Algebraic Geometry: A Problem Solving Approach

Park City Mathematics Institute - 2008

Thomas A. Garrity, Project Lead

Richard Belshoff

Lynette Boos

Ryan Brown

Jim Drouihlet

Carl Lienert

David Murphy

Junalyn Navarra-Madsen

Pedro Poitevin

Shawn Robinson

Brian A. Snyder

Caryn Werner

Williams College

Missouri State University

Trinity College
Current address: Providence College

Georgia College and State University

Minnesota State University
Current address: Jim passed away January 23, 2009 during writing of this book.

Fort Lewis College

Hillsdale College

Texas Woman's University

Salem State College

University of Maine, Presque Isle

Lake Superior State University

Allegheny College

Contents

Preface ix
- 0.1. Algebraic geometry ix
- 0.2. Overview x
- 0.3. Problem book xi
- 0.4. History of book xii
- 0.5. An aside on notation xii
- 0.6. Thanks xiii

Chapter 1. Conics 1
- 1.1. Conics over the Reals 1
- 1.2. Changes of Coordinates 5
- 1.3. Conics over the Complex Numbers 14
- 1.4. The Complex Projective Plane $\mathbb{P}^2$ 18
- 1.5. Projective Change of Coordinates 22
- 1.6. The Complex Projective Line $\mathbb{P}^1$ 24
- 1.7. Ellipses, Hyperbolas, and Parabolas as Spheres 26
- 1.8. Degenerate Conics - Crossing lines and double lines. 30
- 1.9. Tangents and Singular Points 32
- 1.10. Conics via linear algebra 37
- 1.11. Duality 42

Chapter 2. Cubic Curves and Elliptic Curves 47
- 2.1. Cubics in $\mathbb{C}^2$ 47
- 2.2. Inflection Points 48
- 2.3. Group Law 56
- 2.4. Normal forms of cubics 64
- 2.5. The Group Law for a Smooth Cubic in Canonical Form 75
- 2.6. Cubics as Tori 81
- 2.7. Cross-Ratios and the j-Invariant 83
- 2.8. Cross Ratio: A Projective Invariant 88
- 2.9. Torus as $\mathbb{C}/\Lambda$ 90
- 2.10. Mapping $\mathbb{C}/\Lambda$ to a Cubic 95

Chapter 3. Higher Degree Curves 99
3.1. Higher Degree Polynomials and Curves 99
3.2. Higher Degree Curves as Surfaces 100
3.3. Bézout's Theorem 104
3.4. Regular Functions and Function Fields 114
3.5. The Riemann-Roch Theorem 119
3.6. Blowing up 142

Chapter 4. Affine Varieties 149
4.1. Zero Sets of Polynomials 149
4.2. Algebraic Sets 151
4.3. Zero Sets via $V(I)$ 152
4.4. Functions on Zero Sets and the Coordinate Ring 154
4.5. Hilbert Basis Theorem 155
4.6. Hilbert Nullstellensatz 157
4.7. Variety as Irreducible Algebraic Set: Prime Ideals 159
4.8. Subvarieties 161
4.9. Function Fields 163
4.10. Points as Maximal Ideals 165
4.11. The Zariski Topology 165
4.12. Points and Local Rings 172
4.13. Tangent Spaces 175
4.14. Dimension 180
4.15. Singular Points 182
4.16. Morphisms 185
4.17. Isomorphisms of Varieties 187
4.18. Rational Maps 191
4.19. Products of Affine Varieties 196

Chapter 5. Projective Varieties 199
5.1. Definition of Projective n-space $\mathbb{P}^n(k)$ 199
5.2. Graded Rings and Homogeneous Ideals 202
5.3. Projective Varieties 205
5.4. Functions on Projective Varieties 208
5.5. Examples 212

Chapter 6. Sheaves and Cohomology 217
6.1. Intuition and Motivation for Sheaves 217
6.2. The Definition of a Sheaf 220
6.3. The Sheaf of Rational Functions 224

6.4. Divisors 225
6.5. Invertible Sheaves and Divisors 228
6.6. Basic Homology Theory 231
6.7. Cech Cohomology 232

Appendix A. A Brief Review of Complex Analysis 239
A.1. Visualizing Complex Numbers 239
A.2. Power Series 239
A.3. Residues 239
A.4. Liouville's Theorem 239

Appendix. Bibliography 241

Appendix. Index 243

Preface

0.1. Algebraic geometry

As the name suggests, algebraic geometry is the linking of algebra to geometry. For example, the circle, a geometric object, can also be described as the points

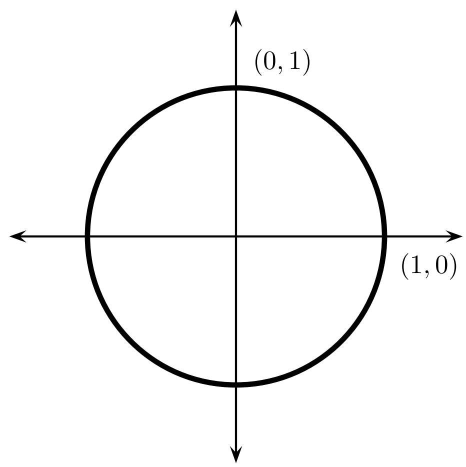


FIGURE 1. The unit circle centered at the origin

(x, y) in the plane satisfying the polynomial

$$x^2 + y^2 - 1 = 0,$$

an algebraic object. Algebraic geometry is thus often described as the study of those geometric objects that can be described by polynomials. Ideally, we want a complete correspondence between the geometry and the algebra, allowing intuitions from one to shape and influence the other.

The building up of this correspondence is at the heart of much of mathematics for the last few hundred years. It touches area after area of mathematics. By now, despite the humble beginnings of the circle

$$(x^2 + y^2 - 1 = 0),$$

algebraic geometry is not an easy area to break into.

Hence this book.

0.2. Overview

Algebraic geometry is amazingly useful, and yet much of its development has been guided by aesthetic considerations: some of the key historical developments in the subject were the result of an impulse to achieve a strong internal sense of beauty.

One way of doing mathematics is to ask bold questions about concepts you are interested in studying. Usually this leads to fairly complicated answers having many special cases. An important advantage of this approach is that the questions are natural and easy to understand. A disadvantage is that, on the other hand, the proofs are hard to follow and often involve clever tricks, the origin of which is very hard to see.

A second approach is to spend time carefully defining the basic terms, with the aim that the eventual theorems and their proofs are straightforward. Here, the difficulty is in understanding how the definitions, which often initially seem somewhat arbitrary, ever came to be. And the payoff is that the deep theorems are more natural, their insights more accessible, and the theory is more aesthetically pleasing. It is this second approach that has prevailed in much of the development of algebraic geometry.

