mathbf{V}(I) = \emptyset$, $\mathbf{V}(\widetilde{I}) = \emptyset$, otherwise we could pull back a root for $\mathbf{V}(I)$. Now if we can show that $1 \in \widetilde{I}$ then we are done, because constants are unaffected by our linear transformation, which would imply that $1 \in I$. So consider the projection map $\pi : \mathbb{A}^n(k) \to \mathbb{A}^{n-1}(k)$ and let $\widetilde{I_1} = \widetilde{I} \cap k[\widetilde{x_2}, \ldots, \widetilde{x_n}]$. We claim that $\mathbf{V}(\widetilde{I_1}) = \pi(\mathbf{V}(\widetilde{I})) = \pi(\emptyset) = \emptyset$. In other words, we claim that π is

surjective, since if $\mathbf{V}(\widetilde{I_1}) \neq \emptyset$, we could pullback a point $(a_2, \ldots, a_n) \in \mathbf{V}(\widetilde{I_1})$ to $(a_1, \ldots, a_n) \in \mathbf{V}(\widetilde{I})$. This follows from a result on ring-finiteness, whose proof can be found in [3] Chapter 1. Since $\mathbf{V}(\widetilde{I_1}) = \emptyset$, we see from the induction hypothesis that $\widetilde{I_1} = k[\widetilde{x_2}, \ldots, \widetilde{x_n}]$. Thus $1 \in \widetilde{I}$ because $1 \in \widetilde{I_1} \subseteq \widetilde{I}$. □

Theorem 2.38 (Nullstellensatz)**.** *Let k be algebraically closed and let J be some ideal in $k[x_1, \ldots, x_n]$. Then $\boldsymbol{I}(\boldsymbol{V}(J)) = \sqrt{J}$.*

Proof. If $f \in \sqrt{J}$, then $f^m \in J$ for some $m \in \mathbb{N}$. Thus $f^m(p) = f(p)^m = 0$ for all $p \in \mathbf{V}(J)$. Since f vanishes on $\mathbf{V}(J)$, f belongs to $\mathbf{I}(\mathbf{V}(J))$. Conversely, suppose $f \in \mathbf{I}(\mathbf{V}(J))$. Thus f vanishes on $\mathbf{V}(J)$ by definition. By Hilbert's Basis Theorem, J is finitely generated, say $J = (f_1, \ldots, f_s)$. Now consider the ideal $J' = (f_1, \ldots, f_s, 1 - yf) \subseteq k[x_1, \ldots, x_n, y]$. We will show that $\mathbf{V}(J') = \emptyset$. Let $p = (a_1, \ldots, a_{n+1}) \in \mathbb{A}^{n+1}(k)$. If $p \in \mathbf{V}(J)$, then $(1 - yf)(p) = 1 - a_{n+1}f(a_1, \ldots, a_n) = 1 \neq 0$. Thus $p \notin \mathbf{V}(J')$. On the other hand, if $p \notin \mathbf{V}(J)$, then there is some f_i such that $f_i(p) \neq 0$. We can consider f_i as a function in $n + 1$ variables independent of the final variable. Again, $p \notin \mathbf{V}(J')$. Since $p \in \mathbb{A}^{n+1}(k)$ was arbitrary, we conclude that $\mathbf{V}(J') = \emptyset$. By the Weak Nullstellensatz, $J' = k[x_1, \ldots, x_n, y]$, thus $1 \in J'$. So $1 = \sum_{i=1}^{s} g_i(x_1, \ldots, x_n, y)f_i + h(x_1, \ldots, x_n, y)(1 - yf)$ for some polynomials $g_i, h \in k[x_1, \ldots, x_n, y]$. Letting $y = 1/f(x_1, \ldots, x_n)$, we have $1 = \sum_{i=1}^{s} g_i(x_1, \ldots, x_n, 1/f)f_i$. Then there exists some N large enough to clear the denominators on the right. Multiplying through by f^N, we obtain $f^N = \sum_{i=1}^{s} p_i f_i$ for some polynomials $p_i \in k[x_1, \ldots, x_n]$. Thus $f^N \in J$, which is exactly the condition for $f \in \sqrt{J}$. □

2.5 Ideal-Variety Correspondence

We end this section by collecting our results about the ideal-variety correspondence. In particular, there is a one-to-one correspondence between radical ideals

and varieties. This dictionary allows us to go between the realms of algebra and geometry, preserving certain features of ideals and varieties. One of these features regards prime ideals and irreducible varieties, whose relationship we determine below. Finally, we end this section by noting that we can decompose any variety into irreducible components.

Theorem 2.39 (The Ideal-Variety Correspondence)**.** *The two maps* $\boldsymbol{I}$ *and* $\boldsymbol{V}$ *are inclusion-reversing, i.e if* $I \subseteq J$ *are ideals, then* $\boldsymbol{V}(I) \supseteq \boldsymbol{V}(J)$ *and if* $V \subseteq W$ *are varieties, then* $\boldsymbol{I}(V) \supseteq \boldsymbol{I}(W)$*. Furthermore,* $\boldsymbol{I}$ *is injective. Moreover, if we take* k *to be algebraically closed and we restrict ourselves to radical ideals, then these maps are actually inclusion-reversing bijections inverse to each other.*

Proof. We have already proved these results save for the final claim. Note that Proposition 2.24 revealed that $\mathbf{I}$ is injective. So suppose k is algebraically closed and consider J, a radical ideal. We must show that $\mathbf{I}(\mathbf{V}(J)) \subseteq J$, since we established the other direction for any ideal in Proposition 2.25. By the Nullstellensatz, $\mathbf{I}(\mathbf{V}(J)) = \sqrt{J}$. Since J is radical by assumption, $J = \sqrt{J}$, as desired. It follows immediately that $\mathbf{V}$ and $\mathbf{I}$ are, indeed, inverses of each other. □

Corollary 2.39.1. *There is a one-to-one correspondence between varieties in* $\mathbb{A}^n(k)$ *and radical ideals in* $k[x_1, \ldots, x_n]$*.*

Next, we note that $\mathbf{V}(\mathbf{I}(S))$ is the smallest variety that contains the set S in a precise sense.

Proposition 2.40. *For any variety* W *containing the set* S*,* W *also contains* $\boldsymbol{V}(\boldsymbol{I}(S))$*.*

Proof. If W is some variety which contains S, then $\mathbf{I}(W) \subseteq \mathbf{I}(S)$ because $\mathbf{I}$ is inclusion-reversing. Similarly, applying $\mathbf{V}$ we obtain $\mathbf{V}(\mathbf{I}(W)) \supseteq \mathbf{V}(\mathbf{I}(S))$. Since

W is a variety, $\mathbf{V}(\mathbf{I}(W)) = W$ by Proposition 2.24. Hence $W \supseteq \mathbf{V}(\mathbf{I}(S))$, and we conclude that $\mathbf{V}(\mathbf{I}(S))$ is the smallest such variety. $\square$

Our final results involve the restriction of the ideal-variety correspondence to subsets of ideals in $k[x_1, \ldots, x_n]$ and subsets of varieties in $\mathbb{A}^n(k)$. In particular, we look at how the ideal-variety correspondence sends irreducible varieties to prime ideals and vice-versa, and likewise for single points and maximal ideals. For these claims, we follow [4] Section 3.7 and [2] Chapter 4, Section 5, Theorem 11, respectively. Lastly, we show that every variety may be written as a disjoint union of irreducible varieties, following [4] Section 3.7. This decomposition will be important as we begin to study the dimension of a variety in Section 6.

Proposition 2.41. *If V is a variety, then V is irreducible if and only if $\boldsymbol{I}(V)$ is a prime ideal.*

Proof. We will argue both directions by contrapositive. Let V be a variety and suppose V is reducible. Thus $V = V_0 \cup V_1$ for some $V_0, V_1 \subsetneq V$. By the inclusion-reversing property of $\mathbf{I}$, there exists some $f_0 \in \mathbf{I}(V_0) \backslash \mathbf{I}(V)$. Similarly, there exists some $f_1 \in \mathbf{I}(V_1) \backslash \mathbf{I}(V)$. Then $f_0 f_1$ vanishes at all points in V, so $f_0 f_1 \in \mathbf{I}(V)$. However, $f_0, f_1 \notin \mathbf{I}(V)$ by construction, so $\mathbf{I}(V)$ is not prime. Conversely, suppose $\mathbf{I}(V)$ is not prime. Then there exists some $f_0, f_1 \notin \mathbf{I}(V)$ such that $f_0 f_1 \in \mathbf{I}(V)$. Consider the ideals $I_0 = (I(V), f_0)$ and $I_1 = (I(V), f_1)$. Let $V_0 = \mathbf{V}(I_0)$ and $V_1 = \mathbf{V}(I_1)$. By construction, $V_0, V_1 \subsetneq V$. However, $V \subseteq V_0 \cup V_1$ because for all $p \in V$, $f_0 f_1(p) = 0$ implies $f_0(p) = 0$ or $f_1(p) = 0$. Thus $V = V_0 \cup V_1$, i.e V is reducible. $\square$

Corollary 2.41.1. *There is a one-to-one correspondence between prime ideals in $k[x_1, \ldots, x_n]$ and irreducible varieties in $\mathbb{A}^n(k)$.*

Proposition 2.42. *If V is a variety, then V is a single point if and only if $\boldsymbol{I}(V)$ is maximal.*

Proof. First, note that $\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$, i.e varieties consisting of a single point are of the form $\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n)$. We will argue that every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$. So suppose I is maximal. Since I is proper by definition, $I \neq k[x_1, \ldots, x_n]$. By the Weak Nullstellensatz, we get that $\mathbf{V}(I) \neq \emptyset$, hence there is some $(a_1, \ldots, a_n) \in \mathbf{V}(I)$ such that $f(a_1, \ldots, a_n) = 0$ for all $f \in I$. It follows that if $f \in I$, then $f \in \mathbf{I}(\{(a_1, \ldots, a_n)\})$, so $I \subseteq \mathbf{I}(\{(a_1, \ldots, a_n)\})$. We claim that $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n)$. Since $\mathbf{V}(\mathbf{I}(\{(a_1, \ldots, a_n)\})) = (a_1, \ldots, a_n)$ by the Nullstellensatz, and since we observed earlier that $\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$, we see that $\mathbf{V}(\mathbf{I}(\{(a_1, \ldots, a_n)\})) \subseteq \mathbf{V}(x_1 - a_1, \ldots, x_n - a_n)$. By the reverse-inclusion of $\mathbf{I}$, we obtain $\mathbf{I}(\{(a_1, \ldots, a_n)\}) \supseteq (x_1 - a_1, \ldots, x_n - a_n)$. Conversely, if $p \in \mathbf{V}(x_1 - a_1, \ldots, x_n - a_n)$, then $p = (a_1, \ldots, a_n)$ from our previous discussion, thus $\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathbf{V}(\mathbf{I}(\{(a_1, \ldots, a_n)\}))$. Since our claim is proved, we see that $I \subseteq \mathbf{I}(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n) \subsetneq k[x_1, \ldots, x_n]$. However, since I is maximal, we must have $I = (x_1 - a_1, \ldots, x_n - a_n)$. Thus every maximal ideal is of the form $(x_1 - a_1, \ldots, x_n - a_n)$.

Now we will argue that if $I \subseteq k[x_1, \ldots, x_n]$ is an ideal of the form $(x_1 - a_1, \ldots, x_n - a_n)$, then I is maximal. Let I be such an ideal and suppose J is an ideal with $I \subsetneq J \subseteq k[x_1, \ldots, x_n]$. So there is some polynomial $f \in J \backslash I$. By the division algorithm, we may write $f = \sum_{i=1}^{n} g_i(x_i - a_i) + r$ for some $r \in k$. We may assume $r \neq 0$, otherwise $f = \sum_{i=1}^{n} g_i(x_i - a_i) \in I$, as the right hand side of our equality is a linear combination of generators from I. Now, since $f \in J$ and $\sum_{i=1}^{n} g_i(x_i - a_i) \in I \subseteq J$, we know that $f - \sum_{i=1}^{n} g_i(x_i - a_i) \in J$ because J is closed under subtraction as an ideal. However, $b = f - \sum_{i=1}^{n} g_i(x_i - a_i)$, which

implies $b \in J$. Since b is a nonzero element of k, it is a unit. Thus $1 \in J$ and $J = k[x_1, \ldots, x_n]$. We conclude that I is maximal. $\square$

Corollary 2.42.1. *There is a one-to-one correspondence between maximal ideals in $k[x_1, \ldots, x_n]$ and points in $\mathbb{A}^n(k)$.*

As it happens, Proposition 2.42 is equivalent to the Weak Nullstellensatz, which we show following [4] Section 3.10.

Proposition 2.43. *Proposition 2.42 is equivalent to the Weak Nullstellensatz*

Proof. We have already showed that the Weak Nullstellensatz implies Proposition 2.42. So suppose that a variety V is a single point if and only if $\mathbf{I}(V)$ is maximal. We will show that if $I \neq k[x_1, \ldots, x_n]$, then $\mathbf{V}(I) \neq \emptyset$. We know that I is contained in some maximal ideal J. By assumption, $J = (x_1 - a_1, \ldots, x_n - a_n)$, i.e $\mathbf{V}(J) = \{(a_1, \ldots, a_n)\}$. Since $I \subseteq J$, we know that $\mathbf{V}(I) \supseteq \mathbf{V}(J)$. Thus $\mathbf{V}(I) \neq \emptyset$ since $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. $\square$

Proposition 2.44 (The Descending Chain Condition)**.** *Any descending chain of varieties must terminate.*

Proof. Let

$$V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots$$

be a descending chain of varieties. Applying $\mathbf{I}$ to this chain, we obtain

$$\mathbf{I}(V_0) \subseteq \mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \cdots .$$

By the ascending chain condition, there exists $N \in \mathbb{N}$ such that

$$\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \cdots .$$

Since V is a variety, $\mathbf{V}(\mathbf{I}(V)) = V$ by Proposition 2.24. Thus $V_N = V_{N+1} = \cdots$ and our claim is proved. $\square$

Proposition 2.45. *Every variety has a decomposition into irreducible varieties.*

Proof. Let Ω be the set of varieties without a decomposition into irreducible varities. Suppose $\Omega \neq \emptyset$. By the descending chain condition, this set has a minimal element, say V. By the definition of Ω, V cannot be irreducible. So $V = V_0 \cup V_1$ for some varieties $V_0, V_1 \subsetneq V$. By the minimality of V, V_0 and V_1 have decompositions. Then the union of their decomposition is a desired decomposition for V, a contradiction. Thus Ω is empty and all varieties have decompositions into irreducible varieties. $\square$

3 Ideals and Varieties in Projective Space

In many senses, our discussion in the previous section of ideals and varieties in affine space is incomplete. Often there are hidden roots, points that should belong to a variety, that are absent from the picture, even literally if we are thinking geometrically. For example, every pair of lines in affine space meets at exactly one point unless the pair of lines is parallel. We resolve this exception in projective space by allowing parallel lines to meet at a point at infinity. This will align with our notion of algebraically closed fields, where polynomials have exactly the number of roots as the degree of the polynomial, with our geometric intuition of roots as intersections on graphs.

To develop some intuition of projective space, we may take the vantage point of an algebraist or a geometer. Algebraically, we consider $\mathbb{P}^2(\mathbb{R})$ as the collection of one dimensional subspaces of $\mathbb{R}^3$. Consequently, the standard results from linear algebra apply. Geometrically, $\mathbb{P}^2(\mathbb{R})$ is the set of lines through the origin in $\mathbb{R}^3$. To see this, consider a point $p \in \mathbb{P}^2(\mathbb{R})$ with homogeneous coordinates $p = (X : Y : Z)$. Then $p = \lambda(X : Y : Z)$ for $\lambda \in \mathbb{R} - \{0\}$. Observe that for every λ, our point considered in $\mathbb{R}^3$ lies on the same line through the p and the origin. Since $p = (X : Y : Z) \neq (0 : 0 : 0)$, the line does indeed lie in $\mathbb{R}^3$. On the other hand, given a line L through the origin in $\mathbb{R}^3$, we can recover a point $p = (x, y, z)$ on $L - \{0\}$, which is a unique point in $\mathbb{P}^2(\mathbb{R})$ since every other point on $L - \{0\}$ has the form $\lambda(x, y, z)$. Either notion of projective space is correct, and like all of mathematics, we will take whichever viewpoint is most convenient for any given situation.

We begin this section by formally generalizing the above notion. We continue by determining what conditions are necessary in order to extend the object of an affine variety to projective space, which allows us to define explicitly a hypersurface, the object we aim to parametrize. The conditions we settle upon allow us to

explore the projective ideal-variety correspondence, which we will use to extend the Nullstellensatz to projective space. Much of this section will mirror the previous section, so throughout we will try to highlight similarieties and differences between the affine and the projective cases.

3.1 Basics

Definition 3.1. Projective n-space over k is

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

where $(x_0, \ldots, x_n) \sim \lambda(x_0, \ldots, x_n)$. Equivalently, this is the set of lines through the origin in $\mathbb{A}^{n+1}(k)$.

We will soon see that one reason we disallow the point $(0, 0, \ldots, 0)$ is that such a point would lie on every hypersurface, as we require a hypersurface in projective space to be homogeneous. Another reason is that $(0, 0, \ldots, 0)$ would lie in multiple equivalence classes.

Definition 3.2. Points in $\mathbb{P}^n(k)$ are given as **homogeneous coordinates**

$$(x_0 : \cdots : x_n).$$

Note that $(x_0 : \cdots : x_n) \sim \lambda(x_0 : \cdots : x_n)$ for all $\lambda \neq 0$.