This second approach is linked to solving *equivalence problems*. By an equivalence problem, we mean the problem of determining, within a certain mathematical context, when two mathematical objects are *the same*. What is meant by *the same* differs from one mathematical context to another. In fact, one way to classify different branches of mathematics is to identify their equivalence problems.

A branch of mathematics is closed if its equivalence problems can be easily solved. Active, currently rich branches of mathematics are frequently where there are partial but not complete solutions. The branches of mathematics that will only be active in the future are those for which there is currently no hint for solving any type of equivalence problem.

To solve, or at least set up the language for a solution to an equivalence problem frequently involves understanding the functions defined on an object. Since we will be concerned with the algebra behind geometric objects, we will spend time on correctly defining natural classes of functions on these objects. This in turn will allow us to correctly describe what we will mean by equivalence.

Now for a bit of an overview of this text. In Chapter One, our motivation will be to find the natural context for being able to state that all conics (all zero loci of second degree polynomials) are the same. The key will be the development of the complex projective plane $\mathbb{P}^2$. We will say that two curves in this new space $\mathbb{P}^2$ are the “same” (we will use the term “isomorphic”) if one curve can be transformed into the other by a projective change of coordinates (which we will define).

Chapter Two will look at when two cubic curves are the same in $\mathbb{P}^2$ (meaning again that one curve can be transformed into the other by a projective change of coordinates). Here we will see that there are many, many different cubics. We will further see that the points on a cubic have incredible structure; technically we will see that the points form an abelian group.

Chapter Three turns to higher degree curves. From our earlier work, we still think of these curves as “living” in the space $\mathbb{P}^2$. The first goal of this chapter is Bezout’s theorem. If we stick to curves in the real plane $\mathbb{R}^2$, which would be the naive first place to work in, one can prove that a curve that is the zero loci of a polynomial of degree d will intersect another curve of degree e in at most de points. In our claimed more natural space of $\mathbb{P}^2$, we will see that these two curves will intersect in exactly de points, with the additional subtlety of needing to also give the correct definition for intersection multiplicity. We will then define on a curve its natural class of functions, which will be called the curve’s *ring of regular functions*.

In Chapter Four we look at the geometry of more complicated objects than curves in the plane $\mathbb{P}^2$. We will be treating the zero loci of collections of polynomials in many variables, and hence looking at geometric objects in $\mathbb{C}^n$. Here the exercises work out how to bring much more of the full force of ring theory to bear on geometry; in particular the function theory plays an increasingly important role. With this language we will see that there are actually two different but natural equivalence problems: isomorphism and birationality.

Chapter Five develops the true natural ambient space, complex projective n-space $\mathbb{P}^n$, and the corresponding ring theory.

Chapter Six moves up the level of mathematics, providing an introduction to the more abstract (and more powerful) developments in algebraic geometry in the nineteen fifties and nineteen sixties.

0.3. Problem book

This is a book of problems. We envision three possible audiences.

The first audience consists of students who have taken a courses in multivariable calculus and linear algebra. The first three chapters are appropriate for a semester long course for these people. If you are in this audience, here is some advice. You are at the stage of your mathematical career of shifting from merely solving homework exercises to proving theorems. While working the problems ask yourself what is the big picture. After working a few problems, close the book and try to think of what is going on. Ideally you would try to write down in your own words the material that you just covered. What is most likely is that the first few times you try this, you will be at a loss for words. This is normal. Use this as an indication that you are not yet mastering this section. Repeat this process until you can describe the mathematics with confidence, ready to lecture to your friends.

The second audience consists of students who have had a course in abstract algebra. Then the whole book is fair game. You are at the stage where you know that much of mathematics is the attempt to prove theorems. The next stage of your mathematical development is in coming up with your own theorems, with the ultimate goal being to become creative mathematicians. This is a long process. We suggest that you follow the advice given in the previous paragraph, with the additional advice being to occasionally ask yourself some of your own questions.

The third audience is what the authors referred to as "mathematicians on an airplane." Many professional mathematicians would like to know some algebraic geometry. But jumping into an algebraic geometry text can be difficult. For the pro, we had the image of them taking this book along on a long flight, with most of the problems just hard enough to be interesting but not so hard so that distractions on the flight will interfere with thinking. It must be emphasized that we do not think of these problems as being easy for student readers.

0.4. History of book

This book, with its many authors, had its start in the summer of 2008 at the Park City Mathematics Institute's Undergraduate Faculty Program on Algebraic and Analytic Geometry. Tom Garrity led a group of mathematicians on the the basics of algebraic geometry, with the goal being for the participants to be able to teach an algebraic geometry at their own college or university.

Since everyone had a Ph.D. in math, each of us knew that you cannot learn math by just listening to someone lecture. The only way to learn is by thinking through the math on ones own. Thus we decided to try to write a new beginning text on algebraic geometry, based on the reader solving many, many exercises. This book is the result.

0.5. An aside on notation

Good notation in mathematics is important but can be tricky. It is often the case that the same mathematical object is best described using different notations depending on context. For example, in this book we will sometimes denote a curve by the symbol $\mathcal{C}$ while at other time denote the curve by the symbol $V(P)$, where the curve is the zero loci of the polynomial $P(x, y)$. Both notations are natural and both will be used.

0.6. Thanks

There are going to be many people and organizations for which the authors are grateful. We would like to thank the Institute for Advanced Study and the Park City Mathematics Institute for their support.

The authors would like to thank the students at Georgia College and State University who will course-test this manuscript and provide many great suggestions.

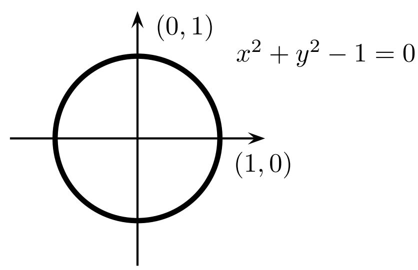
CHAPTER 1

Conics

Linear algebra studies the simplest type of geometric objects, such as straight lines and planes. Straight lines in the plane are the zero sets of linear, or first degree, polynomials, such as $\{(x, y) \in \mathbb{R}^2 : 3x + 4y - 1 = 0\}$. But there are far more plane curves than just straight lines.

We start by looking at conics, which are the zero sets of second degree polynomials. The quintessential conic is the circle:

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0\}.$$



Despite their seeming simplicity, an understanding of second degree equations and their solution sets are the beginning of much of algebraic geometry. By the end of the chapter, we will have developed some beautiful mathematics.

1.1. Conics over the Reals

The goal of this section is to understand the properties and to see how to graph conics in the real plane $\mathbb{R}^2$.

For second degree polynomials, you can usually get a fairly good graph of the corresponding curve by just drawing it "by hand". The first series of exercises will lead you through this process. Our goal is to develop basic techniques for thinking about curves without worrying about too many technical details.

We start with the polynomial $P(x, y) = y - x^2$ and want to look at its zero set

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : P(x, y) = 0\}.$$

We also denote this set by $V(P)$.

EXERCISE 1.1.1. Show that for any $(x, y) \in \mathcal{C}$, then we also have

$$(-x, y) \in \mathcal{C}.$$

Thus the curve $\mathcal{C}$ is symmetric about the y-axis.

EXERCISE 1.1.2. Show that if $(x, y) \in \mathcal{C}$, then we have $y \geq 0$.

EXERCISE 1.1.3. For points $(x, y) \in \mathcal{C}$, show that if y goes to infinity, then one of the corresponding x-coordinates also approaches infinity while the other corresponding x-coordinate must approach negative infinity.

These two exercises show that the curve $\mathcal{C}$ is unbounded in the positive and negative x-directions, unbounded in the positive y-direction, but bounded in the negative y-direction. This means that we can always find $(x, y) \in \mathcal{C}$ so that x is arbitrarily large, in either the positive or negative directions, y is arbitrarily large in the positive direction, but that there is a number M (in this case 0) such that $y \geq M$ (in this case $y \geq 0$).

EXERCISE 1.1.4. Sketch the curve $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : P(x, y) = 0\}$. (The reader is welcome to use Calculus to give a more rigorous sketch of this curve.)

Conics that have these symmetry and boundedness properties and look like this curve $\mathcal{C}$ are called *parabolas*. Of course, we could have analyzed the curve $\{(x, y) : x - y^2 = 0\}$ and made similar observations, but with the roles of x and y reversed. In fact, we could have shifted, stretched, and rotated our parabola many ways and still retained these basic features.

We now perform a similar analysis for the plane curve

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : \left(\frac{x^2}{4}\right) + \left(\frac{y^2}{9}\right) - 1 = 0\}.$$

EXERCISE 1.1.5. Show that if $(x, y) \in \mathcal{C}$, then the three points $(-x, y)$, $(x, -y)$, and $(-x, -y)$ are also on $\mathcal{C}$. Thus the curve $\mathcal{C}$ is symmetric about both the x and y-axes.

EXERCISE 1.1.6. Show that for every $(x, y) \in \mathcal{C}$, we have $|x| \leq 2$ and $|y| \leq 3$.

This shows that the curve $\mathcal{C}$ is bounded in both the positive and negative x and y-directions.

EXERCISE 1.1.7. Sketch $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : \left(\frac{x^2}{4}\right) + \left(\frac{y^2}{9}\right) - 1 = 0\}$.

Conics that have these symmetry and boundedness properties and look like this curve $\mathcal{C}$ are called *ellipses*.

There is a third type of conic. Consider the curve

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : x^2 - y^2 - 4 = 0\}.$$

EXERCISE 1.1.8. Show that if $(x, y) \in \mathcal{C}$, then the three points $(-x, y)$, $(x, -y)$, and $(-x, -y)$ are also on $\mathcal{C}$. Thus the curve $\mathcal{C}$ is also symmetric about both the x and y-axes.

EXERCISE 1.1.9. Show that if $(x, y) \in \mathcal{C}$, then we have $|x| \geq 2$.

This shows that the curve $\mathcal{C}$ has two connected components. Intuitively, this means that $\mathcal{C}$ is composed of two distinct pieces that do not touch.

EXERCISE 1.1.10. Show that the curve $\mathcal{C}$ is unbounded in the positive and negative x-directions and also unbounded in the positive and negative y-directions.

EXERCISE 1.1.11. Sketch $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : x^2 - y^2 - 4 = 0\}$.

Conics that have these symmetry, connectedness, and boundedness properties are called *hyperbolas*.

In the following exercise, the goal is to sketch many concrete conics.

EXERCISE 1.1.12. Sketch the graph of each of the following conics in $\mathbb{R}^2$. Identify which are parabolas, ellipses, or hyperbolas.

(1) $V(x^2 - 8y)$
(2) $V(x^2 + 2x - y^2 - 3y - 1)$
(3) $V(4x^2 + y^2)$
(4) $V(3x^2 + 3y^2 - 75)$
(5) $V(x^2 - 9y^2)$
(6) $V(4x^2 + y^2 - 8)$
(7) $V(x^2 + 9y^2 - 36)$
(8) $V(x^2 - 4y^2 - 16)$
(9) $V(y^2 - x^2 - 9)$

A natural question arises in the study of conics. If we have a second degree polynomial, how can we determine whether its zero set is an ellipse, hyperbola, parabola, or something else in $\mathbb{R}^2$. Suppose we have the following polynomial.

$$P(x, y) = ax^2 + bxy + cy^2 + dx + ey + h$$

What are there conditions on a, b, c, d, e, h that determine what type of conic $V(P)$ is? Whenever we have a polynomial in more than one variable, a useful technique is to treat P as a polynomial in a single variable whose coefficients are themselves polynomials.

EXERCISE 1.1.13. Express the polynomial $P(x, y) = ax^2 + bxy + cy^2 + dx + ey + h$ in the form

$$P(x, y) = Ax^2 + Bx + C$$

where A, B, and C are polynomial functions of y. What are A, B, and C?

Since we are interested in the zero set $V(P)$, we want to find the roots of $Ax^2 + Bx + C = 0$ in terms of y. As we know from high school algebra not all quadratic equations in a single variable have real roots. The number of real roots is determined by the discriminant Δ_x of the equation, so let's find the discriminant of $Ax^2 + Bx + C = 0$ as a function of y.

EXERCISE 1.1.14. Show that the discriminant of $Ax^2 + Bx + C = 0$ is

$$\Delta_x(y) = (b^2 - 4ac)y^2 + (2bd - 4ae)y + (d^2 - 4ah).$$

EXERCISE 1.1.15.

(1) Suppose $\Delta_x(y_0) < 0$. Explain why there is no point on $V(P)$ whose y-coordinate is y_0.
(2) Suppose $\Delta_x(y_0) = 0$. Explain why there is exactly one point $V(P)$ whose y-coordinate is y_0.
(3) Suppose $\Delta_x(y_0) > 0$. Explain why there are exactly two points $V(P)$ whose y-coordinate is y_0.

This exercise demonstrates that in order to understand the set $V(P)$ we need to understand the set $\{y \mid \Delta_x(y) \geq 0\}$.

EXERCISE 1.1.16. Suppose $b^2 - 4ac = 0$.

(1) Show that $\Delta_x(y)$ is linear and that $\Delta_x(y) \geq 0$ if and only if $y \geq \dfrac{4ah - d^2}{2bd - 4ae}$, provided $2bd - 4ae \neq 0$.
(2) Conclude that if $b^2 - 4ac = 0$ (and $2bd - 4ae \neq 0$) , then $V(P)$ is a parabola.