Definition 3.3. $U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(K) \mid x_i \neq 0\}$.

The previous definition gives a standard covering of $\mathbb{P}^n$ by copies of $\mathbb{A}^n$, which we give following [2] Chapter 8, Section 2, Proposition 2.

Proposition 3.4. *The map* $\phi_i : \mathbb{A}^n(k) \to \mathbb{P}^n(k)$ *defined by*

$$\phi((a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)) = (a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$$

is one-to-one between $\mathbb{A}^n(k)$ *and* $U_i \subseteq \mathbb{P}^n(k)$.

Proof. It is clear that im $\phi_i = U_i$. We define an inverse map $\phi^{-1} : U_i \to \mathbb{A}^n(k)$ by

$$\phi^{-1}(a_1, \ldots, a_n) = (\frac{a_1}{a_i}, \ldots, \frac{a_n}{a_i}).$$

Note that $(a_1, \ldots, a_n) \in U_i$ has normalized form $\lambda(a_1, \ldots, a_n) = (\frac{a_1}{a_i}, \ldots, 1, \ldots, \frac{a_n}{a_i})$ with $\lambda = \frac{1}{a_i}$, as $a_i \neq 0$. We remark that ϕ^{-1} is well-defined since $\phi^{-1}(a_1, \ldots, a_n) = \phi^{-1}(\lambda a_1, \ldots, \lambda a_n) = (\frac{a_1}{a_i}, \ldots, \frac{a_n}{a_i})$ for any nonzero λ. Finally, it is clear that these maps are inverses so that ϕ is is one-to-one between $\mathbb{A}^n(k)$ and U_i. □

Definition 3.5. By the previous proposition, we see that $\mathbb{P}^n(k) = U_i \cup H_i$ with $H_i = \{p \in \mathbb{P}^n(k) \mid p = (x_0, \ldots, 0, \ldots, x_n)\}$. That is, projective n-space consists of U_i together with the points where $x_i = 0$. We can identify U_i with the affine space $\mathbb{A}^n(k)$, and we call H_i the **hyperplane at infinity** with respect to x_i. A similar argument to the previous proposition also shows that H is one-to-one with the n-tuples $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ with two points being equal if they are nonzero scalar multiples of each other. It follows that $H \cong \mathbb{P}^{n-1}(k)$.

The previous discussion demonstrates how we can think of $\mathbb{A}^n(k)$ as sitting inside of $\mathbb{P}^n(k)$. As such, we have the following observation:

$$\mathbb{P}^n = U_i \cup H_i$$

with $U_i \cong \mathbb{A}^n$ and $H_i \cong \mathbb{P}^{n-1}$.

We want to next extend the notion of a variety to projective space. However, the evaluation of polynomials at a projective point is not well-defined in general.

Example 3.6. Let $f(x, y) = x^2 - y \in \mathbb{C}[x, y]$. Then $p = (2 : 4) \sim (4 : 8)$ since $(4 : 8) = 2(2 : 4)$, but $f(2 : 4) \neq f(4 : 8)$. So f does not induce on a function on $\mathbb{P}^1$.

To avoid this problem, we restrict ourselves to a certain kind of polynomial.

Definition 3.7. Homogeneous polynomials are polynomials of degree n such that each term has total degree exactly n.

The following proposition guarantees that the notion of a homogeneous polynomial vanishing at a point in $\mathbb{P}^n$ is well-defined.

Proposition 3.8. *Let $p = (a_0 : \cdots : a_n) \in \mathbb{P}^n$ and $f \in k[x_0, \ldots, x_n]$. Then $f(p) = 0$ if and only if $f(\lambda p) = 0$.*

Proof. Let $(a_0 : \cdots : a_n)$ and $(\lambda a_0 : \cdots : \lambda a_n)$ both represent the point $p \in \mathbb{P}^n(k)$. Suppose that $f(a_0 : \cdots : a_n) = 0$. If f is homogeneous of degree l, then each term in f has the form $c \cdot x_0^{\epsilon_0} \cdots x_n^{\epsilon_n}$, where $c \in k$ and $\epsilon_0 + \cdots + \epsilon_n = l$. Setting $x_i = \lambda a_i$, we obtain $c \cdot (\lambda a_0)^{\epsilon_0} \cdots (\lambda a_n)^{\epsilon_n} = \lambda^l \cdot c \cdot a_0^{\epsilon_0} \cdots a_n^{\epsilon_n}$. Consequently $f(\lambda a_0 : \cdots : \lambda a_n) = \lambda^l f(a_0 : \cdots : a_n) = 0$. □

Definition 3.9. Let $f_1, \ldots, f_s$ be homogeneous polynomials in $k[x_0, \ldots, x_n]$. The **projective variety** of $f_1, \ldots, f_s$. is defined as in the affine case,

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_0, \ldots, a_n) \in \mathbb{P}^n(k) \mid f_i(a_0, \ldots, a_n) = 0 \ \forall \ 1 \leq i \leq s\}.$$

As in the affine case, we may define the Zariski topology for $\mathbb{P}^n(k)$.

Definition 3.10. The **Zariski Topology** is given by the varieties of $\mathbb{P}^n(k)$, which are the closed sets of this topology.

We are finally ready to define a particularly nice projective variety, in fact the object of central interest in this thesis. As is common in mathematics, objects defined over a single, other object, are given a special name (e.g *cyclic groups, principal ideals, simple extensions*).

Definition 3.11. A projective variety defined by a single nonzero homogeneous polynomial is called a **hypersurface**. A degree 1 hypersurface is called a **hyperplane**, while hypersurfaces of dimension 1 or 2 are considered **curves** or **surfaces**, respectively.

Note that every variety is the intersection of finitely many hypersurfaces. For any ideal I, Hilbert's Basis Theorem guarantees that $I = (f_1, \ldots, f_s)$. Thus $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(f_1) \cap \cdots \cap \mathbf{V}(f_s)$. Next, we explain how the open sets U_i let us cover projective varieties with affine varieties following [2] Chapter 8, Section 2, Proposition 5.

Proposition 3.12. *If $V = \boldsymbol{V}(f_1, \ldots, f_s) \subseteq P^n(k)$ is a projective variety, then we can identify $V \cap U_0$, the subset of points of V with non-zero first coordinate, with the affine variety $\boldsymbol{V}(g_1, \ldots, g_s) \subseteq \mathbb{A}^n(k)$ where $g_i(x_1, \ldots, x_n) = f_i(1, x_1, \ldots, x_n)$ for each $1 \leq i \leq s$.*

Proof. First, note that $V \cap U_0$ is indeed an affine variety because $V \cap U_0 \subseteq U_0 \subseteq \mathbb{A}^n(k)$, so that $V \cap U_0$ contains all the points in U_0 that vanish on the f_i. Now, using $\phi^{-1} : U_0 \to \mathbb{A}^n(k)$ from Proposition 3.4, we see that

$$\phi^{-1}(V \cap U_0) \subseteq \mathbf{V}(g_1, \ldots, g_s).$$

Conversely, if $(a_1, \ldots, a_n) \in \mathbf{V}(g_1, \ldots, g_s)$, then $(1, a_1, \ldots, a_n) \in U_0$ satisfies

$$f_i(1, a_1, \ldots, a_n) = g_i(a_1, \ldots, a_n) = 0.$$

So using $\phi : \mathbb{A}^n(k) \to U_0$ from Proposition 3.4, $\phi(\mathbf{V}(g_1, \ldots, g_s)) \subseteq V \cap U_0$. As inverse maps, we conclude that points of $V \cap U_0$ correspond directly to points of $\mathbf{V}(g_1, \ldots, g_s)$. □

Remark 3.13. While we proved Proposition 3.12 for $i = 0$, the result holds for any U_i.

Naturally, we wish to understand how the polynomials of an affine variety relate to the homogeneous polynomials of a projective variety. The following gives a technique for making any polynomial homogeneous.

Definition 3.14. Given a polynomial $f \in k[x_1, \ldots, x_n]$, not necessarily homogeneous, let f_j be the sum of all terms of f of total degree j. We can expand f as $f = \sum_j f_j$. Each f_j is the j-th **homogeneous component** of f.

Definition 3.15. If $f = \sum_j f_j$ is the expansion of f, a polynomial of degree d, of its homogeneous components, then

$$\begin{aligned} f^h(x_0, \ldots, x_n) &= \sum_{i=0}^{j} f_i(x_1, \ldots, x_n) x_0^{d-1} \\ &= f_j(x_1, \ldots, x_n) + f_{j-1}(x_1, \ldots, x_n) x_0 + \cdots + f_0(x_1, \ldots, x_n) x_0^d \end{aligned}$$

is a homogeneous polynomial of degree d in $k[x_0, \ldots, x_n]$. We call f^h the **homogenization** of f with respect to x_0.

Essentially, we identify a non-homogeneous polynomial in a polynomial ring over n variables with a homogeneous polynomial in a polynomial ring over $n+1$ variables (say $\mathbf{V}(f) \subseteq \mathbb{A}^n(k)$ to $\mathbf{V}(f^h) \subseteq \mathbb{P}^n(k)$) by scaling by the appropriate monomial x_0^d in each term.

A compact formula for f^h is given by

$$f^h = x_0^k \cdot f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}).$$

Definition 3.16. Given a homogeneous polynomial $f \in k[x_0, \ldots, x_n]$, the **dehomogenization** of f with respect to x_0 is $f(1, x_1, \ldots, x_n)$.

Remark 3.17. Although Definition 3.16 only considers dehomogenizing with respect to x_0, we may dehomogenize with respect to any variable.

Remark 3.18. The dehomogenization of f^h returns f. That is, $f^h(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$.

Definition 3.19. An ideal is **homogeneous** if for each $f \in I$, it follows that the homogeneous components, f_k, of f lie in I.

Definition 3.20. The **homogenization** of an ideal I is

$$I^h = (f^h \mid f \in I).$$

Note that although $(f_1^h, \ldots, f_s^h) \subseteq I^h$ for $I = (f_1, \ldots, f_s)$, equality need not occur.

Proposition 3.21. *I^h is a homogeneous ideal.*

Proof. If $g \in I^h$, then $g = \sum_{i=1}^n p_i f_i^h$. Since g is a linear combination of homogeneous polynomials, every component of g, in particular its homogeneous components, is a a product of some f_i^h, hence in I^h. Thus I^h is a homogeneous ideal, as desired. □

3.2 The Projective Ideal-Variety Correspondence

As in the affine case, we can create a dictionary between varieties and ideals in projective space. However, some caution needs to be applied as the dictionary

does not translate exactly. For example, the sum of two homogeneous ideals is not homogeneous if they are of a different degree. Thus any correspondence between ideals and varieties must require a stricter type of ideal.

Proposition 3.22. *An ideal I is homogeneous if and only if I is generated by a finite set of homogeneous polynomials.*

Proof. If I is a homogeneous ideal then by the Hilbert Basis theorem, we can write $I = (f_1, \ldots, f_s)$ for some polynomials f_i, not necessarily homogeneous. Let J be the ideal generated by the homogeneous components of each f_i. We will show that $I = J$. Clearly $I \subseteq J$ since every f_i is a sum of generators from J. Conversely, $J \subseteq I$ because each homogeneous component of f_i is in I, as I is a homogeneous ideal. Hence I has a basis of homogeneous ideals. Now, suppose I has a basis of homogeneous ideals, say $I = (f_1, \ldots, f_s)$. Then, for $f \in I$, we can write $f = \sum_{i=1}^{s} h_i f_i$ for some polynomials h_i. Moreover, we can expand each h_i as a sum of its homogeneous components, $h_i = \sum_{j=1}^{k} h_{ij}$. Substituting, we obtain

$$f = \sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} f_i.$$

Since h_{ij} and f_i are homogeneous, so is their product. Here, we see that, when sorted by the distinct degrees of $h_{ij} f_i$, each homogeneous component is a linear combination of f_i's. Hence each homogeneous component lies in I, which is exactly the criteria for I to be a homogeneous ideal. □

Proposition 3.23. *Given a homogeneous ideal I,*

$$\boldsymbol{V}(I) = \{p \in \mathbb{P}^n(k) \mid f(p) = 0 \ \forall f \in I\}$$

is a projective variety. Conversely, given a projective variety V and an infinite field

k,

$$\boldsymbol{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid f(a_0, \ldots, a_n) = 0 \ \forall (a_0, \ldots, a_n) \in V\}$$

is a homogeneous ideal.

Proof. Since $I = (f_1, \ldots, f_s)$ for some homogeneous polynomials f_i, it follows that $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$ is a projective variety. For the second claim, it is clear that $\mathbf{I}(V)$ is an ideal. To see that it is homogeneous, let $f \in \mathbf{I}(V)$ and $p \in V$. Then $f(\lambda(a_0, \ldots, a_n)) = 0$, where $\lambda(a_0, \ldots, a_n)$ represent the homogeneous coordinates of p. Expanding f as its homogeneous components, $f = \sum_k f_k$, we see that $f(\lambda(a_0, \ldots, a_n)) = f(\lambda a_0, \ldots, \lambda a_n) = \sum_k \lambda^k f_k(a_0, \ldots, a_n) = 0$. Hence each f_k vanishes at p, so $f_i \in \mathbf{I}(V)$, showing that $\mathbf{I}(V)$ is homogeneous. □

Proposition 3.24. *As in the affine case, the maps $\boldsymbol{I}$ and $\boldsymbol{V}$ are inclusion-reversing given the conditions of Proposition 3.23, namely the restriction to homogeneous ideals and projective varieties. Moreover, for any projective variety, $\boldsymbol{V}(\boldsymbol{I}(W)) = W$.*

Proof. The proofs of these claims follow closely the affine case, and so are omitted.

The complete correspondence between ideals and varieties in projective space will be presented at the end of the next section, when we have the proper tools to state the correspondence in full form.

3.3 The Projective Nullstellensatz

The next question is whether the different Nullstellensatz theorems have analogues in the projective case. However, the Weak Nullstellensatz fails for some homogeneous ideals.

Example 3.25. Let $I = (x_0, \ldots, x_n) \subsetneq k[x_0, \ldots, x_n]$ be an ideal. Clearly this is a homogeneous ideal, as its generating polynomials are each homogeneous. However,

$\mathbf{V}(I) = \emptyset$ since the only point that simultaneously vanishes on each x_i is $(0 : \cdots : 0)$, which is not in $\mathbb{P}^n(k)$.

Remark 3.26. We call I the **irrelevant ideal**.

Fortunately this is the only type of example, where $(0 : \cdots : 0)$ is the only vanishing point, where the Nullstellensatz fails. We will establish this with the Projective Weak Nullstellensatz, but first we examine what happens when we take the radical of a homogeneous ideal following [2] Chapter 8, Section 3, Proposition 7.

Proposition 3.27. *The radical of a homoegeneous ideal is homogeneous.*

Proof. If $f \in \sqrt{I}$, then $f^m \in I$ for some $m \in \mathbb{N}$. Suppose f is nonzero, otherwise we are done. Let f have degree d. Writing f as a sum of its homogeneous components, we obtain $f = \sum_k f_k = f_d + \sum_{k<d} f_k$. Then f^m has leading term $(f_d)^m$, i.e $(f^m)_d = (f_d)^m$. So $(f^m)_d = (f_d)^m \in I$ because I is homogeneous, implying that $f_d \in \sqrt{I}$. Now, since $f, f_d \in \sqrt{I}$, their difference is in I. Say $g = f - f_d$. Repeating this argument, we see that $g_{d'} \in \sqrt{I}$, where the degree of g is d', and likewise for all homogeneous components of f. By definition, $\sqrt{I}$ is a homogeneous ideal. □

We now present the Projective Nullstellensatz following [4] Section 5.3.

Theorem 3.28 (Projective Weak Nullstellensatz)**.** *If J is a homogeneous ideal, then $\boldsymbol{V}(J) = \emptyset$ if and only if $(x_0, \ldots, x_n) \subseteq \sqrt{J}$.*

Proof. Suppose J is a homogeneous ideal. Let $\mathbf{V}_{\text{aff}}(J) \subseteq \mathbb{A}^{n+1}$ be the corresponding affine variety of J. Then $\mathbf{V}(J) = \emptyset$ if and only if $\mathbf{V}_{\text{aff}}(J) \subseteq \{0\}$, i.e $\mathbf{V}_{\text{aff}}(J) = \{0\}$ or $\mathbf{V}_{\text{aff}}(J) = \emptyset$. By the inclusion-reversing property of $\mathbf{I}_{\text{aff}}$, this occurs just in case $\mathbf{I}_{\text{aff}}(\mathbf{V}_{\text{aff}}(J)) \supseteq \mathbf{I}_{\text{aff}}(\{0\})$. But $\mathbf{I}_{\text{aff}}(\mathbf{V}_{\text{aff}}(J)) = \sqrt{J}$ by the affine Nullstellensatz. Also, $\mathbf{I}_{\text{aff}}(\{0\}) = (x_0, \ldots, x_n)$. Thus $\mathbf{V}(J) = \emptyset$ if and only if $\sqrt{J} \supseteq (x_0, \ldots, x_n)$. □

Remark 3.29. In the proof of the Projective Weak Nullstellensatz, we were careful to distinguish between the affine variety and ideal maps and their projective analogues. We ignore this distinction moving forward when it is clear from context which maps we are using.

Definition 3.30. $\mathbf{V}_{\text{aff}}(J)$ from above is called the **affine cone** over the projective variety $\mathbf{V}(J)$. Note that $\mathbf{V}_{\text{aff}}(J)$ contains all homogeneous coordinates of the points in $\mathbf{V}(J)$.

The Strong Nullstellensatz will complete the missing pieces of the projective ideal-variety correspondence.

Theorem 3.31 (Projective Strong Nullstellensatz)**.** *If k is algebraically closed, J is homogeneous, and $V = \boldsymbol{V}(J)$ is a nonempty projective variety, then $\boldsymbol{I}(\boldsymbol{V}(J)) = \sqrt{J}$.*

Proof. Let J be a homogeneous ideal and suppose $\mathbf{V}(J) \neq \emptyset$. By the Projective Weak Nullstellensatz, $(x_0, \ldots, x_n) \not\subseteq \sqrt{J}$. Then $f \in \mathbf{I}(\mathbf{V}(J))$ if and only if $f \in \mathbf{I}(\mathbf{V}_{\text{aff}}(J))$ if and only if $f \in \sqrt{J}$, by the affine Nullstellensatz. Hence $\mathbf{I}(\mathbf{V}(J)) \subseteq \sqrt{J}$. The reverse inclusion is the same as the affine case. □

We now present, in full, the correspondence between ideals and varieties in projective space. Through the Projective Nullstellensatz and Propositions 3.23 and 3.24 from the previous section, we have actually already proved all of these claims.

Theorem 3.32 (Projective Ideal-Variety Correspondence)**.** *The ideal and variety maps defined over nonempty, projective varieties and radical, homogeneous ideals properly contained in $(x_0, \ldots, x_n)$, respectively, are inclusion-reversing bijections. Moreover, they are inverses of each other.*

Finally, we state Bezout's Theorem, which describes the intersection of curves in $\mathbb{P}^2$. We give the theorem without proof since the known arguments are beyond

the scope of what we have covered. A proof can be found in [3] Section 5.3.

Theorem 3.33 (Bezout's Theorem)**.** *Let k be an algebraically closed field. Let C and D be curves in $\mathbb{P}^2(k)$ with no common components. Suppose the degrees of their reduced, defining equations are m and n, respectively. Then they intersect at mn points, counting multiplicity.*

4 Polynomial and Rational Functions

In this section we discuss different mappings between varieties. As before, we explore the connection between geometry and algebra when we pass from polynomial maps to coordinate rings. To this end, we describe sufficient and necessary criteria for two varieties to be isomorphic, in a precise sense described below. We then turn our attention to the function field of a variety, where we define rational maps, although we will see that these are not actually functions. We conclude with an equivalency weaker than isomorphism known as birational equivalence which characterizes irreducible varieties.

4.1 Polynomial Maps and Coordinate Rings

We begin by defining a map from an affine variety to its base field.

Definition 4.1. If $V \subseteq \mathbb{A}^n$ is a variety, then a function $\phi : V \to k$ is a **polynomial function** if there exists some polynomial $f \in k[x_1, \ldots, x_n]$ with $\phi(p) = f(p)$ for all $p \in V$, i.e ϕ is the restriction map $f \restriction_V : \mathbb{A}^n(k) \to k$. We say that f **represents** ϕ.

Using this idea, we define a map between varieties and introduce the notion of isomorphism of varieties.

Definition 4.2. If $V \subseteq \mathbb{A}^m(k), W \subseteq \mathbb{A}^n(k)$ are varieties, then a function $\phi : V \to W$ is a **polynomial mapping** or **regular mapping** if there exists some polynomials $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$ satisfying $\phi(p) = (f_1(p), \ldots, f_n(p))$ for all $p \in V$. Again, we say that $f_1, \ldots, f_n$ **represent** ϕ.

Definition 4.3. Two varieties V and W are **isomorphic** provided there exists regular mappings $\phi : V \to W$ and $\psi : W \to V$ such that $\phi \circ \psi = \psi \circ \phi = \mathrm{id}$.

Definition 4.4. The **coordinate ring** $k[V]$ is the set of all regular mappings from V to k together with coordinate-wise addition and multiplication.

Since $\mathbf{I}(V)$ is an ideal, it is natural to consider the quotient $k[x_1, \ldots, x_n]/\mathbf{I}(V)$. First, however, we connect the idea of a polynomial representing a regular mapping with the equivalence relation of belonging to an ideal.

Proposition 4.5. *If V is an affine variety, then f and g represent the same regular function if and only if $f - g \in \boldsymbol{I}(V)$.*

Proof. If f and g represent the same function, then $f(p) - g(p) = 0$ for every $p \in V$ by definition. Thus $f - g \in \mathbf{I}(V)$. Conversely, if $f - g \in \mathbf{I}(V)$, then $f(p) - g(p) = 0$ for all $p \in V$. □

Proposition 4.6. $k[V] \cong k[x_1, \ldots, x_n]/\boldsymbol{I}(V)$.

Proof. We define $\varphi : k[x_1, \ldots, x_n] \to k[V]$ by $f \mapsto f \restriction_V$. It is trivial to check that φ is a homomorphism. By definition, the kernel is $\mathbf{I}(V)$, since these are all the polynomials vanishing on V, each of which gets mapped to $0 : V \to k \in k[V]$. Since this map is clearly surjective, $k[V] \cong k[x_1, \ldots, x_n]/\mathbf{I}(V)$. □

In the same way we defined maps between varieties, we may define maps between coordinate rings. Since coordinate rings are rings, these maps will turn out to be ring homomorphisms, and our usual notion of ring isomorphism will apply. We will see that, in fact, both notions of isomorphism are equivalent. Propositions 4.7 and 4.8 follow [2] Chapter 5, Section 4, Proposition 8 and Theorem 9, respectively.

Proposition 4.7. *Let $\phi : V \to W$ be a regular mapping. Then for every polynomial function $\psi \in k[W]$, there is an associated homomorphism $\phi^* : k[W] \to k[V]$ defined by $\phi^*(\psi) = \psi \circ \phi$. $\phi*$ is a k-homomorphism, called the **pullback mapping** of*

functions. Conversely, given such a ring homomorphism $f : k[V] \to k[W]$, there is a unique regular mapping $\sigma : V \to W$ with $f = \sigma^*$.

Proof. Since ψ is a map from $W \to k$, and $\psi \circ \phi$ is a map from $V \to k$, it is clear that $\phi^*(\psi)$ is a map from $V \to K$. Thus ϕ^* is indeed a map from $k[V]$ to $k[W]$. To see that ϕ^* is a k-homomorphism, let $\alpha, \beta \in k[W]$. Then $\phi^*(\alpha + \beta) = (\alpha + \beta) \circ \phi^* = (\alpha \circ \phi^*) + (\beta \circ \phi^*) = \phi^*(\alpha) + \phi^*(\beta)$. Similarly, $\phi^*(\alpha\beta) = (\alpha\beta) \circ \phi^* = (\alpha \circ \phi^*)(\beta \circ \phi^*) = \phi^*(\alpha)\phi^*(\beta)$. Finally, since α and β fix constants, it follows that ϕ^* fixes constants, hence ϕ^* is a k-homomorphism. A similar argument shows that every k-homomorphism comes from a pullback mapping. □

Proposition 4.8. *Two varieties are isomorphic if and only if their coordinate rings are isomorphic.*

Proof. Let V and W be isomorphic varieties, and let $\phi : V \to W$ and $\psi : W \to V$ be their inverse regular mappings. Suppose $\alpha \in k[W]$. Then $(\phi \circ \psi)^*(\alpha) = \mathrm{id}^*(\psi) = \psi \circ \mathrm{id} = \alpha$. Furthermore $(\phi \circ \psi)^*(\alpha) = \alpha \circ (\phi \circ \psi) = (\alpha \circ \phi) \circ \psi = \phi^*(\alpha) \circ \psi = \psi^*(\phi^*(\alpha)) = (\psi^* \circ \phi^*)(\alpha)$. Together this implies that $(\phi \circ \psi)^* = \psi^* \circ \phi^* = \mathrm{id}$, where $(\phi \circ \psi)^*$ maps $k[W]$ to itself. Likewise, $(\psi \circ \phi)^* = \phi^* \circ \psi^* = \mathrm{id}$, where $(\psi \circ \phi)^*$ maps $k[V]$ to itself. This shows that $k[V]$ and $k[W]$ are isomorphic as rings. Conversely, suppose $\phi^* : k[W] \to k[V]$ is a k-isomorphism. We can assume that ϕ^* is the pullback of some regular map $\phi : V \to W$ from our previous results. Similarly, ϕ^{*-1} is the pullback of the regular map $\phi^{-1} : W \to V$. We need to show that $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \mathrm{id}$. Using a similar argument as the forward direction, we see that for any $\alpha \in k[W]$, $(\phi \circ \phi^{-1})^*(\alpha) = \phi^{*-1}(\phi^*(\alpha)) = (\phi^{*-1} \circ \phi^*)(\alpha) = \alpha$. Hence $(\phi \circ \phi^{-1})^* = \mathrm{id}$ and thus $\phi \circ \phi^{-1} = \mathrm{id}$. Likewise, $\phi^{-1} \circ \phi = \mathrm{id}$. We conclude that V and W are isomorphic as varieties. □

4.2 Rational Maps and Birational Equivalence

By introducing the fraction field of $k[V]$, we may expand our class of functions on V.

Definition 4.9. If V is an irreducible variety, then

$$k(V) := \{\phi/\psi \mid \phi, \psi \in k[V],\ \psi \neq 0\} = \{[f]/[g] \mid f, g \in k[x_1, \ldots, x_n],\ g \notin \mathbf{I}(V)\}$$

is the **function field** on V, where $[f]$ is $f/\mathbf{I}(V)$.

As always, we consider the maps of $k(V)$ and how they admit an equivalence of varieties.

Definition 4.10. If $V \subseteq k^n$ and $W \subseteq k^m$ are varieties, then a **rational mapping** from V to W is a function ϕ represented by

$$\phi(\overline{x}) = (\frac{f_1(\overline{x})}{g_1(\overline{x})}, \ldots, \frac{f_m(\overline{x})}{g_m(\overline{x})})$$

with $\overline{x} = (x_1, \ldots, x_n)$, where $\frac{f_i}{g_i}$ are such that ϕ is defined at some point in V and for every point $p \in V$ where ϕ is defined, it follows that $\phi(p) \in W$. We write $\phi : V - - \to W$ to denote a rational mapping because ϕ is not necessarily a function, as ϕ may not be defined at every point of V.

Definition 4.11. Two rational mappings $\phi, \psi : V - - \to W$ are **equivalent** if $f_i k_i - h_i g_i \in \mathbf{I}(V)$ for all i, where such mappings are represented by $(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n})$ and $(\frac{h_1}{k_1}, \ldots, \frac{h_n}{k_n})$.

Proposition 4.12. *Let $\phi, \psi : V - - \to W$ be rational maps. Then $\phi = \psi$ if and only if there exists a subvariety $V' \subsetneq V$ with ϕ and ψ defined on $V - V'$ and $\phi(p) = \psi(p)$ for all $p \in V - V'$.*

Proof. Suppose $\phi = \psi$, with $\phi = (f_1/g_1, \ldots, f_n/g_n)$ and $\psi = (h_1/k_1, \ldots, h_n/k_n)$. Let $V_1 = \mathbf{V}(g_1 \cdots g_n)$ and $V_2 = \mathbf{V}(k_1 \cdots k_n)$. Then $V' = V_1 \cup V_2$ is a proper subvariety of V, since V_1 and V_2 are proper subvarieties and V is irreducible. Then ϕ and ψ are defined on $V - V'$. Since $f_i k_i - h_i g_i \in \mathbf{I}(V)$ by definition of equality, it follows that $f_i/g_i = \phi$ and $h_i/k_i = \psi$ are identical on $V - V'$. For the converse, if ϕ and ψ are identical on $V - V'$, then, by definition, $f_i/g_i = k_i/h_i$ on $V - V'$ for each $1 \leq i \leq n$, so that $f_i/g_i - k_i/h_i$ vanishes everywhere in $V - V'$. Then $f_i/g_i - k_i/h_i \in \mathbf{I}(V)$, hence $\phi = \psi$. □

Since a rational map on V is not necessarily a function on V, we need to specify where such maps are actually defined. This will allow us to compose rational maps, or at least identify where such compositions are possible. The immediate relevance of composition is that we may check when the composition of two maps is an identity map, which will lead to another type of equivalence.

Definition 4.13. Given two rational mappings ϕ and ψ, then $\psi \circ \phi$ is **defined** if there is some point $p \in V$ such that ϕ is defined at p and ψ is defined at $\phi(p)$.

Definition 4.14. Two irreducible varieties V and W are **birationally equivalent** if there exist rational mappings $\phi : V - - \to W$ and $\psi : W - - \to V$ with $\phi \circ \psi$ defined and $\phi \circ \psi = \mathrm{id}$. A variety that is birationally equivalent to k^n for some n is called a **rational variety**.

We end this section by specifying when rational maps are regular.

Definition 4.15. Let $f : V - - \to W$ be a rational map. Suppose $U \subseteq V$. Then $f : U \to W$ is a **morphism** if f is defined at every point in U. Moreover, if $U_1 \subseteq V$ and $U_2 \subseteq W$, then a morphism $f : U_1 \to U_2$ is a morphism $f : U_1 \to W$ with $f(U_1) \subseteq U_2$. If a morphism has a two-sided inverse which is also a morphism, we say it is an **isomorphism**.

5 A Computational Approach to Algebraic Geometry

We review the algorithms underlying our computational search. To do so, we introduce the notion of a monomial ordering which allows us to order polynomials in several variables. This brings to light an analogue to the usual division algorithm. With this tool, we define Groebner bases and an algorithm for constructing them. Along the way, we provide an alternate proof for Hilbert's Basis Theorem.

5.1 Polynomials in Many Variables

We begin our computational approach by defining the many parts of a polynomial in multiple variables. Unlike in the single variable case, we lack an obvious way to distinguish between terms of a polynomial. For example, it is not apparent how we should define the degree of a polynomial. To do this, we must decide how to order our terms.

Definition 5.1. We say that $>$ is a **total ordering** on a set X if $>$ is transitive, antisymmetric, and total, i.e for any $a, b \in X$, one of $a > b, b > a$, or $a = b$ is true.

Definition 5.2. We say that $>$ is a **monomial ordering** on monic monomials in $k[x_1, \ldots, x_n]$ if (i) $>$ is a total ordering on $\mathbb{Z}^n$ (ii) if $a > b$ and $c \in \mathbb{Z}^n$, then $a + c > b + c$ and (iii) $>$ is well ordered on $\mathbb{Z}^n$.

Definition 5.3. If $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$, then $\alpha >_{\text{lex}} \beta$ if the leftmost nonzero entry of $\alpha - \beta$ is positive. We say $x^\alpha >_{\text{lex}} x^\beta$ if $\alpha >_{\text{lex}} \beta$. This is called **lexicographic ordering** or **lex** ordering.

The name derives from the fact this ordering is analogous to a dictionary ordering. In practice, we will often use lex ordering by specifying, for example, that $x > y > z$. However, any defined ordering is legitimate, and a simple counting

argument shows that for n variables, there are $n!$ possible lex orderings. For our computations, we use lex ordering with $X > Y > Z > W$.

We are familiar with some properties of polynomials in a single variable, such as degree or leading coefficient. Specifying a monomial ordering allows us to identify analogous aspects of a polynomial in multiple variables. These definitions will be necessary as we develop the different algorithms for our computational approach to algebraic geometry.

Definition 5.4. Let $f \in k[x_1, \ldots, x_n]$ be nonzero and let $>$ be a monomial order. Write $f = \sum_\alpha a_\alpha x^\alpha$. Then the **multidegree** of f is

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n \mid a_\alpha \neq 0)$$

with respect to $>$. The **leading coefficient** of f is $\text{LC}(f) = a_{\text{multideg}(f)} \in k$. The **leading monomial** of f is $\text{LM}(f) = x^{\text{multideg}(f)}$, monic by definition. The **leading term** of f is $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$.

Example 5.5. Let $f(x) = xyz + x^2y - 2z^2y^2 - 3x^3z + 5z^4 + 8yz \in \mathbb{C}[x, y, z]$ with lex order $x > y > z$. Then,

$$\text{multideg}(f) = (3, 0, 1)$$
$$\text{LC}(f) = -3$$
$$\text{LM}(f) = x^3z$$
$$\text{LT}(f) = -3x^3z$$

Proposition 5.6. *If $f, g \in k[x_1, \ldots, x_n]$ are nonzero, then*

$$\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g).$$

If $f + g \neq 0$, then

$$\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g)).$$

Proof. Suppose $\text{multideg}(f) = n$ and $\text{multideg}(g) = m$, with a_n and b_m the leading terms of f and g, respectively. Then fg has leading term $a_n b_m \neq 0$, as k is a field and $a_n, b_m \neq 0$, whose multidegree is $n + m$. Next, suppose $f + g \neq 0$. If $n \neq m$, then without loss of generality we may assume $n > m$. Then the leading term of $f+g$ is just the leading term of f, so that $\text{multideg}(f+g) = n$. Otherwise, if $n = m$, then the leading coefficient of $f + g$ is $a_n + b_m$. If $a_n + b_m \neq 0$, then the degree of $f+g$ is $n+m$. On the other hand, if $a_n+b_m = 0$, then the degree of $f+g$ is strictly less than $m = n$. Note that, since $f + g$ is nonzero by assumption, it follows that $\text{multideg}(f + g) \geq 1$. □

Theorem 5.7 (Division Algorithm)**.** *Given an ordering and a collection $(f_1, \ldots, f_s)$ of polynomials in $k[x_1, \ldots, x_n]$, then every $f \in k[x_1, \ldots, x_n]$ can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

with $a_i \in k[x_1, \ldots, x_n]$, where no term of r is divisible by $LT(f_i)$ for $1 \leq i \leq s$.