Notice that if $b^2 - 4ac \neq 0$, then $\Delta_x(y)$ is itself a quadratic function in y, and the features of the set over which $\Delta_x(y)$ is nonnegative is determined by its quadratic coefficient.

EXERCISE 1.1.17. Suppose $b^2 - 4ac < 0$.

(1) Show that one of the following occurs: $\{y \mid \Delta_x(y) \geq 0\} = \emptyset$, $\{y \mid \Delta_x(y) \geq 0\} = \{y_0\}$, or there exist real numbers α and β, $\alpha < \beta$, such that $\{y \mid \Delta_x(y) \geq 0\} = \{y \mid \alpha \leq y \leq \beta\}$.
(2) Conclude that $V(P)$ is either empty, a point, or an ellipse.

EXERCISE 1.1.18. Suppose $b^2 - 4ac > 0$.

(1) Show that one of the following occurs: $\{y \mid \Delta_x(y) \geq 0\} = \mathbb{R}$ and $\Delta_x(y) \neq 0$, $\{y \mid \Delta_x(y) = 0\} = \{y_0\}$ and $\{y \mid \Delta_x(y) > 0\} = \{y \mid |y| > y_0\}$, or there exist real numbers α and β, $\alpha < \beta$, such that $\{y \mid \Delta_x(y) \geq 0\} = \{y \mid y \leq \alpha\} \cup \{y \mid y \geq \beta\}$.

(2) Show that if there exist real numbers α and β, $\alpha < \beta$, such that $\{y \mid \Delta_x(y) \geq 0\} = \{y \mid y \leq \alpha\} \cup \{y \mid y \geq \beta\}$, then $V(P)$ is a hyperbola.

Above we decided to treat P as a function of x, but we could have treated P as a function of y, $P(x,y) = A'y^2 + B'y + C'$ each of whose coefficients is a polynomial in x.

EXERCISE 1.1.19. Show that the discriminant of $A'y^2 + B'y + C' = 0$ is

$$\Delta_y(x) = (b^2 - 4ac)x^2 + (2be - 4cd)x + (e^2 - 4ch).$$

Note that the quadratic coefficient is again $b^2 - 4ac$, so our observations from above are the same in this case as well. In the preceding exercises we were intentionally vague about some cases. For example, we do not say anything about what happens when $b^2 - 4ac = 0$ and $2bd - 4ae = 0$. This is an example of a "degenerate" conic. We treat degenerate conics later in this chapter, but for now it suffices to note that if $b^2 - 4ac = 0$, then $V(P)$ is not an ellipse or hyperbola. If $b^2 - 4ac < 0$, then $V(P)$ is not a parabola or hyperbola. And if $b^2 - 4ac > 0$, then $V(P)$ is not a parabola or ellipse. This leads us to the following theorem.

THEOREM 1.1.20. Suppose $P(x,y) = ax^2 + bxy + cy^2 + dx + ey + h$. If $V(P)$ is a parabola in $\mathbb{R}^2$, then $b^2 - 4ac = 0$; if $V(P)$ is an ellipse in $\mathbb{R}^2$, then $b^2 - 4ac < 0$; and if $V(P)$ is a hyperbola in $\mathbb{R}^2$, then $b^2 - 4ac > 0$.

In general, it is not immediately clear whether a given conic $V(ax^2 + bxy + cy^2 + dx + e + h)$ is an ellipse, hyperbola, or parabola, but if the coefficient $b = 0$, then it is much easier to determine whether $\mathcal{C} = V(ax^2 + cy^2 + dx + ey + h)$ is an ellipse, hyperbola, or parabola.

COROLLARY 1.1.1. Suppose $P(x,y) = ax^2 + cy^2 + dx + ey + h$. If $V(P)$ is a parabola in $\mathbb{R}^2$, then $ac = 0$; if $V(P)$ is an ellipse in $\mathbb{R}^2$, then $ac < 0$, i.e. a and c have opposite signs; and if $V(P)$ is a hyperbola in $\mathbb{R}^2$, then $ac > 0$, i.e. a and c have the same sign.

1.2. Changes of Coordinates

The goal of this section is to sketch intuitively how, in $\mathbb{R}^2$, any ellipse can be transformed into any other ellipse, any hyperbola into any other hyperbola, and any parabola into any other parabola.

Here we start to investigate what it could mean for two conics to be the "same"; thus we start to solve an equivalence problem for conics. Intuitively, two curves are the same if we can shift, stretch, or rotate one to obtain the other. Cutting or gluing however is not allowed.

Our conics live in the real plane, $\mathbb{R}^2$. In order to describe conics as the zero sets of second degree polynomials, we first must choose a coordinate system for the plane $\mathbb{R}^2$. Different choices for these coordinates will give different polynomials, even for the same curve. (To make this concrete, have 10 people separately go to a blank blackboard, put a dot on it to correspond to an origin and then draw two axes. There will be 10 quite different coordinate systems chosen.)

Consider the two coordinate systems: There is a dictionary between these

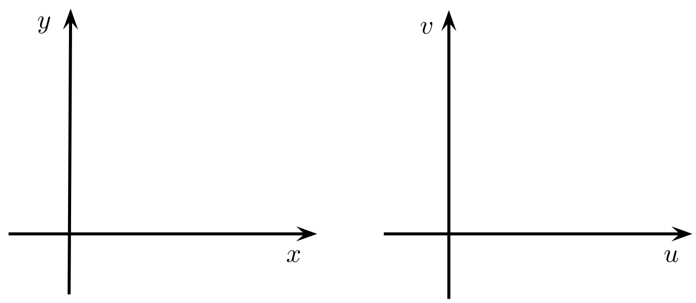


FIGURE 1. xy and uv-coordinate systems

coordinate systems, given by

$$u = x - 3,$$
$$v = y - 2.$$

Then the circle of radius 4 has either the equation

$$u^2 + v^2 - 4 = 0$$

or the equation

$$(x-3)^2 + (y-2)^2 - 4 = 0,$$

which is the same as $x^2 - 6x + y^2 - 4y + 9 = 0$. These two coordinate systems differ only by where you place the origin. Coordinate systems can also differ in their orientation. Consider two coordinate systems where the dictionary between the coordinate systems is:

$$u = x - y$$
$$v = x + y.$$

Coordinate systems can also vary by the chosen units of length. Consider two coordinate systems where the dictionary between the coordinate systems is:

$$u = 2x$$
$$v = 3y.$$

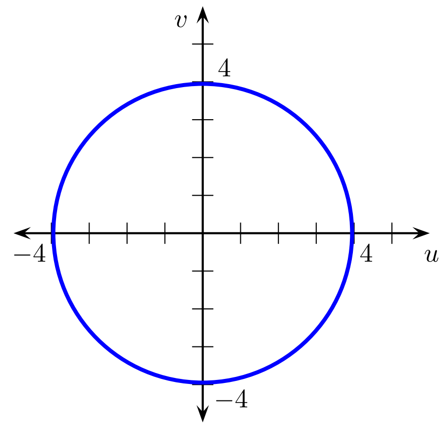


FIGURE 2. Circle of radius 4 centered at the origin in the uv-coordinate system

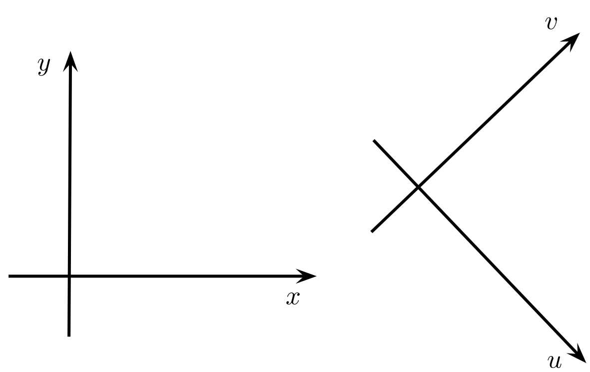


FIGURE 3. xy and uv-coordinate systems with different orientations

All of these possibilities are captured in the following.

DEFINITION 1.2.1. A *real affine change of coordinates* in the real plane, $\mathbb{R}^2$, is given by

$$u = ax + by + e$$
$$v = cx + dy + f,$$

where $a, b, c, d, e, f \in \mathbb{R}$ and

$$ad - bc \neq 0.$$

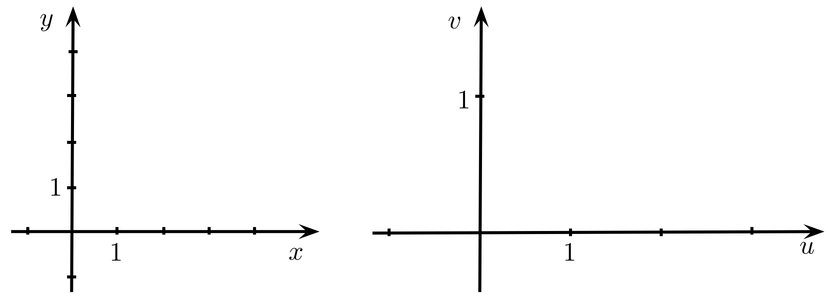


FIGURE 4. xy and uv-coordinate systems with different units

In matrix language, we have

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix},$$

where $a, b, c, d, e, f \in \mathbb{R}$, and

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0.$$

EXERCISE 1.2.1. Show that the origin in the xy-coordinate system agrees with the origin in the uv-coordinate system if and only if $e = f = 0$. Thus the constants e and f describe translations of the origin.

EXERCISE 1.2.2. Show that if $u = ax + by + e$ and $v = cx + dy + f$ is a change of coordinates, then the inverse change of coordinates is

$$\begin{aligned} x &= \left(\frac{1}{ad - bc}\right)(du - bv) - \left(\frac{1}{ad - bc}\right)(de - bf) \\ y &= \left(\frac{1}{ad - bc}\right)(-cu + av) - \left(\frac{1}{ad - bc}\right)(-ce + af). \end{aligned}$$

This is why we require that $ad - bc \neq 0$. There are two ways of working this problem. One method is to just start fiddling with the equations. The second is to translate the change of coordinates into the matrix language and then use a little linear algebra.

We frequently go back and forth between using a change of coordinates and its inverse. For example, suppose we have the ellipse $V(x^2 + y^2 - 1)$ in the xy-plane. Under the real affine change of coordinates

$$\begin{aligned} u &= x + y \\ v &= 2x - y, \end{aligned}$$

this ellipse becomes $V(5u^2 - 2uv + 2v^2 - 9)$ in the uv-plane (verify this). To change coordinates from the xy-plane to the uv-plane we replace x and y with $\frac{u}{3} + \frac{v}{4}$ and $\frac{2u}{3} - \frac{v}{3}$, respectively. In other words to change from the xy-coordinate system to the uv-coordinate system, we use the inverse change of coordinates

$$x = \frac{1}{3}u + \frac{1}{3}v$$

$$y = \frac{2}{3}u - \frac{1}{3}v.$$

Since any affine transformation has an inverse transformation, we will not worry too much about whether we are using a transformation or its inverse in our calculations. When the context requires care, we will make the distinction.

It is also common for us to change coordinates multiple times, but we need to ensure that a composition of real affine changes of coordinates is a real affine change of coordinates.

EXERCISE 1.2.3. Show that if

$$u = ax + by + e$$
$$v = cx + dy + f$$

and

$$s = Au + By + E$$
$$t = Cu + Dy + F$$

are two real affine changes of coordinates from the xy-plane to the uv-plane and from the uv-plane to the st-plane, respectively, then the composition from the xy-plane to the st-plane is a real affine change of coordinates.

EXERCISE 1.2.4. For each pair of ellipses, find a real affine change of coordinates that maps the ellipse in the xy-plane to the ellipse in the uv-plane.

(1) $V(x^2 + y^2 - 1)$, $V(16u^2 + 9v^2 - 1)$
(2) $V((x-1)^2 + y^2 - 1)$, $V(16u^2 + 9(v+2)^2 - 1)$
(3) $V(4x^2 + y^2 - 6y + 8)$, $V(u^2 - 4u + v^2 - 2v + 4)$
(4) $V(13x^2 - 10xy + 13y^2 - 1)$, $V(4u^2 + 9v^2 - 1)$

We can apply a similar argument for hyperbolas.

EXERCISE 1.2.5. For each pair of hyperbolas, find a real affine change of coordinates that maps the hyperbola in the xy-plane to the hyperbola in the uv-plane.

(1) $V(xy-1)$, $V(u^2-v^2-1)$
(2) $V(x^2-y^2-1)$, $V(16u^2-9v^2-1)$
(3) $V((x-1)^2-y^2-1)$, $V(16u^2-9(v+2)^2-1)$
(4) $V(x^2-y^2-1)$, $V(v^2-u^2-1)$
(5) $V(8xy-1)$, $V(2u^2-2v^2-1)$

Exercise 1.2.6. Give an intuitive argument, based on number of connected components, for the fact that no ellipse can be transformed into a hyperbola by a real affine change of coordinates.

Now we move on to parabolas.

Exercise 1.2.7. For each pair of parabolas, find a real affine change of coordinates that maps the parabola in the xy-plane to the parabola in the uv-plane.

(1) $V(x^2-y)$, $V(9v^2-4u)$
(2) $V((x-1)^2-y)$, $V(u^2-9(v+2))$
(3) $V(x^2-y)$, $V(u^2+2uv+v^2-u+v-2)$.
(4) $V(x^2-4x+y+4)$, $V(4u^2-(v+1))$
(5) $V(4x^2+4xy+y^2-y+1)$, $V(4u^2+v)$

The preceding three problems suggest that we can transform ellipses to ellipses, hyperbolas to hyperbolas, and parabolas to parabolas by way of real affine changes of coordinates. This turns out to be the case. Suppose $\mathcal{C} = V(ax^2+bxy+cy^2+dx+ey+h)$ is a smooth conic in $\mathbb{R}^2$. Our goal in the next several exercises is to show that if $\mathcal{C}$ is an ellipse, we can transform it to $V(x^2+y^2-1)$; if $\mathcal{C}$ is a hyperbola, we can transform it to $V(x^2-y^2-1)$; and if $\mathcal{C}$ is a parabola, we can transform it to $V(x^2-y)$. We will pass through a series of real affine transformations and appeal to Exercise 1.2.3. This result ensures that the final composition of our individual transformations is the real affine transformation we seek. This composition is, however, a mess, so we won't write it down explicitly. We will see in Section 1.10 that we can organize this information much more efficiently by using tools from linear algebra.

We begin with ellipses. Suppose $\mathcal{C} = V(ax^2+bxy+cy^2+dx+ey+h)$ is an ellipse in $\mathbb{R}^2$. Our first transformation will be to remove the xy term, i.e. to find a real affine transformation that will align our given curve with the coordinate axes. By Theorem 1.1.20 we know that $b^2-4ac<0$.

Exercise 1.2.8. Explain why if $b^2-4ac<0$, then $ac>0$.

EXERCISE 1.2.9. Show that under the real affine transformation

$$x = \sqrt{\frac{c}{a}}u + v$$

$$y = u - \sqrt{\frac{a}{c}}v$$

$\mathcal{C}$ in the xy-plane becomes an ellipse in the uv-plane whose defining equation is $Au^2 + Cv^2 + Du + Ev + H = 0$. Find A and C in terms of a, b, c. Show that if $b^2 - 4ac > 0$, then $A \neq 0$ and $C \neq 0$.

Now we have a new ellipse $V(Au^2 + Cv^2 + Du + Ev + H)$ in the uv-plane. If our original ellipse already had $b = 0$, then we would have skipped the previous step and gone directly to this one.

EXERCISE 1.2.10. Complete the square two times on the left hand side of the equation

$$Au^2 + Cv^2 + Du + Ev + H = 0$$

to rewrite this in the factored form

$$A(u - R)^2 + C(v - S)^2 - T = 0.$$

Express R, S, and T in terms of A, C, D, E, and H.

To simplify notation we revert our notation to x and y instead of u and v, but we keep in mind that we are not really still working in our original xy-plane. This is a convenience to avoid subscripts. Without loss of generality we can assume $A, C > 0$, since if $A, C < 0$ we could simply multiply the above equation by -1 without affecting the conic. Note that we assume that our original conic is an ellipse, i.e. it is nondegenerate. A consequence of this is that $T \neq 0$.

EXERCISE 1.2.11. Suppose $A, C > 0$. Find a real affine change of coordinates that maps the ellipse

$$V(A(x - R)^2 + C(y - S)^2 - T),$$

to the circle

$$V(u^2 + v^2 - 1).$$

Hence, we have found a (composition) real affine change of coordinates that transforms any ellipse $V(ax^2 + bxy + cy^2 + dx + ey + h)$ to the circle $V(u^2 + v^2 - 1)$. We can repeat this process in the case of parabolas.

Suppose $\mathcal{C} = V(ax^2 + bxy + cy^2 + dx + ey + h)$ is an parabola in $\mathbb{R}^2$. By Theorem 1.1.20 we know that $b^2 - 4ac = 0$. As before our first task is to eliminate the xy term. Suppose first that $b \neq 0$. Since $b^2 > 0$ ($b \in \mathbb{R}$) and $4ac = b^2$ we know $ac > 0$, so we repeat Exercise 1.2.9.

Exercise 1.2.12. Consider the values A and C found in Exercise 1.2.9. Show that if $b^2 - 4ac = 0$, then either $A = 0$ or $C = 0$, depending on the signs of a, b, c. [Hint: Recall, $\sqrt{\alpha^2} = -\alpha$ if $\alpha < 0$.]

Since either $A = 0$ or $C = 0$ we can assume $C = 0$ without loss of generality, so our transformed parabola is $V(Au^2 + Du + Ev + H)$ in the uv-plane. If our original parabola already had $b = 0$, then we also know, since $b^2 - 4ac$, that either $a = 0$ or $c = 0$, so we could have skipped ahead to this step.

Exercise 1.2.13. Complete the square on the left hand side of the equation

$$Au^2 + Du + Ev + H = 0$$

to rewrite this in the factored form

$$A(u - R)^2 + E(v - T) = 0.$$

Express R and T in terms of A, D, and H.

As above we revert our notation to x and y with the same caveat as before.

Exercise 1.2.14. Suppose $A, B \neq 0$. Find a real affine change of coordinates that maps the parabola

$$V(A(x - R)^2 - E(y - T)),$$

to the parabola

$$V(u^2 - v).$$

Hence, we have found a (composition) real affine change of coordinates that transforms any parabola $V(ax^2+bxy+cy^2+dx+ey+h)$ to the parabola $V(u^2-v)$. Finally, suppose $\mathcal{C} = V(ax^2 + bxy + cy^2 + dx + ey + h)$ is a hyperbola in $\mathbb{R}^2$. By Theorem 1.1.20 we know that $b^2 - 4ac > 0$. Suppose first that $b \neq 0$. Unlike before we could have $ac > 0$, $ac < 0$, or $ac = 0$.

Exercise 1.2.15. Suppose $ac > 0$. Use the real affine transformation in Exercise 1.2.9 to transform $\mathcal{C}$ to a conic in the uv-plane. Find the coefficients of u^2 and v^2 in the resulting equation and show that they have opposite signs.

Exercise 1.2.16. Suppose $ac < 0$. Use the real affine transformation

$$x = \sqrt{-\frac{c}{a}}u + v$$
$$y = u - \sqrt{-\frac{a}{c}}v$$

to transform $\mathcal{C}$ to a conic in the uv-plane. Find the coefficients of u^2 and v^2 in the resulting equation and show that they have opposite signs.