One major difference between this and the division algorithm in $k[x]$ is that the remainder is not unique. Instead it depends on the order of the polynomials $(f_1, \ldots, f_s)$. This problem indicates that regarding membership in ideals, a 0 remainder is a sufficient condition, but not a necessary one, as different orderings may give different remainders. We resolve this problem by first passing to the ideal generated by the polynomials $f_1, \ldots, f_s$. Then we consider a different generating set for this ideal, which behaves more like the division algorithm in a single variable,

where membership to an ideal occurs exactly when the remainder is 0. As we will see, such generating sets always exist.

5.2 Groebner Bases

Before we are able to resolve the uniqueness problem of our new division algorithm, we must define a simple type of ideal and explore some of its properties.

Definition 5.8. A **monomial ideal** is an ideal generated by single term, monic polynomials. That is, I is a monomial ideal if there is some set of n-tuples $A \subseteq \mathbb{N}^n$ such that $I = (x^a : a \in A)$.

Proposition 5.9. *If $I = (x^a \mid a \in A)$ is a monomial ideal, then $x^b \in I$ if and only if $x^a \mid x^b$ for some $a \in A$. Here, $x = (x_1, \ldots, x_n)$.*

Proof. If $x^a \mid x^b$ for some $a \in A$, then $x^b \in I$ by definition. Conversely, if $x^b \in I$, then $x^b = \sum_{i=1}^{s} f_i x^{a_i}$ with $f_i \in k[x_1, \ldots, x_n]$. Since x^b is monomial, it follows that the right hand side of the equation is also monomial. This happens just in case $\sum_{i=1}^{s} f_i x^{a_i}$ is divisible by x^{a_i} for some $a_i \in A$. □

The following lemma supplants the difficulty of proving Hilbert's Basis Theorem. We follow closely the proof of Theorem 5 from [2] Chapter 2, Section 4.

Lemma 5.10 (Dickson's Lemma)**.** *Monomial ideals are finitely generated by monomials.*

Proof. We proceed by induction on the number of variables in our polynomial ring. Let I be a monomial ideal. Then $I = (x^a \mid a \in A) \subseteq k[x_1, \ldots, x_n]$. When $n = 1$, $I = (x_1^a \mid a \in \mathbb{N})$ is generated by x_1^b where b is the smallest element in $A \subseteq \mathbb{N}$. In particular, I is finitely generated. Now suppose this holds for $n - 1$ variables and let I be a monomial ideal in $k[x_1, \ldots, x_{n-1}, y]$. Note that we emphasize y as the nth

variable in order to write monomials in $k[x_1, \ldots, x_{n-1}, y]$ as $x^a y^m$ with $a \in A \subseteq \mathbb{N}^{n-1}$ and $m \in M \subseteq \mathbb{N}$. We must find a finite generating set for I, so let $J = (x^a \mid x^a y^m \in I$ for some $m \in M) \subseteq k[x_1, \ldots, x_{n-1}$. (We think of J as the projection of I onto $n-1$ variables). This is a monomial ideal and so by the induction hypothesis, J is finitely generated, say $J = (x^{a_1}, \ldots, x^{a_s})$. For $1 \leq i \leq s$, $x^{a_i} y^{m_i} \in I$ for some $m_i \in M$. Let $m = \max(\{m_i\})$ and let $J_k = (x^b \mid x^b y^k \in I)$ for $0 \leq k \leq m-1$. We can think of J_k as the elements of I with each y exactly to the k-power. Again, by the induction hypothesis, J_k is finitely generated, say $J_k = (x^{a_k(1)}, \ldots, x^{a_k(s_k)})$. We claim that I is generated by the following: $x^{a_1} y^m, \ldots, x^{a_s} y^m \in J$ and $x^{a_k(1)} y^k, \ldots, x^{a_k(s_k)} y^k \in J_k$ for $0 \leq k \leq m-1$. By construction, the ideal generated by the aforementioned elements is contained in I. Conversely, suppose $x^a y^p \in I$. If $p \geq m$, $x^a y^p$ is divisible by $x^{a_i} y^m \in J$. Otherwise, it is divisible by $x^a y^p \in J_p$. Thus I is generated by the monomials from above, and we conclude that all monomial ideals are finitely generated. □

We are now prepared to prove Hilbert's Basis Theorem with relative ease, letting Dickson's Lemma carry most of the weight. There is no philosophical distinction between this proof and the proof from Section 2.1, as both rely on an ideal generated by leading coefficients and leading terms. Before we present the second proof, we give a name to these special ideals, which we will use throughout the remainder of this section. The proofs of these propositions are taken from the propositions and exercises in [2] Chapter 2.

Definition 5.11. If I is a nonzero ideal, then $\text{LT}(I)$ is the set of leading terms of elements of I and $(\text{LT}(I))$ is the **ideal of leading terms**. Note that if $I = (f_1, \ldots, f_s)$, then $(\text{LT}(f_1), \ldots, \text{LT}(f_s)) \subseteq (\text{LT}(I))$ as $\text{LT}(f_i) \subset \text{LT}(I)$ by definition, but equality need not occur.

Proposition 5.12. *The ideal of leading terms is a monomial ideal and there exist* $f_1, \ldots, f_s \in I$ *such that* $(\text{LT}(f_1), \ldots, \text{LT}(f_s)) = (\text{LT}(I))$.

Proof. Let I be an ideal. We claim that $(\text{LM}(f) \mid f \in I\backslash\{0\})$ and $(\text{LT}(I))$ are equal. This follows from the fact that for $f \in I\backslash\{0\}$, $\text{LM}(f)$ and $\text{LT}(f)$ differ by nonzero constants, where the absorption property of ideals ensures that these sets generate the same ideal. Since $(\text{LT}(f) \mid f \in I\backslash\{0\}) = (\text{LT}(I))$ and $(\text{LM}(f) \mid f \in I\backslash\{0\})$ is a monomial ideal, we have by transitivity that $(\text{LT}(I))$ is a monomial ideal. Consequently, by Dickson's Lemma, we know that $(\text{LT}(I)) = (\text{LM}(f_1), \ldots, \text{LM}(f_s))$ for some $f_1, \ldots, f_s$. Again, since $\text{LM}(f_i)$ and $\text{LT}(f_i)$ differ by nonzero constants, we have $(\text{LT}(f_1), \ldots, \text{LT}(f_s)) = (\text{LT}(I))$. □

Definition 5.13. Given a monomial ordering, we say that $\{g_1, \ldots, g_s\} \subseteq I$ is a **Groebner basis** for I if $(\text{LT}(g_1), \ldots, \text{LT}(g_s)) = (\text{LT}(I))$. From Proposition 5.12, we see that all nonzero ideals have Groebner bases.

Proposition 5.14. *G is a Groebner basis for an ideal I if and only if the leading term of every element of I is divisible by some leading term of an element of G.*

Proof. Let I be an ideal. Suppose $G = \{g_1, \ldots, g_s\}$ is a Groebner basis for I and let $f \in I$. We want to show that $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$ for some i. Since G is a Groebner basis, $\text{LT}(f) \in (\text{LT}(I)) = (\text{LT}(g_1), \ldots, \text{LT}(g_s))$. By Proposition 5.9, it follows that $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$ for some i. Conversely, suppose the leading term of every element of I is divisible by some leading term of an element of G. So let $f \in I$. We want to show that $\text{LT}(f) \in (\text{LT}(g_1), \ldots, \text{LT}(g_s))$, which would imply that $(\text{LT}(g_1), \ldots, \text{LT}(g_s)) \subseteq (\text{LT}(I))$, where the reverse equality always holds. But this follows again from Proposition 5.9, since $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$ for some i. Thus our claim holds. □

Theorem 5.15 (Hilbert's Basis Theorem)**.** *Every ideal in $k[x_1, \ldots, x_n]$ is finitely generated.*

Proof. If I is the zero ideal, then $\{0\}$ generates it. Now, if I is nonzero, then from Proposition 5.12, we know that a Groebner basis exists, say $g_1, \ldots, g_s \in I$. We will show that $I = (g_1, \ldots, g_s)$. First, $(g_1, \ldots, g_s) \subseteq I$ since each $g_i \in I$ by construction. Conversely, let $f \in I$. Fixing a monomial ordering, we divide f by $(g_1, \ldots, g_s)$ using the division algorithm to obtain $f = a_1 g_1 + \cdots + a_s g_s + r$, where no term of r is divisible by $\mathrm{LT}(f_i)$ for $1 \leq i \leq s$. We will show that $r = 0$. Since $r = f - a_1 g_1 - \cdots - a_s g_s \in I$ we have that $\textsc{lt}(r) \in (\textsc{lt}(I)) = (\textsc{lt}(g_1), \ldots, \textsc{lt}(g_s))$, hence $\textsc{lt}(g_i) \mid \textsc{lt}(r)$ for some g_i. This is only possible if $r = 0$. Thus $f \in (g_1, \ldots, g_s)$ and $I \subseteq (g_1, \ldots, g_s)$. □

The use of Groebner bases in the proof of Hilbert's Basis Theorem is a common approach. Note that our proof holds for an arbitrary monomial ordering. Such generality holds for all Groebner bases, an important property that we demonstrate here.

Proposition 5.16. *Polynomials divided by a Groebner basis for an ideal I have unique remainders irrespective of the ordering of elements in the basis.*

Proof. Suppose that $f = g + r = g' + r'$ satisfy the criteria of the division algorithm. So $r - r' = g - g' \in I$. If $r \neq r'$, then $\textsc{lt}(r - r') \in (\textsc{lt}(I)) = (\textsc{lt}(g_1), \ldots, \textsc{lt}(g_s))$. But then $\textsc{lt}(r - r')$ is divisible by some $\textsc{lt}(g_i)$, contradicting the definition of a remainder. Hence $r - r' = 0$ and remainders are unique. □

Corollary 5.16.1. *Groebner bases for polynomials in many variables have the ideal membership property. That is, a polynomial f belongs to an ideal I if and only if the remainder on division of f by a Groebner basis of I is* 0.

This ideal membership property provides a necessary and sufficient criteria for being a Groebner bases. This inspires an important algorithm, Buchberger's Algorithm, which is akin to the Euclidean Algorithm. Much of computational algebraic geometry relies upon Buchberger's algorithm. First, we state some definitions.

Definition 5.17. Let f and g be nonzero polynomials in $k[x_1, \ldots, x_n]$ with multidegree α and β, respectively. Set $\gamma = (\gamma_1, \ldots, \gamma_n)$ where $\gamma_i = \max(\alpha_i, \beta_i)$. The monomial x^γ is the **least common multiple** of $\text{LM}(f)$ and $\text{LM}(g)$.

Definition 5.18. The **S-polynomial** of f and g is $S(f,g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g$.

The next theorem shows that Definition 5.18 gives a necessary and sufficient condition for a set of polynomials to be a Groebner basis. A proof of this can be found in [2] Chapter 2, Section 6, Theorem 6.

Theorem 5.19 (Buchberger's Criterion)**.** *Let I be an ideal. Then $G = (g_1, \ldots, g_t)$ is a Groebner basis for I if and only if the remainder of $S(g_i, g_j)$ by G is zero for every pair $i \neq j$.*

Theorem 5.20 (Buchberger's Algorithm)**.** *A Groebner basis can be constructed for any ideal I in a finite number of steps using Buchberger's Criterion.*

A complete proof of Buchberger's algorithm can be found in [2] Chapter 2, Section 7, Theorem 2. Essentially, the algorithm runs as follows: Given a polynomial ideal I, we know by Hilbert's Basis Theorem that $I = (f_1, \ldots, f_s)$. Using Buchberger's Criterion, we can determine if this set is a Groebner basis for I. If it is, we are done; otherwise, compute $\text{S}_{i,j}$, the S-polynomial for every pair of distinct polynomials (f_i, f_j). For $\text{S}_{i,j} \neq 0$, add $\text{S}_{i,j}$ to our generating set. We repeat this process until our new set, which is our original generating set with some additional polynomials, is a Groebner basis because, by construction, it satisfies Buchberger's Criterion. That this algorithm terminates is a consequence of the ascending chain

condition for the ideal of leading terms of our set. Along the way, it is clear that our set remains a generating set since $\{f_1, \ldots, f_s\}$ is always contained in our set.

Buchberger's algorithm is also useful for producing Groebner bases with additional properties. In fact, while Groebner bases are not unique in general, we have the tools to produce a special, unique Groebner basis for any ideal.

Definition 5.21. A **minimal Groebner basis** is a Groebner basis where each polynomial is monic and, with respect to the ordering, no leading term is divisible by any of the other leading terms.

Remark 5.22. We do not know *a priori* that minimal Groebner bases exist. However, we will show that this is true in Proposition 5.26.

Proposition 5.23. *If G and H are both minimal Groebner bases for an ideal I, then $\text{LT}(G) = \text{LT}(H)$.*

Proof. Let $G = \{g_1, \ldots, g_s\}$ and $H = \{h_1, \ldots, h_t\}$ be minimal Groebner bases for I. Suppose $s \leq t$. Since $g_1 \in G \subseteq I$, and H is a Groebner basis for I, we know that, for some i, $\text{LT}(h_i)$ divides $\text{LT}(g_1)$. Without loss of generality we may assume that $i = 1$. On the other hand, we know that there is some g_j whose leading term divides the leading term of h_1. We claim that $j = 1$. Suppose not. Then there is some g_j such that $\text{LT}(g_j) \mid \text{LT}(h_1)$, but $\text{LT}(h_1) \mid \text{LT}(g_1)$, which implies that $\text{LT}(g_j) \mid \text{LT}(g_1)$, contradicting the minimality of G. Thus $j = 1$ and $\text{LT}(g_1) = \text{LT}(h_1)$. We can show similarly that $\text{LT}(g_2) = \text{LT}(h_2)$. Continuing this process, we see that $\text{LT}(g_s) = \text{LT}(h_s)$. In particular, this implies that $s = t$, since every leading term of H is divisible by exactly 1 leading term of G. Thus the ideal of leading terms is equal, as desired. □

Definition 5.24. A **reduced Groebner basis** is a Groebner basis where each polynomial is monic and for any polynomial in the basis, no monomial is divisible

by any leading terms.

Remark 5.25. If G is a reduced Groebner basis for an ideal I, then G is necessarily a minimal Groebner basis.

Next we show that ideals have reduced Groebner bases, and thus minimal Groebner bases. Moreover, we show that these reduced Groebner bases are unique.

Proposition 5.26. *Nonzero ideals have a unique reduced Groebner basis.*

Proof. That a reduced Groebner basis exists is a consequence of Buchberger's Algorithm. Let I be an ideal. Obtain a Groebner basis for I, call it G, through Buchberger's Algorithm. Suppose $f \in G$ satisfies $\text{LT}(f) \in (\text{LT}(G \backslash \{f\}))$, the ideal of leading terms of all other polynomials of G. It follows that $(\text{LT}(G - \{f\})) = (\text{LT}(G))$. One containment is obvious, and the other follows from the fact that $\text{LT}(f) \in (\text{LT}(G \backslash \{f\}))$ by assumption. So, by definition, $G - \{f\}$ is also a Groebner basis. We may repeat this process until we have a minimal Groebner basis, say G', since each step we remove elements from G whose leading terms are divisible by other elements from G. Now, we may use the division algorithm for multivariate polynomials to reduce polynomials in G', in the sense of Proposition 5.25, as follows. Simply divide the polynomial in question by all other polynomials in the basis and replace the original polynomial with the remainder. This ensures that no monomial is divisible by any leading term of another polynomial. To show uniqueness, suppose G and H are both reduced Groebner bases for a polynomial I. Then G and H are also minimal Groebner bases, so that $\text{LT}(G) = \text{LT}(H)$ by Proposition 5.23. So let $G = (g_1, \ldots, g_s)$ and $H = (h_1, \ldots, h_s)$. Arrange them such that $\text{LT}(g_i) = \text{LT}(h_i)$ for each i. We are done if we can show, for an arbitrary i, that $g_i = h_i$. Consider $g_i - h_i$. Since g_i and h_i are in I, their difference is. Thus $\text{LT}(g_i - h_i)$ is divisible by $\text{LT}(g_j) = \text{LT}(h_j)$ for some j. Since G and H are reduced Groebner bases, we know

that $\text{LT}(g_j) = \text{LT}(h_j)$ does not divide $\text{LT}(g_i - h_i)$ for $j \neq i$. However, for $j = i$, we see that $g_i - h_i$ has degree strictly less than $g_i = h_i$ since their leading terms are equal, hence $\text{LT}(g_i - h_i)$ cannot be divisible by $\text{LT}(g_i) = \text{LT}(h_i)$. This forces $g_i - h_i = 0$, hence $g_i = h_i$, and $G = H$. We conclude that reduced Groebner bases are unique. $\square$

6 Miscellaneous Topics

Before we begin with the project proper, we must make explicit some of the notions we have referenced throughout. These include the ideas of dimension and singularity.

6.1 Dimension

In order to define dimension, we first introduce the concept of a chain of varieties. Such chains are commonplace throughout mathematics. Here, a chain enables us to define the dimension of a variety.

Definition 6.1. Let V be an irreducible affine variety. A **chain** of length d in V is a collection $V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_d = V$ where V_i is an irreducible subvariety of V_{i+1}.

Definition 6.2. Let V be an irreducible, affine variety. The **dimension** of V, $\dim V$, is the supremum of the lengths of all chains of V. If V is reducible, then the **dimension** of V at a point p, $\dim_p V$, is the supremum of the dimensions of the irreducible components of V containing p.

Although this definition is straightforward, the computation of dimension is not trivial from this definition. Instead, we can use the ideal-variety correspondence to view dimension algebraically. This allows us to more easily compute dimension.

Definition 6.3. Let I be an ideal. Then the **Krull dimension** of I is the supremum of the lengths of all chains of prime ideals of I.

Definition 6.4. Let $F \subseteq K$ be fields. Then the **transcendence degree** of K over F, written tr deg K/F, is the number of algebraically independent elements of K over F.

Proposition 6.5. *Let V be an irreducible affine variety. Then*

$$\dim V = \text{Krull}\dim \boldsymbol{I}(V) = \text{tr deg } k(V)/k.$$

Proof. Suppose $\dim V = d$. By definition, there exists a chain $V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_d = V$ where V_i is a subvariety of V_{i+1}. Using the ideal-variety correspondence, we obtain the following chain of ideals:

$$\mathbf{I}(V) = \mathbf{I}(V_d) \subsetneq \mathbf{I}(V_{d-1}) \subsetneq \cdots \subsetneq \mathbf{I}(V_0).$$

Note that the inclusion is reversed. Furthermore, since V is irreducible, we know that $\mathbf{I}(V)$ is prime and we have a prime chain. It is clear that the Krull dimension of $\mathbf{I}(V)$ is d, since we could pass any longer prime chain to the corresponding chain of varieties, which would have length greater than d, contradicting the dimension of V. The equivalence of $\text{Krull}\dim \mathbf{I}(V)$ and tr deg $k(V)/k$ is a nontrivial problem, whose proof relies on the use of Hilbert polynomials. A discussion of this fact can be found in [4] Section 6, and a more complete proof can be found in [1] Chapter 11. □

6.2 Singularities

In this section, we define singularities on varieties. Often it is easier to find rational points on a singular variety and we will use this in our search for rational points on our surface. We present several proofs specific to hypersurfaces and more specifically to cubic surfaces.

Definition 6.6. The **tangent space** of V at a point $p = (a_1, \ldots, a_n)$ is the variety

$$T_p(V) = \mathbf{V}(d_p(f) \mid f \in \mathbf{I}(V)),$$

where

$$d_p(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_1}(p)(x_i - a_i).$$

Remark 6.7. From [4] Section 6.6, we may define $r = \min_{p \in V} \dim T_p(V)$ to be the dimension of V.

Definition 6.8. If p is a point on the variety V, then p is **nonsingular** provided $\dim T_p(V) = \dim_p(V)$, otherwise p is **singular**.

Definition 6.9. A variety is **nonsingular** if it is nonsingular at every point $p \in V$, otherwise V is **singular**.

The following results we collect and justify from comments throughout [4] Chapter 6.

Proposition 6.10. *If $V \subseteq \mathbb{A}^n(k)$ is a hypersurface for a nonconstant polynomial f, then dim $V = n - 1$.*

Proof. We can write the coordinate ring $k[V]$ as $k[x_1, \ldots, x_n]/(f)$ by Proposition 4.6. Without loss of generality, we may assume that x_1 occurs nontrivially in f since f is nonconstant. Thus $k(V) \cong k(x_2, \ldots, x_n)[x_1]/(f)$, i.e $k(V)$ is constructed by adjoining $n - 1$ algebraically independent elements. Thus dim $V = n - 1$. □

There is a quick and easy method to checking whether or not a variety is singular, which we justify in the following proposition.

Definition 6.11. If f is a polynomial in n variables, then the **Jacobian matrix** of f is

$$\begin{pmatrix} \frac{\partial f}{\partial x_1} & \cdots & \frac{\partial f}{\partial x_n} \end{pmatrix}$$

where $\frac{\partial f}{\partial x_i}$ is the partial derivative of f with respect to x_i.

Proposition 6.12. *A hypersurface $V \subseteq \mathbb{A}^n$ is singular at p if and only if the rank of its Jacobian drops at p.*

Proof. Let $V = \mathbf{V}(f)$. From linear algebra, we know that

$$\dim T_p(V) = n - \text{rank } \nabla f(p),$$

where $\nabla f(p)$ is the Jacobian of f at a point p. Note that at a nonsingular point, the rank also satisfies $\dim V = n - \text{rank } \nabla f(p)$. So if for all $p, \nabla f(p) \neq 0$, then the rank of $\nabla f(p) = 1$, and $\dim T_p(S) = n - 1 = \dim V$, hence the rank remained as expected for the Jacobian of a hypersurface at a nonsingular point. Thus $V(f)$ is nonsingular. On the other hand, if for some $p, \nabla f(p) = 0$, then the rank drops, as $\nabla f(p) = 0$, and $\dim T_p(V) = n \neq \dim V$, hence V is singular at p. □

Remark 6.13. We may generalize the previous proposition to show that any variety is singular if and only if the rank of its Jacobian drops.

We end this section (and begin the next) with a proposition regarding the intersection of a surface with a plane.

Proposition 6.14. *Let $V \subseteq \mathbb{A}^n$ be a hypersurface and $p \in V$. Then $V \cap T_pV$ is singular at p.*

Proof. Let $V = \mathbf{V}(f)$. Suppose V is singular at p. Then, by the previous proposition, $\frac{\partial f}{x_i}(p) = 0$ for all i. Then

$$T_p(V) = \mathbf{V}(\sum_{i=1}^{n} \frac{\partial f}{\partial x_1}(p)(x_i - a_i)) = \mathbf{V}(0) = \mathbb{A}^n(k).$$

Thus $V \cap T_p(V) = V \cap \mathbb{A}^n(k) = V$. Since V is singular at p by assumption, it follows that $V \cap T_p(V)$ is singular at p.

Now suppose that V is nonsingular at p. By Proposition 6.12, it suffices to consider the Jacobian. A generic plane is defined by a linear polynomial $g = \sum_{i=1}^{n} a_i x_i$. Then the Jacobian of V and $\mathbf{V}(g)$ is

$$\nabla \begin{pmatrix} \frac{\partial f}{\partial x_1}(p) & \cdots & \frac{\partial f}{\partial x_n}(p) \\ a_1 & \cdots & a_n \end{pmatrix}$$

But the tangent plane is defined exactly so that $a_i = \frac{\partial f}{\partial x_i}(p)$. Thus the rank of the Jacobian of $V \cap T_p(V)$ drops at p, as claimed. □

6.3 Cubic Surfaces

We collect several results about cubic surfaces that are fundamental to our project. Note that here, as in our project, we work over projective space. Our first proposition follows [4] Section 7.1.

Proposition 6.15. *Every plane intersects a nonsingular cubic surface as an irreducible cubic, a conic plus a line, or three distinct lines.*

Proof. Let S be a nonsingular cubic surface defined by a homogeneous cubic polynomial $f(X, Y, Z, W)$ and let H be a plane. Without loss of generality, we may assume H is the plane $W = 0$. We know that the intersection of S and H is a cubic curve. Thus $S \cap H$ must either be irreducible, a qudratic and a linear component, or three linear components. Note that a quadratic component is a conic and a linear component is a line. We must rule out the possibility that $S \cap H$ has a multiple linear component, i.e there is not a multiple line. So suppose l were a multiple line on $S \cap H$. Through some change of coordinates, we may assume l is the line $Z = 0$.

Then substituting l back into f, we see that f has the form

$$Z^2 \cdot g(X, Y, Z, W) + W \cdot h(X, Y, Z, W)$$

with g a linear polynomial and h a quadratic as f is homogeneous. We know f has this form since f vanishes at $Z = 0$ and $W = 0$, and its derivative also vanishes at $Z = 0$, as a multiple line. However, this implies that S is singular at the point $Z = W = p = 0$, where p is a root of h. Such a p exists since we are working over an algebraically closed field. This contradicts the nonsingularity of S, hence no such multiple line exists. □

It will be useful to identify when an arbitrary conic

$$f = AX^2 + BXY + CY^2 + DX + EY + F$$

where $A, B, C, D, E, F \in \mathbb{C}[Z, W]$ is nonsingular. Note that by degree considerations, a conic is singular just in case it is degenerate.

Proposition 6.16. *The conic f is singular if and only if $\Delta(Z, W) = 4ACF + BDE - AE^2 - B^2F - CD^2 = 0$.*

Proof. We know that f is singular just in case there is some point $p = (x_0, y_0)$ such that $f(p) = \nabla(2Ax_0 + By_0 + D, Bx_0 + 2Cy_0 + E) = 0$. Since $2AX + BY + D$ and $BX + 2CY + E$ are two linear equations in two variables, we know there is at most one solution for (x_0, y_0). Furthermore, since f is a conic, we know that at least one of A, B, or C is nonzero. First suppose that each is nonzero. Then we obtain the solution

$$x_0 = \frac{2CD - BE}{B^2 - 4AC} \qquad y_0 = -\frac{BD - 2AE}{B^2 - 4AC}.$$

Note that since none of A, B, C are zero, $B^2 - 4AC$ is nonzero. Substituting these values into $f(p)$ gives

$$\frac{(2\,CD-BE)^2\,A}{(B^2-4\,AC)^2} - \frac{(BD-2\,AE)(2\,CD-BE)\,B}{(B^2-4\,AC)^2} + \frac{(BD-2\,AE)^2\,C}{(B^2-4\,AC)^2} + \frac{(2\,CD-BE)\,D}{B^2-4\,AC} - \frac{(BD-2\,AE)\,E}{B^2-4\,AC} + F.$$

Now f vanishes just in case the numerator vanishes. Clearing denominators, we obtain

$$\begin{aligned} f(p) =& B^2CD^2 - 4\,AC^2D^2 - B^3DE + 4\,ABCDE + AB^2E^2 - 4\,A^2CE^2 \\ &+ B^4F - 8\,AB^2CF + 16\,A^2C^2F \\ =& 4AC(4ACF + BDE - AE^2 - B^2F - CD^2) \\ &- B^2(4ACF + BDE - AE^2 - B^2F - CD^2) \\ =& (4AC - B^2)\Delta = -1(B^2 - 4AC)\Delta. \end{aligned}$$

Again, since $4AC - B^2 \neq 0$, this vanishes just in case Δ vanishes, which is what we claimed. Note that in our solution, we needed the denominator $B^2 - 4AC$ to not vanish anywhere. This held for our previous case since none of A, B, C were zero. Now we must consider the other cases. When B and C are nonzero with $A = 0$, we find that

$$x_0 = \frac{2CD - BE}{B^2} \qquad y_0 = -\frac{D}{B}.$$

Substituting these values into f gives

$$\frac{CD^2}{B^2} - \frac{DE}{B} + F.$$

Clearing denominators we obtain (as $A = 0$)

$$f = CD^2 - BDE + B^2F = (-1)(BDE - B^2F - CD^2) = (-1)\Delta.$$

Again, f vanishes exactly when Δ vanishes. For $B = 0$ and $C = 0$, we get the solutions

$$x_0 = -\frac{D}{2A} \qquad y_0 = -\frac{E}{2C}$$

and

$$x_0 = -\frac{E}{B} \qquad y_0 = -\frac{BD - 2AE}{B^2},$$

respectively. Substituting these into f and clearing denominators gives us (with $B = C = 0$)

$$f = -\frac{1}{4}CD^2 - \frac{1}{4}AE^2 + ACF = \frac{1}{4}\Delta$$

and

$$f = -BDE + AE^2 + B^2F = (-1)\Delta,$$

respectively. When $A = C = 0$, we have

$$x_0 = -\frac{E}{B} \qquad y_0 = -\frac{D}{B}$$

and

$$f = -DE + BF = -\frac{1}{B}\Delta.$$

Note that since $A = C = 0$, B is nonzero so $\frac{1}{B}$ is defined.

Finally, suppose $A = B = 0$. Then $\Delta = -CD^2$. Since $C \neq 0$, as A, B, C cannot all be zero, Δ vanishes just in case $D = 0$. Also, since $A = B = 0, f = CY^2 + DX + EY + F$, so that $f_X = D$. In particular, if $D \neq 0$, then f is not

singular. On the other hand, if $D = 0$, then $f = CY^2 + EY + F$, which splits completely over $\mathbb{C}$, so that f is indeed singular. Thus f is singular just in case $D = 0$, which happens just in case Δ vanishes, and our claim holds. Note that $B = C = 0$ has a parallel argument as here. $\square$

We record a well-known fact about cubic surfaces. We borrow techniques used in the proof, which can be found in full in [4] Chapter 7, during our search for a two parameter family of points on S.

Theorem 6.17 (27 lines)**.** *There exist exactly 27 lines on a cubic surface.*

The major challenge to this proof is showing that even a single line lies on a cubic surface. This fact uses Proposition 6.15 as well as the fact that at most 3 lines of a cubic surface contain a given point. Let V be a cubic surface. There are then several arguments that demonstrate that a line lies on V, some involving dimension-counts and others using Hessian matrices and resultants. Once it is established that a single line l lies on V, it is not too difficult to show that there are exactly 5 pairs of lines on V that intersect l. The tools involved to prove this fact enable us to compute the lines on S during our parametrization. A corollary to this fact is that there exists disjoint lines on V. The remainder of the proof considers the configuration of the lines and essentially uses a counting argument to determine that there are exactly 27 lines on V.

7 Parametrizing the Surface

7.1 Motivation

Consider the equation for the unit circle:

$$X^2 + Y^2 = 1.$$

We can find all of the rational solutions to this equation using some geometry. First, we must identify one rational point on the unit circle, say $(1, 0)$. It is evident that this point lies on our curve from both the algebraic expression (simply plug in the point) and its subsequent geometric representation (consider its graph). Next, we choose an equation for a line through the point $(1, 0)$ of slope t

$$Y = tX - t.$$

Substituting this line in for the equation of the unit circle, we obtain

$$\begin{aligned} X^2 + (tX - t)^2 &= 1 \\ X^2 + t^2X^2 - 2t^2X + t^2 &= 1 \\ (t^2 + 1)X^2 - 2t^2X + t^2 - 1 &= 0. \end{aligned}$$

We expect this equation to intersect the unit circle at most two times, based on the degree of the equation, i.e the final equation treated as a quadratic of the variable X should factor as two linear components. Note that a single point of intersection occurs exactly when our line is vertical, corresponding to the line tangent to the initial point $(1, 0)$. For all other lines, our equation intersects the circle at exactly two distinct points, one of which is $(1, 0)$ by construction. That is, $X = 1$ is one root of the equation $(t^2 + 1)X^2 - 2t^2X + t^2 - 1 = 0$, hence $(X - 1)$ is a linear factor

of this equation. Using polynomial long division, we find that the other linear factor is

$$(t^2+1)X - t^2 + 1.$$

Thus the other root is

$$X = \frac{t^2-1}{t^2+1}.$$

Solving for Y using our equation for a line above, we have that

$$P = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$$

is a rational parametrization for the unit circle. To see this, we must demonstrate that when t is rational, P is rational and conversely that any rational point on the unit circle has a corresponding t. The first claim is clear. On the other hand, if $(p,q) \in \mathbb{Q}^2$ is some point on the unit circle other than $(1,0)$, then we may compute the slope through (p,q) and $(1,0)$ using the equation for a line to obtain

$$t = \frac{q}{p-1},$$

and indeed $P = (p,q)$ for this value of t. Since every $(p,q) \neq (1,0)$ has a corresponding t value, our parametrization is a complete solution. Hereinafter, we refer to this method of parametrization as the "sweeping strategy."

What allowed us to sweep through the rational points on the unit circle? For one, we had a rational point to begin with, $(1,0)$. If we attempt to repeat this process for higher degree polynomials, we find success for some equations, like $Y^2 = X(X-1)^2$ and $Y^2 = X^2(X+1)$, but not for others. For example, even though $(0,1)$ satisfies the equation $Y^2 = X^3 - X + 1$, we cannot simply spin a line of slope t through this point to obtain a parametrization. Likewise for the equations $Y^2 = X^3 - X^2 - X$

and $Y^2 = X^3 - X$. What, then, is the difference? It turns out that the former curves all have singular points, whereas the latter curves are nonsingular and have no such singularity.

The explanation for why the sweeping strategy works for singular cubic curves is as follows: We expect 3 points of intersection between a line and a cubic curve, but a singularity counts (at least) two points of intersection. Therefore three points of intersection, at least two of which occur at a rational singulatity, imply that the sweeping strategy will work. This is the reason that we must find a singular cubic curve on S, which we accomplish by first finding lines on S.

7.2 Finding Lines on the Surface

Let

$$f = X^3 + Y^3 + YZ^2 + W^3 \in \mathbb{Q}[X, Y, Z, W]$$

and let

$$S = \mathbf{V}(f) \subseteq \mathbb{P}^3(\mathbb{C}).$$

Our aim is to find all of the rational points on the hypersurface S. By Proposition 6.12, we can check if S is singular by checking to see if the rank of its Jacobian drops at any point. Recall that we calculate this by seeing if the partial derivatives of each variable in S simultaneously vanish at any points on S. Here, we check directly that S is non-singular:

$$\nabla f = \begin{pmatrix} 3X^2 & 3Y^2 + Z^2 & 2YZ & 3W^2 \end{pmatrix}$$

It is clear that in order for ∇f to vanish, $X = W = 0$, and $Y = 0$ or $Z = 0$. When $Y = 0$, it forces $Z = 0$. Likewise, if $Z = 0$, then $Y = 0$. Thus $X = Y = Z = W = 0$ is the only possible solution and, as we said earlier, $(0 : 0 : 0 : 0) \notin \mathbb{P}^3$. It follows

that S is nonsingular.