Exercise 1.2.17. Suppose $ac = 0$ (so $b \neq 0$). Since either $a = 0$ or $c = 0$ we can assume $c = 0$. Use the real affine transformation

$$x = u + v$$
$$y = u - \frac{2a}{b}v$$

to transform $\mathcal{C} = V(ax^2 + bxy + dx + ey + h)$ to a conic in the uv-plane. Find the coefficients of u^2 and v^2 in the resulting equation and show that they have opposite signs.

In all three cases we find the $\mathcal{C}$ is transformed to $V(Au^2 - Cv^2 + Du + Ev + H)$ in the uv-plane. We can now complete the hyperbolic transformation as we did above with parabolas and ellipses.

Exercise 1.2.18. Complete the square two times on the left hand side of the equation

$$Au^2 - Cv^2 + Du + Ev + H = 0$$

to rewrite this in the factored form

$$A(u - R)^2 - C(v - S)^2 - T = 0.$$

Express R, S, and T in terms of A, C, D, E, and H.

Exercise 1.2.19. Suppose $A, C > 0$. Find a real affine change of coordinates that maps the hyperbola

$$V(A(x - R)^2 - C(y - S)^2 - T),$$

to the hyperbola

$$V(u^2 - v^2 - 1).$$

We have now shown that in $\mathbb{R}^2$ we can find a real affine change of coordinates that will transform any ellipse to $V(x^2 + y^2 - 1)$, any hyperbola to $V(x^2 - y^2 - 1)$, and any parabola to $V(x^2 - y)$. Thus we have three classes of smooth conics in $\mathbb{R}^2$. Our next task is to show that these are distinct, that is, that we cannot transform an ellipse to a parabola and so on.

Exercise 1.2.20. Give an intuitive argument, based on number of connected components, for the fact that no ellipse can be transformed into a hyperbola by a real affine change of coordinates.

Exercise 1.2.21. Show that there is no real affine change of coordinates

$$u = ax + by + e$$
$$v = cx + dy + f$$

that transforms the ellipse $V(x^2 + y^2 - 1)$ to the hyperbola $V(u^2 - v^2 - 1)$.

Exercise 1.2.22. Give an intuitive argument, based on boundedness, for the fact that no parabola can be transformed into an ellipse by a real affine change of coordinates.

Exercise 1.2.23. Show that there is no real affine change of coordinates that transforms the parabola $V(x^2 - y)$ to the circle $V(u^2 + v^2 - 1)$.

Exercise 1.2.24. Give an intuitive argument, based on the number of connected components, for the fact that no parabola can be transformed into a hyperbola by a real affine change of coordinates.

Exercise 1.2.25. Show that there is no real affine change of coordinates that transforms the parabola $V(x^2 - y)$ to the hyperbola $V(u^2 - v^2 - 1)$.

Definition 1.2.2. The zero loci of two conics are *equivalent under a real affine change of coordinates* if the defining polynomial for one of the conics can be transformed via a real affine change of coordinates into the defining polynomial of the other conic.

Combining all of the work in this section, we have just proven the following theorem.

Theorem 1.2.26. Under a real affine change of coordinates, all ellipses in $\mathbb{R}^2$ are equivalent, all hyperbolas in $\mathbb{R}^2$ are equivalent, and all parabolas in $\mathbb{R}^2$ are equivalent. Further, these three classes of conics are distinct; no conic of one class can be transformed via a real affine change of coordinates to a conic of a different class.

In Section 1.10 we will revisit this theorem using tools from linear algebra. This approach will yield a cleaner and more straightforward proof than the one we have in the current setting. The linear algebraic setting will also make all of our transformations simpler, and it will become apparent how we arrived at the particular transformations.

1.3. Conics over the Complex Numbers

The goal of this section is to see how, under a complex affine changes of coordinates, all ellipses and hyperbolas are equivalent, while parabolas are still distinct.

While it is certainly natural to begin with the zero set of a polynomial $P(x, y)$ as a curve in the real plane $\mathbb{R}^2$, polynomials also have roots over the complex numbers. In fact, throughout mathematics it is almost always easier to work over the complex numbers than over the real numbers. This can be seen even in the solutions given by the quadratic equation, as seen in the following exercises:

EXERCISE 1.3.1. Show that $x^2+1=0$ has no solutions if we require $x \in \mathbb{R}$ but does have the two solutions, $x = \pm i$, in the complex numbers $\mathbb{C}$.

EXERCISE 1.3.2. Show that the set

$$\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = -1\}$$

is empty but that the set

$$\mathcal{C} = \{(x,y) \in \mathbb{C}^2 : x^2 + y^2 = -1\}$$

is not empty. If fact, show that given any complex number x that there must exist a $y \in \mathbb{C}$ such that

$$(x,y) \in \mathcal{C}.$$

Then show that if $x \neq \pm i$, then there are two distinct values $y \in \mathbb{C}$ such that $(x,y) \in \mathcal{C}$, while if $x = \pm i$, there is only one such y.

Thus if we only allow a solution to be a real number, some zero sets of second degree polynomials will be empty. This does not happen over the complex numbers.

EXERCISE 1.3.3. Let

$$P(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

with $a \neq 0$. Show that for any value $y \in \mathbb{C}$, there must be at least one $x \in \mathbb{C}$, but no more than two such x's, such that

$$P(x,y) = 0.$$

[Hint: Write $P(x,y) = Ax^2 + Bx + C$ as a function of x whose coefficients A, B, and C are themselves functions of y, and use the quadratic formula. This technique will be used frequently.]

Thus for any second order polynomial, its zero set is non-empty provided we work over the complex numbers.

But even more happens. We start with:

EXERCISE 1.3.4. Let $\mathcal{C} = V\left(\left(\frac{x^2}{4}\right) + \left(\frac{y^2}{9}\right) - 1\right) \subset \mathbb{C}^2$. Show that $\mathcal{C}$ is unbounded in both x and y. (Over the complex numbers $\mathbb{C}$, being unbounded in x, say, means, given any number M, there will be point $(x,y) \in \mathcal{C}$ such that $|x| > M$.)

Hyperbolas in $\mathbb{R}^2$ come in two pieces. In $\mathbb{C}^2$, it can be shown that hyperbolas are connected, meaning there is a continuous path from any point to any other point. The following shows this for a specific hyperbola.

EXERCISE 1.3.5. Let $\mathcal{C} = V(x^2 - y^2 - 0) \subset \mathbb{C}^2$. Show that there is a continuous path on the curve $\mathcal{C}$ from the point $(-1, 0)$ to the point $(1, 0)$, despite the fact that no such continuous path exists in $\mathbb{R}^2$. (Compare this exercise with Exercise 1.1.9.)