In order to employ the sweeping strategy, we need a singular curve. We can find a plane in $\mathbb{P}^3$ whose intersection with S is necessarily singular. Recall that a hyperplane in $\mathbb{P}^3$ is defined by a polynomial of the form

$$aX + bY + cZ + dW = 0.$$

First, we dehomogenize S with respect to $W = 1$, say $S_{W=1} \subseteq \mathbb{A}^3$. (We do so for convenience, as computations are often easier in affine space.) Then $S_{W=1} = \mathbf{V}(f_0)$, where

$$f_0(x, y, z) = f(x : y : z : 1).$$

We then intersect $S_{W=1}$ with the plane

$$H_{a,b} = \mathbf{V}(g) \subseteq \mathbb{A}^3,$$

where $g_{a,b} = ax + by$. Let

$$C_{a,b} = S_{W=1} \cap H_{a,b}.$$

Thus

$$C_{a,b} = \mathbf{V}(f_0, g).$$

The subsequent Jacobian for $C_{a,b}$ is as follows:

$$\begin{pmatrix} 3x^2 & 3y^2 + z^2 & 2yz \\ a & b & 0 \end{pmatrix}$$

We will find values for a and b that forces a singularity on $C_{a,b}$. Setting $y = 0$, we see that $x = \frac{\sqrt{3a}}{3}$ and $z = \pm\sqrt{b}$. Let $b = d^2$. Then our desired condition for a

singular point on $C_{a,b}$ becomes

$$x^3 + 1 = 0$$
$$\frac{a\sqrt{3a}}{9} + 1 = 0.$$

Letting $a = 3c^2$, we find that $c = -1$. Hence the rank of the Jacobian drops at the point

$$P_d = (x, y, z) = (c, 0, \pm\sqrt{b}) = (-1, 0, \pm d),$$

and thus a singularity occurs on $C_{a,b}$ at P_d by Proposition 6.12. We want to consider the plane containing P_d. At first, we may believe that the polynomial $3x + d^2y = 0$ will define this plane. However, we observe that this plane does not contain the point $(-1, 0, d)$. Instead, translate to

$$g = 3x + d^2y + 3,$$

which does contain P_d. Thus our desired plane is

$$H = \mathbf{V}(g) \subseteq \mathbb{A}^3.$$

By Proposition 6.15,

$$C_{a,b} = S_{W=1} \cap H \subseteq \mathbb{A}^3$$

is either a nondegenerate cubic curve, a conic and a line, or three distinct lines. Ultimately, we want a nondegenerate cubic curve so that the sweeping strategy will yield points with new tangent planes. In particular, we are looking for a rational point not contained on any of the 27 lines so that $C_{a,b}$ is a nondegenerate, singular cubic curve.

This singularity will allow us to first sweep through rational points on S whose tangent plane intersects with S at a nondegenerate, singular cubic curve, and then sweep through each of these curves to obtain a dense set of rational points on our surface. If we attempted the sweeping strategy with a curve produced by the intersection of S and the tangent plane to a point lying on one of the 27 lines, then our two parameter solution would only produce points on a single plane. This is because the first time we employ the sweeping strategy, we will only obtain a family of nondegenerate, singular cubic curves contained on the same tangent plane. Thus we must be sure that we have a curve that fits these requirements before we can attempt a parametrization.

In any case, $C_{a,b}$ is singular and contains a family of singular points at

$$P_d = (-1, 0, d).$$

We claim that $C_{a,b}$ is a conic plus a line. To see this, we calculate $C_{a,b}$ explicitly:

$$\begin{aligned} C_{a,b} &= (-1 - \frac{d^2 y}{3})^3 + y^3 + yz^2 + 1 \\ &= \frac{1}{27} \cdot y \cdot (-d^6 y^2 - 9d^4 y - 27d^2 + 27y^2 + 27z^2) \end{aligned}$$

It becomes apparent that $y = 0$ is a degenerate component of $C_{a,b}$. Since $x = -1 - \frac{d^2 y}{3}$, we see that $x = -1$ when $y = 0$. Thus $\mathbf{V}(x + 1, y)$ is a line on $C_{a,b}$. Note that the second component of $C_{a,b}$,

$$-d^6 y^2 - 9d^4 y - 27d^2 + 27y^2 + 27z^2$$

is nonsingular (by Proposition 6.16, it suffices to check that $\Delta \neq 0$) and hence nondegenerate.

Since $C_{a,b}$ is a curve on the subvariety of S with $W = 1$, it follows that S contains

the line $\mathbf{V}(X+W,Y)$. As we mentioned in Section 6.3, there are exactly 27 lines on a cubic, and we have just found one. Recall that the existence of even a single line on a cubic surface was the most challenging part of the proof of Theorem 6.17. From this line, all other 26 can be generated. Here, we demonstrate how to compute these other lines. The subsequent SAGE code can be found in the appendix.

Let L be the line

$$\mathbf{V}(X+W,Y).$$

We change coordinates so that L is

$$\mathbf{V}(X,Y).$$

We now expand the polynomial f' defining our surface, or more accurately a copy of our surface, say S', as

$$f' = AZ^2 + BZW + CW^2 + DZ + EW + F,$$

a variable conic in W and Z, where $A, B, C, D, E, F \in \mathbb{Q}[X,Y]$. Moreover, A, B, and C are linear, D and E are quadratic, and F is cubic because f' is a homogeneous cubic. By Proposition 6.16, this new equation in Z and W is singular if and only if

$$\Delta(X,Y) = 4ACF + BDE - AE^2 - B^2F - CD^2 = 0.$$

Here, Δ is a scalar multiple of the determinant of our conic. This follows from the

matrix form of a general conic:

$$\begin{pmatrix} A & B/2 & D/2 \\ B/2 & C & E/2 \\ D/2 & E/2 & F \end{pmatrix}$$

The solutions to $\Delta = 0$ will reveal when our curve degenerates as three distinct lines as opposed to a line and a degenerate conic, like with $C_{a,b}$.

To find the other lines on S, we must first transform our L to $\mathbf{V}(X, Y)$. Consider the basis

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} v_2 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} v_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} v_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

of $\mathbb{A}^4$. Observe that these satisfy $v_1, v_2, v_4 \in \mathbf{V}(X+W)$ and $v_1, v_2, v_3 \in \mathbf{V}(Y)$. Since automorphisms of $\mathbb{P}^3$ are induced by invertible linear transformations of $\mathbb{A}^4$, we need an appropriate linear transformation, $\varphi : \mathbb{A}^4 \to \mathbb{A}^4$. We need to choose $\varphi(v_i)$ such that v_i satisfies $X = 0$ and $Y = 0$. So define φ as follows:

$$\varphi(v_1) = v_1, \varphi(v_2) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \varphi(v_3) = v_3, \varphi(v_4) = v_4.$$

Here we have changed our basis to the standard basis for convenience. We can then

obtain $\varphi(v_2)$ as $v_2 + v_3$. Thus $\varphi(v_2) + \varphi(v_3) =$

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

We are left with the following transformation which induced an isomorphism $S \to S'$.

$$\begin{pmatrix} X' \\ Y' \\ Z' \\ W' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}$$

Explicitly,

$$X' = X + W$$

$$Y' = Y$$

$$Z' = Z$$

$$W' = W.$$

Likewise, the inverse is

$$X = X' - W'$$

$$Y = Y'$$

$$Z = Z'$$

$$W = W'.$$

To compute $\varphi(S)$, we simply substitute the aforementioned values into f. Thus

$$f' = X'^3 - 3W'X'^2 + 3W'^2X' + Y'^3 + Y'Z'^2.$$

The surface $S' = \mathbf{V}(f')$ is isomorphic to S and contains the shifted line $\mathbf{V}(X', Y')$. We will be able to go back and forth between S and S' by using this isomorphism. Now we are able to calculate the determinant Δ, which will be a homogeneous quintic. Over $\mathbb{C}$, we split Δ into its five linear components in order to compute lines on our surface. So, considered as a variable conic in W and Z, we see that f' has

$$A = Y'$$

$$B = 0$$

$$C = 3X'$$

$$D = 0$$

$$E = -3X'^2$$

$$F = X'^3 + Y'^3$$

Thus

$$\Delta = 12X'Y'^4 + 3X'^4Y' = 3 \cdot X' \cdot Y' \cdot (4Y'^3 + X'^3).$$

Since a singularity occurs if and only if $\Delta = 0$ by Proposition 6.16, we first observe that, indeed, $X' = 0$ and $Y' = 0$ satisfy this requirement. This corresponds to the fact that S' contains the line $\mathbf{V}(X', Y')$. We can factor the remaining solutions as

$$4Y'^3 + X'^3 = (\alpha Y' + X')(\alpha\zeta_3 Y' + X')(\alpha\zeta_3^2 Y' + X'),$$

where $\alpha^3 = 4$ and ζ_3 is a primitive cube root of unity. These correspond with the

other 3 solutions

$$X' = -\alpha Y'$$

$$X' = -\alpha\zeta_3 Y'$$

$$X' = -\alpha\zeta_3^2 Y'.$$

Each of these 5 solutions, including $X' = 0$ and $Y' = 0$, yields 3 lines on S'. For example, when $X' = 0$,

$$f' \restriction_{X'=0} = Y'^3 + Y'Z'^2 = Y'(Y'^2 + Z'^2) = Y'(Y' - iZ')(Y' + iZ').$$

Thus we obtain the original line

$$\mathbf{V}(X', Y')$$

as well as the lines

$$\mathbf{V}(X', Y' - iZ') \qquad \mathbf{V}(X', Y' + iZ').$$

To complete our process, we use our isomorphism to find the analogous lines on S. These 3 lines are

$$\mathbf{V}(X + W, Y) \qquad \mathbf{V}(X + W, Y - iZ) \qquad \mathbf{V}(X + W, Y + iZ).$$

We can repeat this process with the other 4 roots of Δ, namely

$$Y' = 0$$
$$X' = -\alpha Y'$$
$$X' = -\alpha\zeta_3 Y'$$
$$X' = -\alpha\zeta_3^2 Y'.$$

From this Δ we will have 10 new lines (2 new lines from each root) plus our original line, for a total of 11 lines on the surface. We can repeat this process moving any one of these new lines to the line $\mathbf{V}(X'', Y'')$ on a new surface, S''. Considered as another variable conic, we then obtain its determinant, say Δ', in order to find more lines. Since the union of these 27 lines is connected, this process is exhaustive [4] Section 7.6.

7.3 Rationalizing Lines

Now that we have computed the lines on S, consider the line

$$l := \mathbf{V}(X + \zeta_3 W, Y - iZ).$$

Points on l are parametrized by

$$P_{z_0} = (-\zeta_3 : iz_0 : z_0 : 1).$$

We have chosen this line because its complex conjugate

$$\bar{l} := \mathbf{V}(X + \zeta_3^2 W, Y + iZ)$$

also lines on our surface with a parametrization

$$P_{z_1} = (-\zeta_3^2 : -iz_1 : z_1 : 1).$$

Note that although l and $\bar{l}$ are complex conjugate, P_{z_0} and P_{z_1} generally are not. In addition to l and $\bar{l}$ being conjugates, they are also skew. By Bezout's Theorem, we know that the line through P_{z_0} and P_{z_1} intersects the surface at 3 points, two of which are P_{z_0} and P_{z_1} by construction. We can parametrize the points on the line through P_{z_0} and P_{z_1} using z_0 and z_1 from before, and introducing a third parameter t as follows:

$$\begin{aligned} P(t) &= P_{z_0} + t(P_{z_0} - P_{z_1}) \\ &= (-\zeta_3 + t(-\zeta_3 + \zeta_3^2) : iz_0 + t(iz_0 + iz_1) : z_0 + t(z_0 - iz_1) : 1). \end{aligned}$$

We let P be the third point of intersection, and we check directly that P does not lie on any of the lines on S. This is an important property of P, since if P were on a line of S, then the sweeping strategy would fail to produce points off of the plane containing the line through P. Substituting these values back into our surface gives the line

$$\begin{aligned} m = &-4\zeta^3 t^3 z_0^2 z_1 - 4\zeta^3 t^3 z_0 z_1^2 - 8\zeta^3 t^2 z_0^2 z_1 - 4\zeta^3 t^2 z_0 z_1^2 \\ &- 4\zeta^3 t z_0^2 z_1 + (6\zeta^2 - 3)t^3 + (9\zeta^2 - 9)t^2 + (3\zeta^2 - 6)t \end{aligned}$$

where ζ is a primitive twelfth root of unity. We verify that m does not lie on S by checking if m vanishes on S. Suppose $z_0, z_1 \in \mathbb{Q}(\zeta)$. Since l and $\bar{l}$ are $\mathbb{Q}(\zeta)$-rational, any Galois automorphism which fixes $\mathbb{Q}(\zeta)$ must fix P_{z_0} and P_{z_1}. By Proposition 2.14,

$$m \cap S = \{P_{z_0}, P_{z_1}, P\}$$

is a variety. As a Galois automorphism fixing $\mathbb{Q}(\zeta)$ permutes $m \cap S$, it follows that P is a $\mathbb{Q}(\zeta)$ point.

Now in order to explicitly find the third point of intersection, P, we factor m into three components as follows:

$$m = (-4\zeta^3) \cdot t \cdot (t+1) \cdot (tz_0^2 z_1 + tz_0 z_1^2 + z_0^2 z_1 + (\frac{3}{4}\zeta^3 - \frac{3}{2}\zeta)t - \frac{3}{4}\zeta^3 - \frac{3}{4}\zeta)$$

Here the values $t = 0$ and $t = -1$ correspond to the points P_{z_0} and P_{z_1}, as $t = 0$ gives $P = P_{z_0}$ and $t = -1$ gives $P = P_{z_0} - P_{z_0} + P_{z_1}$. Instead, we are interested in the third, nontrivial root, t_3. Isolating the third factor, we find that

$$t_3 = \frac{-4z_0^2 z_1 + 3\zeta^3 + 3\zeta}{4z_0^2 z_1 + 4z_0 z_1^2 + 3\zeta^3 - 6\zeta}.$$

When substituted back into our point $P_{z_0} + t(P_{z_0} - P_{z_1})$, we obtain

$$P = (-\zeta_3 + t_3(-\zeta_3 + \zeta_3^2) : iz_0 + t_3(iz_0 + iz_1) : z_0 + t_3(z_0 - iz_1) : 1),$$

where ζ_3 is a primitive third root of unity. P vanishes when substituted back into our surface, verifying that this new point does, in fact, lie on S. Substituting in our value of t_3 and clearing denominators, we see that

$$P = (X_z : Y_z : Z_z : W_z)$$

where

$$\begin{aligned}
X_z &= 4\zeta^2 z_0^2 z_1 + (-4\zeta^2 + 4) z_0 z_1^2 - 3\zeta^3 + 6\zeta \\
Y_z &= (-3\zeta^2 - 3) z_0 + (3\zeta^2 - 6) z_1 \\
Z_z &= 8 z_0^2 z_1^2 + (6\zeta^3 - 3\zeta) z_0 + (-3\zeta^3 - 3\zeta) z_1 \\
W_z &= 4 z_0^2 z_1 + 4 z_0 z_1^2 + 3\zeta^3 - 6\zeta.
\end{aligned}$$

We want P to be a rational point. As we discussed, P is a $\mathbb{Q}(\zeta)$ point. So to rationalize P, we must consider z_0 and z_1 as elements of $\mathbb{Q}(\zeta)$, which has $\{1, \zeta, \zeta^2, \zeta^3\}$ as a basis. So, let

$$\begin{aligned}
z_0 &= a_0 + \zeta \cdot a_1 + \zeta^2 \cdot a_2 + \zeta^3 \cdot a_3 \\
z_1 &= b_0 + \zeta \cdot b_1 + \zeta^2 \cdot b_2 + \zeta^3 \cdot b_3
\end{aligned}$$

with $a_i, b_i \in \mathbb{Q}$ for $0 \leq i \leq 3$. We need values of these coefficients that make P rational. To accomplish this, we consider the individual coordinates of P. For example, the Y-coodinate of P is

$$\begin{aligned}
Y = &-(3\zeta^2 + 3)a_0 + (-3\zeta^3 - 3\zeta)a_1 + (-6\zeta^2 + 3)a_2 + (-6\zeta^3 + 3\zeta)a_3 \\
&+ (3\zeta^2 - 6)b_0 + (3\zeta^3 - 6\zeta)b_1 + (-3\zeta^2 - 3)b_2 + (-3\zeta^3 - 3\zeta)b_3
\end{aligned}$$

We omit the other coordinates because each is significantly messier than this, although they can be found in the appendix. Next, we sort the coefficients of each basis element, i.e

$$\begin{aligned}
Y_\zeta &= -3a_1 + 3a_3 - 6b_1 - 3b_3 \\
Y_{\zeta^2} &= -3a_0 - 6a_2 + 3b_0 - 3b_2 \\
Y_{\zeta^3} &= -3a_1 - 6a_3 + 3b_1 - 3b_3
\end{aligned}$$

where

$$Y = c + Y_\zeta \zeta + Y_{\zeta^2}\zeta^2 + Y_{\zeta^3}\zeta^3$$

with $c = -3a_0 + 3a_2 - 6b_0 - 3b_2$ a constant. We do this for each coordinate and consider the ideal

$$I = (X_\zeta, X_{\zeta^2}, X_{\zeta^3}, Y_\zeta, Y_{\zeta^2}, Y_{\zeta^3}, Z_\zeta, Z_{\zeta^2}, Z_{\zeta^3}, W_\zeta, W_{\zeta^2}, W_{\zeta^3})$$

inside $\mathbb{C}[a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3]$. Next, we compute a Groebner basis for I. Again, this can be found in the appendix. The reason for doing so is that we are presented with several equations which allow us to eliminate some of our variables. In this case, we eliminate $b_0, b_1, b_3, a_0, a_1, a_2$. What we are left with is an ideal in b_2 and a_3. We observe that

$$4a_3^3 + 4a_3 b_2^2 - 1$$

is a factor in each of the remaining generators. We are fortunate that such a factor exists, since now the parametrization depends only on our finding a rational solution to this factor. In fact, we spot the solution $a_3 = b_2 = 1/2$ without much difficulty. We thus obtain our desired rational point by setting

$$\begin{aligned} a_0 &= 1 \\ a_1 = a_3 = b_0 = b_1 = b_2 &= 1/2 \\ a_2 &= -1/2 \\ b_3 &= -1 \end{aligned}$$

Hence

$$P = (1 : -1 : 1 : 1).$$

This will be the toehold for parametrizing our singular curve.

The existence of a rational solution for the a_is and b_is does not depend on there being a common factor, although it would have been more challenging for us to find such a solution without one. However, if no rational values satisfied our equations, then we would have needed another approach to finding our desired rational point. It remains an open problem whether this technique guarantees such a solution.

7.4 Parametrizing the Singular Curve

Now that we have a rational point $P \in S$, we can find a new hyperplane whose intersection with S is a nondegenerate, singular cubic. First, we notice that $P \in U_{W\neq 0}$, where U is defined in Definition 3.3. Given this, we dehomogenize with respect to $W = 1$ so that

$$P_{\text{aff}} = (1, -1, 1) \in S_{W=1}.$$

Next, we calculate the tangent space at P:

$$\begin{aligned}\partial_P f &= \frac{\partial f}{\partial x}(P)(x-1) + \frac{\partial f}{\partial y}(P)(y+1) + \frac{\partial f}{\partial z}(P)(z-1) \\ &= 3x^2|_P(x-1) + (3y^2+z^2)|_P(y+1) + 2yx|_P(z-1) \\ &= 3x + 4y - 2z + 3.\end{aligned}$$

Thus our tangent space is

$$T_P S = \mathbf{V}(\partial_P f).$$

By Proposition 6.14, we expect

$$C = S_{W=1} \cap T_P S$$

to be a singular curve with P a singular point. We verify this by checking that the rank of the Jacobian drops at P:

$$\begin{pmatrix} 3x^2 & 3y^2+z^2 & 2yz \\ 3 & 4 & -2 \end{pmatrix}.$$

At $P_{\text{aff}} = (1,-1,1)$, we have

$$\begin{pmatrix} 3 & 4 & -2 \\ 3 & 4 & -2 \end{pmatrix},$$

hence C is indeed singular at P_{aff}. Before proceeding, we calculate C explicitly by using the equality $\partial_P f = 3x + 4y - 2z + 3 = 0$, i.e $z = \frac{3}{2}x + 2y + \frac{3}{2}$:

$$\begin{aligned} C &= x^3 + y^3 + y(\frac{3}{2}x + 2y + \frac{3}{2})^2 + 1 \\ &= x^3 + \frac{9}{4}x^2y + 6xy^2 + 5y^3 + \frac{9}{2}xy + 6y^2 + \frac{9}{4}y + 1 \end{aligned}$$

In fact, eliminating z actually gives an isomorphic copy of C in $\mathbb{A}^2$, say C'. Since C' is a nondegenerate, singular curve, we can now employ our sweeping strategy centered with P. Using point-slope form, we write the line through $\mathbf{V}(x-1, y+1)$ with generic slope t as

$$y + 1 = t(x - 1).$$

Thus

$$y = tx - t - 1.$$

By Bezout's Theorem, this line will intersect C' at three points. To find these points, we substitute $y = tx - t - 1$ into C' and obtain

$$\begin{aligned} C_t =&(5t^3 + 6t^2 + \frac{9}{4}t + 1)x^3 + (-15t^3 - 21t^2 - \frac{39}{4}t - \frac{9}{4})x^2 \\ &+ (15t^3 + 24t^2 + \frac{51}{4}t + \frac{3}{2})x - 5t^3 - 9t^2 - \frac{21}{4}t - \frac{1}{4} \\ =&(\frac{1}{4}) \cdot ((20t^3 + 24t^2 + 9t + 4)x - 20t^3 - 36t^2 - 21t - 1) \cdot (x - 1)^2 \end{aligned}$$

Note that the double root $x = 1$ corresponds to $y = t - t - 1 = -1$, which is our singular point. We are interested in the non-trivial root, so we solve for x in the first factor:

$$x_t = \frac{20t^3 + 36t^2 + 21t + 1}{20t^3 + 24t^2 + 9t + 4}.$$

Using our equality $y = t - t - 1 = -1$, we have,

$$y_t = \frac{-8t^3 - 12t^2 - 12t - 4}{20t^3 + 24t^2 + 9t + 4}.$$

It is straightforward to verify that $(x_t, y_t) \in C'$, which we explain how to do in the appendix. We find z_t using the fact that

$$z = \frac{3}{2}x + 2y + \frac{3}{2}.$$

Thus

$$z_t = \frac{44t^3 + 66t^2 + 21t - \frac{1}{2}}{20t^3 + 24t^2 + 9t + 4}.$$

Again, it is straightforward to verify that

$$P_t = (x_t, y_t, z_t)$$

lies on our surface S. Generically, each P_t will also possess a tangent plane that meets S in a nondegenerate singular cubic curve.

We repeat this process with our single term parametrization in order to obtain a two-parameter solution. We begin by defining a hyperplane in terms of t by using the coordinates of P_t:

$$\begin{aligned}\partial_{P_t} f =& \frac{\partial f}{\partial x_t}(P_t)(x - x_t) + \frac{\partial f}{\partial y_t}(P_t)(y - y_t) + \frac{\partial f}{\partial z_t}(P_t)(z - z_t) \\ =& 3x_t^2|_{P_t}(x - x_t) + (3y_t^2 + Zzt^2)|_{P_t}(y - y_t) + 2y_t x_t|_{P_t}(z - z_t) \\ =& (\frac{1200t^6 + 4320t^5 + 6408t^4 + 4656t^3 + 1539t^2 + 126t + 3}{400t^6 + 960t^5 + 936t^4 + 592t^3 + 273t^2 + 72t + 16})x \\ &+ (\frac{2128t^6 + 6384t^5 + 7212t^4 + 3784t^3 + 1095t^2 + 267t + \frac{193}{4}}{400t^6 + 960t^5 + 936t^4 + 592t^3 + 273t^2 + 72t + 16})y \\ &+ (\frac{-704t^6 - 2112t^5 - 2976t^4 - 2432t^3 - 1020t^2 - 156t + 4}{400t^6 + 960t^5 + 936t^4 + 592t^3 + 273t^2 + 72t + 16})z + 3\end{aligned}$$

As before, we define the tangent space to be

$$T_{P_t} S = \mathbf{V}(\partial_{P_t} f).$$

Again, we expect the intersection between S and $\mathbf{V}(\partial_{P_t} f)$ to be a singular curve by Proposition 6.14. Using our substitution technique, we find

$$C_t = S_{W=1} \cap T_{P_t}(S),$$

which is a large equation in x and y. The code for finding the explicit equation can be found in the appendix. Since C_t is a singular cubic with a singularity at P_t, we parametrize the line through P_t as

$$y - y_t = u(x - x_t).$$

Hence

$$y = ux - ux_t + y_t.$$

Substituting this into C_t, we obtain our singular cubic curve defined over two parameters:

$$C_u = C_t(y = ux - ux_t + y_t).$$

Again, the explicit equation for C_u can be found in the appendix. Solving for x, we obtain

$$x_u = \frac{x_{u,N}}{x_{u,D}},$$

where

$$\begin{aligned}
x_{u,N} &= 1607680000t^{15}u^3 + 294912000t^{15}u^2 + 12539904000t^{14}u^3 - 74956800t^{15}u + 3682713600t^{14}u^2 \\
&+ 44683161600t^{13}u^3 - 132874240t^{15} - 192430080t^{14}u + 18559549440t^{13}u^2 + 96085012480t^{12}u^3 \\
&- 870531072t^{14} + 998166528t^{13}u + 52406304768t^{12}u^2 + 139102049280t^{11}u^3 - 2670772224t^{13} \\
&+ 6548877312t^{12}u + 95136104448t^{11}u^2 + 143709711360t^{10}u^3 - 5080711168t^{12} \\
&+ 17419954176t^{11}u + 119681805312t^{10}u^2 + 110101753600t^9u^3 - 6643421184t^{11} + 28432742400t^{10}u \\
&+ 109363092480t^9u^2 + 64480101120t^8u^3 - 6229211136t^{10} + 32022735360t^9u + 75019115520t^8u^2 \\
&+ 29548647360t^7u^3 - 4229558272t^9 + 26316430848t^8u + 39596387328t^7u^2 + 10678172480t^6u^3 \\
&- 2036173824t^8 + 16312318272t^7u + 16325391168t^6u^2 + 2991251280t^5u^3 - 629497728t^7 \\
&+ 7784216256t^6u + 5230153152t^5u^2 + 629699280t^4u^3 - 60378944t^6 + 2875078800t^5u \\
&+ 1252843200t^4u^2 + 99743420t^3u^3 + 57119424t^5 + 802102320t^4u + 211072320t^3u^2 + 12678180t^2u^3 \\
&+ 38451648t^4 + 156047808t^3u + 24914628t^2u^2 + 1179885tu^3 + 12572416t^3 + 17904672t^2u \\
&+ 2416068tu^2 + 37505u^3 + 2056512t^2 + 958896tu + 153612u^2 + 79296t + 18480u + 64
\end{aligned}$$

and

$$\begin{aligned}
x_{u,D} &= 1607680000t^{15}u^3 + 1634304000t^{15}u^2 + 11575296000t^{14}u^3 + 460800000t^{15}u + 12747571200t^{14}u^2 \\
&+ 37930905600t^{13}u^3 + 158597120t^{15} + 3870720000t^{14}u + 45595607040t^{13}u^2 + 75159224320t^{12}u^3 \\
&+ 1141899264t^{14} + 15081984000t^{13}u + 98849021952t^{12}u^2 + 101326648320t^{11}u^3 + 3981508608t^{13} \\
&+ 35949772800t^{12}u + 144961431552t^{11}u^2 + 99605360640t^{10}u^3 + 8900182016t^{12} + 58311567360t^{11}u
\end{aligned}$$

$$+ 152399904768t^{10}u^2 + 74925740800t^9u^3 + 14159020032t^{11} + 67840782336t^{10}u + 119179223040t^9u^2$$
$$+ 44573690880t^8u^3 + 16835149824t^{10} + 58231503360t^9u + 71224704000t^8u^2 + 21327560640t^7u^3$$
$$+ 15326879744t^9 + 37420185600t^8u + 33179836032t^7u^2 + 8234673920t^6u^3 + 10785374208t^8$$
$$+ 18087935040t^7u + 12169882752t^6u^2 + 2552933520t^5u^3 + 5859542016t^7 + 6527698560t^6u$$
$$+ 3512357568t^5u^2 + 626041920t^4u^3 + 2431946752t^6 + 1705450896t^5u + 794043360t^4u^2$$
$$+ 117890780t^3u^3 + 751428864t^5 + 298892160t^4u + 137863320t^3u^2 + 16791120t^2u^3 + 162461184t^4$$
$$+ 30517920t^3u + 16324272t^2u^2 + 1906665tu^3 + 20977408t^3 + 1719360t^2u + 922392tu^2 + 150020u^3$$
$$+ 861696t^2 + 49680tu + 18528u^2 - 77568t + 576u + 1024.$$

Consequently, we have

$$y_u = \frac{y_{u,N}}{y_{u,D}},$$

where

$$\begin{aligned}
y_{u,N} = &-1982464000t^{15}u^3 - 1189478400t^{15}u^2 - 14868480000t^{14}u^3 - 475791360t^{15}u \\
&- 9634775040t^{14}u^2 - 51493601280t^{13}u^3 - 63438848t^{15} - 3711172608t^{14}u - 36569972736t^{13}u^2 \\
&- 109203128320t^{12}u^3 - 475791360t^{14} - 13942849536t^{13}u - 85954412544t^{12}u^2 \\
&- 157800652800t^{11}u^3 - 1773404160t^{13} - 33324859392t^{12}u - 139033608192t^{11}u^2 \\
&- 162780794880t^{10}u^3 - 4310958080t^{12} - 56244731904t^{11}u - 1623511941112t^{10}u^2 \\
&- 121750712320t^9u^3 - 7554662400t^{11} - 70318522368t^{10}u - 139359621120t^9u^2 \\
&- 65777541120t^8u^3 - 10005676032t^{10} - 66469060608t^9u - 87696193536t^8u^2 \\
&- 25248130560t^7u^3 - 10238689280t^9 - 47620694016t^8u - 39567343104t^7u^2 - 6738187520t^6u^3 \\
&- 8143257600t^8 - 25504975872t^7u - 12213311232t^6u^2 - 1245649920t^5u^3 - 4997744640t^7 \\
&- 9881232384t^6u - 2357880192t^5u^2 - 170828160t^4u^3 - 2315607040t^6 - 2603305728t^5u \\
&- 233640000t^4u^2 - 18782240t^3u^3 - 776174592t^5 - 413146368t^4u - 5318976t^3u^2 - 951600t^2u^3 \\
&- 173936640t^4 - 28505856t^3u + 314496t^2u^2 + 79440tu^3 - 21990400t^3 + 453888t^2u + 7488tu^2 \\
&- 1040u^3 - 798720t^2 + 43776tu - 192u^2 + 76800t - 768u - 1024.
\end{aligned}$$

and

$$\begin{aligned}
y_{u,D} = &-1607680000t^{15}u^3 + 1634304000t^{15}u^2 + 11575296000t^{14}u^3 + 460800000t^{15}u \\
&+ 12747571200t^{14}u^2 + 37930905600t^{13}u^3 + 158597120t^{15} + 3870720000t^{14}u \\
&+ 45595607040t^{13}u^2 + 75159224320t^{12}u^3 + 1141899264t^{14} + 15081984000t^{13}u \\
&+ 98849021952t^{12}u^2 + 101326648320t^{11}u^3 + 3981508608t^{13} + 35949772800t^{12}u
\end{aligned}$$

$$+ 1449614315552t^{11}u^2 + 99605360640t^{10}u^3 + 8900182016t^{12} + 58311567360t^{11}u$$
$$+ 152399904768t^{10}u^2 + 74925740800t^9u^3 + 14159020032t^{11} + 67840782336t^{10}u$$
$$+ 119179223040t^9u^2 + 44573690880t^8u^3 + 16835149824t^{10} + 58231503360t^9u$$
$$+ 71224704000t^8u^2 + 21327560640t^7u^3 + 15326879744t^9 + 37420185600t^8u$$
$$+ 33179836032t^7u^2 + 8234673920t^6u^3 + 10785374208t^8 + 18087935040t^7u + 12169882752t^6u^2$$
$$+ 2552933520t^5u^3 + 5859542016t^7 + 6527698560t^6u + 3512357568t^5u^2 + 626041920t^4u^3$$
$$+ 2431946752t^6 + 1705450896t^5u + 794043360t^4u^2 + 117890780t^3u^3 + 751428864t^5$$
$$+ 298892160t^4u + 137863320t^3u^2 + 16791120t^2u^3 + 162461184t^4 + 30517920t^3u$$
$$+ 16324272t^2u^2 + 1906665tu^3 + 20977408t^3 + 1719360t^2u + 922392tu^2 + 150020u^3 + 861696t^2$$
$$+ 49680tu + 18528u^2 - 77568t + 576u + 1024,$$

and

$$z_u = \frac{z_{u,N}}{z_{u,D}},$$

where

$$z_{u,N} = -2882011136000t^{18}u^3 + 1729206681600t^{18}u^2 + 25938100224000t^{17}u^3 + 4395777392640t^{18}u$$
$$+ 16600384143360t^{17}u^2 + 95440176414720t^{16}u^3 + 833043300352t^{18} + 37547044503552t^{17}u$$
$$+ 67068707733504t^{16}u^2 + 175591139573760t^{15}u^3 + 8423177453568t^{17} + 148027827290112t^{16}u$$
$$+ 143168102203392t^{15}u^2 + 117469347840000t^{14}u^3 + 38707950256128t^{16} + 356559630630912t^{15}u$$
$$+ 143235096772608t^{14}u^2 - 192803556556800t^{13}u^3 + 107791754723328t^{15} + 583251904954368t^{14}u$$
$$- 63348923695104t^{13}u^2 - 618403371417600t^{12}u^3 + 204747433574400t^{14} + 675985138384896t^{13}u$$
$$- 447341167116288t^{12}u^2 - 857670675333120t^{11}u^3 + 282806032269312t^{13} + 552358962855936t^{12}u$$
$$- 771540334018560t^{11}u^2 - 770760431861760t^{10}u^3 + 294838523658240t^{12} + 290284672647168t^{11}u$$
$$- 818612502626304t^{10}u^2 - 493075984384000t^9u^3 + 236534858514432t^{11} + 516319344230 40t^{10}u$$
$$- 608381362470912t^9u^2 - 233632712908800t^8u^3 + 146526352883712t^{10} - 64141850591232t^9u$$
$$- 330281030467584t^8u^2 - 84218145177600t^7u^3 + 69070917959680t^9 - 72467714985984t^8u$$
$$- 133097431523328t^7u^2 - 23805230161920t^6u^3 + 23756748890112t^8 - 40769736597504t^7u$$
$$- 40186128936960t^6u^2 - 5468939919360t^5u^3 + 5367558389760t^7 - 14821338074112t^6u$$
$$- 9235159271424t^5u^2 - 1040229273600t^4u^3 + 525872919552t^6 - 3615700331520t^5u$$
$$- 1658038920192t^4u^2 - 159685017600t^3u^3 - 91462883328t^5 - 588206852352t^4u$$
$$- 232279617024t^3u^2 - 19129636800t^2u^3 - 37487784960t^4 - 64376561664t^3u - 22607869248t^2u^2$$

$$- 1823279040tu^3 - 4637368320t^3 - 4813871616t^2u - 1138679424tu^2 - 116212720u^3 - 352355328t^2$$
$$- 151732224tu - 21454656u^2 - 2820096t - 736512u + 1024$$

and

$$\begin{aligned}
z_{u,D} = &-9054453760000t^{18}u^3 - 9204400128000t^{18}u^2 - 78773747712000t^{17}u^3 - 2595225600000t^{18}u \\
&- 85600921190400t^{17}u^2 - 315736404787200t^{16}u^3 - 893218979840t^{18} - 256927334400000t^{17}u \\
&- 368878949498880t^{16}u^2 - 774748546007040t^{15}u^3 - 7771005124608t^{17} - 1188802068480000t^{16}u \\
&- 976070255837184t^{15}u^2 - 1306834265702400t^{14}u^3 - 32496930521088t^{16} - 340256725401600t^{15}u \\
&- 1773244467118080t^{14}u^2 - 1616585333145600t^{13}u^3 - 86820884840448t^{15} - 672407074897920t^{14}u \\
&- 2345738489561088t^{13}u^2 - 1531003699200000t^{12}u^3 - 165561552076800t^{14} - 970363149484032t^{13}u \\
&- 2342021770248192t^{12}u^2 - 1145265989222400t^{11}u^3 - 238099837747200t^{13} \\
&- 1055519463702528t^{12}u - 1808337021566976t^{11}u^2 - 691701010268160t^{10}u^3 \\
&- 266034166628352t^{12} - 881314308292608t^{11}u - 1099175293550592t^{10}u^2 \\
&- 341571749478400t^9u^3 - 234571413061632t^{11} - 570181449056256t^{10}u - 532668568535040t^9u^2 \\
&- 138420413644800t^8u^3 - 164236985106432t^{10} - 286429516185600t^9u - 207221785509888t^8u^2 \\
&- 45862890086400t^7u^3 - 91208300625920t^9 - 110976574390272t^8u - 64733584269312t^7u^2 \\
&- 12288029184000t^6u^3 - 39837318512640t^8 - 32479835701248t^7u - 16146869170176t^6u^2 \\
&- 2609921832960t^5u^3 - 13425114611712t^7 - 6863397193728t^6u - 3166205294592t^5u^2 \\
&- 429413452800t^4u^3 - 3354813038592t^6 - 961772092416t^5u - 462860190720t^4u^2 \\
&- 54541939200t^3u^3 - 570674429952t^5 - 77708021760t^4u - 42953107968t^3u^2 - 5317852800t^2u^3 \\
&- 52832501760t^4 - 3091433472t^3u - 1591160832t^2u^2 - 281227200tu^3 - 324157440t^3 \\
&- 28366848t^2u + 9229824tu^2 + 9601280u^3 + 255000576t^2 + 1631232tu + 1185792u^2 - 7716864t \\
&+ 36864u + 65536.
\end{aligned}$$

We use SAGE to verify that these points lie on our surface, as desired. Thus our family of rational points on S is given by the parametrization

$$(x_u, y_u, z_u) \in S_{W=1}.$$

Let

$$S_N = \{(x_u : y_u : z_u : 1) \mid u, t \in \mathbb{Q}\} \subseteq S$$

be the set of rational points from our 2-parameter solution. We may assume that this parametrization is dense in $S(\mathbb{Q})$, the set of all rational points of S. This is a consequence of having a 2-parameter family of solutions for a 2-dimensional object, which holds for rational varieties. To show this, we would need to consider the Zariski closure of the set of solutions we have found, which is beyond the scope of this project. Additionally, it is nontrivial to show that our parametrization is genuinely a 2-parameter solution, and not merely a 1-parameter solution in disguise. Nevertheless, we expect

$$S_N \subseteq S(\mathbb{Q}) \subseteq S \subseteq \mathbb{P}^3(\mathbb{C})$$

is dense in $S(\mathbb{Q})$.

7.5 Rational Points on $W = 0$

Recall that throughout we only worked on the subvariety of S with W nonzero. To finish, we must consider the points on the subvariety $W = 0$. That is, the surface defined by $f = X^3 + Y^3 + YZ^2$. Dehomogenizing with respect to $Y = 1$, we have $g = X^3 + Z^2 + 1$, which we recognize as an elliptic curve. We take full advantage of the powers of SAGE in computing the rational points on this elliptic curve. In fact, there are only 6 such points, which are as follows:

```
(2 :  3 :  1)    (0 :  1 :  1)    (-1 :  0 :  1)

(0 :  -1 :  1)    (2 :  -3 :  1)    (0 :  1 :  0)
```

8 Appendix

8.1 Verifying Lines on Surface

The following SAGE code verifies that the line $\mathbf{V}(X+W, Y)$ lies on our surface:

```
sage: R.<W,X,Y,Z> = QQ[]
sage: f = X^3 + Y^3 + Y * Z^2 + W^3
sage: p1 = X + W
sage: p2 = Y
sage: Iell = (p1, p2) * R
sage: f in Iell
```

The first line of code defines the polynomial ring we are working over. In this case, we know that the coefficients of the components of the line are rational, so the rational polynomial ring over X, Y, Z, W suffices. Next we define our surface, $S = \mathbf{V}(f)$, and the given line, $\mathbf{V}(X+W, Y)$. We verify that this line lies on the surface by passing to the ideal generated by the components of the line, which we call `Iell`. Then, by the inclusion-reversing correspondence between ideals and varieties, we simply check whether or not our surface lies in this ideal.

In order to verify that the line from Section 7.2 actually lies on our surface, we modify the previous code as follows:

```
sage: K.<zeta> = CyclotomicField(12)
sage: R.<W,X,Y,Z> = K[]
sage: f = X^3 + Y^3 + Y * Z^2 + W^3
sage: p1 = X + zeta^4 * W
sage: p2 = Y - i*Z
sage: Iell = (p1, p2) * R
sage: f in Iell
```

First, we need to modify our polynomial ring, as this new line has nonrational coefficients. In this case, we know that the 12-th cyclotomic field over the variables

X, Y, Z, W suffices. However, we could instead define the smallest field containing the coefficients, the composite field. Note that $\zeta^4 = \zeta_3 = \frac{1+i\sqrt{3}}{2}$, where as before, ζ is a primitive twelfth root of unity and ζ_3 is a primitive third root of unity. The SAGE code is as follows:

```
sage: K.<a> = NumberField(x^2 + 1)
sage: L.<b> = NumberField(x^2 - 3)
sage: F = K.composite_fields(L,'c')[0]
sage: phi = K.embeddings(F)[0]
sage: psi = L.embeddings(F)[0]
sage: i = phi(a)
sage: root3 = psi(b)
sage: R.<W,X,Y,Z> = F[]
sage: f = X^3 + Y^3 + Y * Z^2 + W^3
sage: p1 = Y - i * Z
sage: p2 = X - (1 / 2) * (1 + i * root3) * W
sage: Iell = (p1, p2) * R
f in Iell
```

Here, we begin by adjoining i to the rationals using the minimal polynomial $x^2 + 1$; likewise for $\sqrt{3}$. Next we create a compositum using the command for composite fields. To complete this, we specify embeddings, injective maps, from K and L into F. For convenience, we choose the first embedding that SAGE provides. This allows us to "put" $i = a$ and $\sqrt{3} = b$ into our composite field F. Thus we obtain the smallest field containing the coefficients for our line, and check that this line is on our surface as before.

8.2 Rationalizing Lines

The key to our solution was finding a rational point on a line not contained on our surface. Here, we present the SAGE code that yielded this point:

```
sage: var('W X Y Z')
sage: K.<zeta> = CyclotomicField(12)
sage: A.<t, z0, z1> = K[]
sage: B = A.fraction_field()
sage: R.<W,X,Y,Z> = B[]
sage: S = X^3 + Y^3 + Y*Z^2 + W^3
sage: i = zeta^3
sage: m = S.subs(X = zeta^(-2) + t*(zeta^(-2) - zeta^2),
...   Y = i*z0 + t*i*(z0 + z1), Z = z0 + t*(z0 - z1), W = 1)
sage: third_root = factor(m)[2][0]
sage: t3 = -((third_root - t*third_root.coefficient(t)) /
...   third_root.coefficient(t))
sage: X3 = zeta^(-2) + t3*(zeta^(-2) - zeta^2)
sage: Y3 = i*z0 + t3*i*(z0 + z1)
sage: Z3 = z0 + t3*(z0 - z1)
sage: W3 = 1
sage: expand(S.subs(X = X3, Y = Y3, Z = Z3, W = W3))
sage: P3 = ProjectiveSpace(3,B)
sage: P = P3.point((X3,Y3,Z3,W3))
sage: P.clear_denominators()
sage: P.scale_by(64)
sage: R2.<t, a0, a1, a2, a3, b0, b1, b2, b3> = K[]
sage: A2 = R2.fraction_field()
sage: psi = A.hom([t, a0 + zeta*a1 + zeta^2*a2 + zeta^3*a3,
...   b0 + zeta*b1 + zeta^2*b2 + zeta^3*b3], A2)
sage: psi(P[0]).subs(a0=1, a1=1/2, a2=-1/2, a3=1/2,
...   b0=1/2, b1=1/2, b2=1/2, b3=-1)
sage: psi(P[1]).subs(a0=1, a1=1/2, a2=-1/2, a3=1/2,
...   b0=1/2, b1=1/2, b2=1/2, b3=-1)
sage: psi(P[2]).subs(a0=1, a1=1/2, a2=-1/2, a3=1/2,
...   b0=1/2, b1=1/2, b2=1/2, b3=-1)
sage: psi(P[3]).subs(a0=1, a1=1/2, a2=-1/2, a3=1/2,
...   b0=1/2, b1=1/2, b2=1/2, b3=-1)
```

We begin by defining our variables X, Y, Z, W. We then define the cyclotomic field for the 12-th root of unity, since we know *a priori* that this field contains the coefficients for the skew lines l and $\bar{l}$ that we chose to work with. Next, we define a polynomial ring over this cyclotomic field with the variables t, z_0, z_1. Eventually we will use t as our parameter and the z_i will be used to parametrize points on l

and $\bar{l}$. We construct the field of fractions B so that we may invert t, z_0, and z_1 if necessary. Finally we define the polynomial ring over this fraction field with our variables X, Y, Z, W.

We begin by defining our surface S. For any choice of z_0 and z_1, we take the line through l and $\bar{l}$ and substitute it into S, the result of which we call m. Since thie line is defined over $\mathbb{Q}(i)$, we must first define i in terms of the 12-th root of unity. Then we factor m and isolate its nontrivial root, t_3. Note that the trivial roots correspond to the points on l and $\bar{l}$ specified by z_0 and z_1, respectively. We use t_3 to obtain (X_3, Y_3, Z_3, W_3), which is the third point on S when intersected by the line through l and $\bar{l}$. We verify that this point actually lies on our surface by substituting this point back into our surface, which does in fact vanish.

Finally, we define the projective space of dimension 3 over B. This allows us to define our new point in projective space, which we call P. We clear denominators for clarity. Next, we define a polynomial ring over our cyclotomic field with variables $t, a0, a1, a2, a3, b0, b1, b2, b3$. Again, t is our parameter and the a_i, b_i will allow us to write z_0 and z_1 as linear combinations of basis elements of our cyclotomic field. That is

$$z_0 = a_0 + \zeta \cdot a_1 + \zeta^2 \cdot a_2 + \zeta^3 \cdot a_3$$
$$z_1 = b_0 + \zeta \cdot b_1 + \zeta^2 \cdot b_2 + \zeta^3 \cdot b_3,$$

with $a_i, b_i \in \mathbb{Q}$. We define a homomorphism ψ which executes this substitution for us. Finally, letting $a0 = 1, a1 = 1/2, a2 = -1/2, a3 = 1/2, b0 = 1/2, b1 = 1/2, b2 = 1/2, b3 = -1$ we obtain our rational point on the surface which is not contained on any line of the surface. The next section will explain how we derived these values for a_i and b_i.

8.3 Elimination

```
sage: R = PolynomialRing(QQ, 8, 'a0, a1, a2, a3, b0,
...
...   b1, b2, b3')
sage: a0, a1, a2, a3, b0, b1, b2, b3 = R.gens()
sage: y0 = -3*a1 + 3*a3 - 6*b1 - 3*b3
sage: y1 = -3*a0 - 6*a2 + 3*b0 - 3*b2
sage: y2 = -3*a1 - 6*a3 + 3*b1 - 3*b3
sage: x0 = -8*a1*a2*b0 + ...
sage: x1 = 4*a0^2*b0 + ...
sage: x2 = 8*a0*a1*b0 + ...
sage: z0 = 16  *a0 *a1 *b0^2 + ...
sage: z1 = 8  *a1^2 *b0^2 + ...
sage: z2 = 16  *a1 *a2 *b0^2 + ...
sage: w0 = 8*a0*a1*b0 + ...
sage: w1 = 4  *a1^2 *b0 + ...
sage: w2 = 8*a1*a2*b0 + ...
sage: I = (y0, y1, y2, x0, x1, x2, z0, z1, z2, w0, w1, w2)*R
sage: B = I.groebner_basis()
sage: elim_gens = (I.elimination_ideal([b0,b1,b3,
...   a0,a1,a2])*R).gens()
sage: len(elim_gens)
sage: factor(elim_gens[0])
sage: factor(elim_gens[1])
sage: factor(elim_gens[2])
sage: factor(elim_gens[3])
sage: factor(elim_gens[4])
sage: factor(elim_gens[5])
sage: factor(elim_gens[6])
```

We begin by defining our polynomial ring over the rationals with variables a_i, b_i for $0 \leq i \leq 3$. We then define each of the coordinates of our point P, as described in Section 7.3. We then define the ideal generated by each of these coordinates and find a Groebner basis for this ideal. This gives us a presentation of the ideal revealing eliminable coordinates. What remains is is an ideal in b_2 and a_3. The length of our eliminated ideal is seven, so we observe the factorization of each of

these 7 polynomials. In our case, each has the factor $4a_3^3 + 4a_3b_2^2 - 1$, which we used in Section 7.3 to determine the acceptable values for the a_i and b_i.

8.4 Parametrizing a Singular Curve

```
sage: R0 = PolynomialRing(QQ, 2, 't,u')
sage: t,u = R0.gens()
sage: K0 = R0.fraction_field()
sage: R = PolynomialRing(K0, 4, 'X, Y, Z, W')
sage: X, Y, Z, W = R.gens()
sage: c_t = c.subs(Y = t*X - t - 1)
sage: xpoly = factor(c_t)[0][0]
sage: X_t = (-xpoly.coefficient({X:0}) /
...   xpoly.coefficient({X:1}))
sage: Y_t = t*X_t - t - 1
sage: c_p = c.subs(X = X_t, Y = Y_t); c_p
sage: Z_t = 3/2*X_t + 2*Y_t + 3/2
sage: f_p = f.subs(X = X_t, Y = Y_t, Z = Z_t); f_p
sage: h = 3*X_t^2*(X - X_t) + (3*Y_t^2 + Z_t^2)*(Y - Y_t)
...   + 2*Y_t*Z_t*(Z - Z_t)
sage: hZ = (-h.coefficient({Z:0}) /
...   h.coefficient({Z:1})
...   .coefficient({X:0})
...   .coefficient({Y:0}))
sage: C = f.subs(Z = hZ)
sage: C_u = C.subs(Y = u*X - u*X_t + Y_t)
sage: xpoly1 = factor(C_u)[0][0]
sage: X_u = (-xpoly1.coefficient({X:0}) /
...   xpoly1.coefficient({X:1}))
sage: Y_u = u*X_u - u*X_t + Y_t
sage: C_p = C.subs(X = X_u, Y = Y_u); C_p
sage: Z_u = hZ.subs(X = X_u, Y = Y_u)
sage: f_u = f.subs(X = X_u, Y = Y_u, Z = Z_u); f_u
```

We began as usual by defining the necessary polynomial ring. In this case, we define a polynomial ring in X, Y, Z, W over a fraction field of a polynomial ring over the rationals with the variables t and u. These last variables will be the two required parameters for our parametrization. What follows is simply the execution of what

we explained in Section 7.4. We parametrize the line through our rational point using t as the slope of our line. We find the subsequent X and Y coordinates for the nontrivial point on the surface intersecting this line, and verify that this lies on our curve (the intersection of our surface and the tangent plane). We then recover the Z coordinate and again verify that this lies on our surface. Using this point, X_t, Y_t, Z_t, we repeat the same process. This time around we use u as the parameter for the slope of the line. As before, this process lets us obtain the X, Y, and Z coordinates for our point. We check that this point is actually on our surface and, voila, we have our parametrization.

8.5 Rational Points on an Elliptic Curve

We recognize in Section 7.5 that

$$X^3 + Y^3 + YZ^2$$

is an elliptic curve. Since much is known about elliptic curves, we simply look up our curve on the Cremona Database of elliptic curves. We consider the rank and torsion subgroup associated to our elliptic curve, which in this case is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The six rational points are then computed by taking powers of the generator.

```
sage: E = EllipticCurve(QQ,[0,1])
sage: E.conductor()
sage: E.cremona_label()
sage: E.rank(); E.torsion_subgroup()
sage: P = E.torsion_subgroup().gens()[0]
sage: 2*P
sage: 3*P
sage: 4*P
sage: 5*P
sage: 6*P
```

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[3] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[4] Miles Reid. *Undergraduate algebraic geometry*, volume 12 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1988.

[5] W. A. Stein et al. *Sage Mathematics Software (Version 6.5)*. The Sage Development Team, 2015. `http://www.sagemath.org`.