DEFINITION 1.3.1. A *complex affine change of coordinates* in the complex plane $\mathbb{C}^2$ is given by

$$\begin{aligned} u &= ax + by + e \\ v &= cx + dy + f, \end{aligned}$$

where $a, b, c, d, e, f \in \mathbb{C}$ and

$$ad - bc \neq 0.$$

EXERCISE 1.3.6. Show that if $u = ax + by + e$ and $v = cx + dy + f$ is a change of coordinates, then the inverse change of coordinates is

$$\begin{aligned} x &= \left(\frac{1}{ad-bc}\right)(du - bv) - \left(\frac{1}{ad-bc}\right)(de - bf) \\ y &= \left(\frac{1}{ad-bc}\right)(-cu + av) - \left(\frac{1}{ad-bc}\right)(-ce + af). \end{aligned}$$

This proof should look almost identical to the solution of Exercise 1.2.2.

DEFINITION 1.3.2. The zero loci of two conics are *equivalent under a complex affine change of coordinates* if the defining polynomial for one of the conics can be transformed via a complex affine change of coordinates into the defining polynomial for the other conic.

EXERCISE 1.3.7. Use Theorem 1.2.26 together with the new result of Exercise 1.3.6 to conclude that all ellipses and hyperbolas are equivalent under complex affine changes of coordinates.

Parabolas, though, are still different:

EXERCISE 1.3.8. Show that $\{(x, y) \in \mathbb{C}^2 : x^2 + y^2 - 1 = 0\}$ is not equivalent under a complex affine change of coordinates to the parabola $\{(u, v) \in \mathbb{C}^2 : u^2 - v = 0\}$.

We now want to look more directly at $\mathbb{C}^2$ in order to understand more clearly why the class of ellipses and the class of hyperbolas are different as real objects but the same as complex objects. We start by looking more closely at $\mathbb{C}$. Algebraic geometers regularly use the variable x for a complex number. Complex analysts more often use the variable z, which allows a complex number to be expressed in terms of its real and imaginary parts.

$$z = x + iy,$$

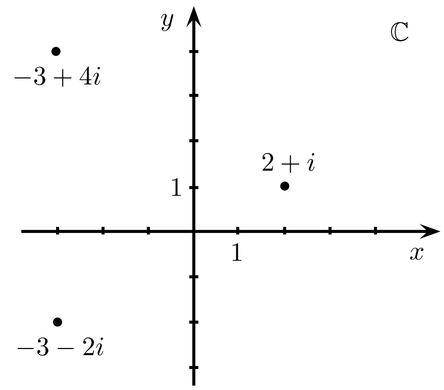


FIGURE 5. Points in the complex plane

where x is the real part of z and y is the imaginary part.

Similarly, an algebraic geometer will usually use (x, y) to denote points in the complex plane $\mathbb{C}^2$ while a complex analyst will instead use (z, w) to denote points in the complex plane $\mathbb{C}^2$. Here the complex analyst will write

$$w = u + iv.$$

There is a natural bijection from C^2 to $\mathbb{R}^4$ given by

$$(z, w) = (x + iy, u + iv) \to (x, y, u, v).$$

In the same way, there is a natural bijection from $\mathbb{C}^2 \cap \{(x, y, u, v) \in \mathbb{R}^4 : y = 0, v = 0\}$ to the real plane $\mathbb{R}^2$, given by

$$(x + 0i, u + 0i) \to (x, 0, u, 0) \to (x, u).$$

Likewise, there is a similar natural bijection from $\mathbb{C}^2 = \{(z, w) \in \mathbb{C}^2\} \cap \{(x, y, u, v) \in \mathbb{R}^4; y = 0, u = 0\}$ to $\mathbb{R}^2$, given this time by

$$(x + 0i, 0 + vi) \to (x, 0, 0, v) \to (x, v).$$

One way to think about conics in $\mathbb{C}^2$ is to consider two dimensional slices of $\mathbb{C}^2$. Let

$$\mathcal{C} = \{(z, w) \in \mathbb{C}^2 : z^2 + w^2 = 1\}.$$

EXERCISE 1.3.9. Give a bijection from

$$\mathcal{C} \cap \{(x + iy, u + iv) : x, u \in \mathbb{R}, y = 0, v = 0\}$$

to the real circle of unit radius in $\mathbb{R}^2$. (Thus a real circle in the plane $\mathbb{R}^2$ can be thought of as real slice of the complex curve $\mathcal{C}$.)

Taking a different real slice of $\mathcal{C}$ will yield not a circle but a hyperbola.

Exercise 1.3.10. Give a bijection from

$$\mathcal{C} \cap \{(x+iy, u+iv) \in \mathbb{R}^4 : x, v \in \mathbb{R}, y = 0, u = 0\}$$

to the hyperbola $(x^2 - v^2 = 1)$ in $\mathbb{R}^2$.

Thus the single complex curve $\mathcal{C}$ contains both real circles and real hyperbolas.

1.4. The Complex Projective Plane $\mathbb{P}^2$

The goal of this section is to introduce the complex projective plane $\mathbb{P}^2$, the natural ambient space (with its higher dimensional analog $\mathbb{P}^n$) for much of algebraic geometry. In $\mathbb{P}^2$, we will see that all ellipses, hyperbolas and parabolas are equivalent.

In $\mathbb{R}^2$ all ellipses are equivalent, all hyperbolas are equivalent, and all parabolas are equivalent under a real affine change of coordinates. Further, these classes of conics are distinct in $\mathbb{R}^2$. When we move to $\mathbb{C}^2$ ellipses and hyperbolas are equivalent under a complex affine change of coordinates, but parabolas remain distinct. The next step is to understand the "points at infinity" in $\mathbb{C}^2$.

We will give the definition for the complex projective plane $\mathbb{P}^2$ together with exercises to demonstrate its basic properties. It may not be immediately clear what this definition has to do with the "ordinary" complex plane $\mathbb{C}^2$. We will then see how $\mathbb{C}^2$ naturally lives in $\mathbb{P}^2$ and how the "extra" points in $\mathbb{P}^2$ that are not in $\mathbb{C}^2$ are viewed as points at infinity. In the next section we will look at the projective analogue of change of coordinates and see how we can view all ellipses, hyperbolas and parabolas as equivalent.

Definition 1.4.1. Define a relation $\sim$ on points in $\mathbb{C}^3 - \{(0,0,0)\}$ as follows: $(x, y, z) \sim (u, v, w)$ if and only if there exists $\lambda \in \mathbb{C} - \{0\}$ such that $(x, y, z) = (\lambda u, \lambda v, \lambda w)$.

Exercise 1.4.1. Show that $\sim$ is an equivalence relation.

Exercise 1.4.2.

(1) Show that $(2, 1+i, 3i) \sim (2-2i, 2, 3+3i)$.
(2) Show that $(1,2,3) \sim (2,4,6) \sim (-2,-4,-6) \sim (-i,-2i,-3i)$.
(3) Show that $(2, 1+i, 3i) \not\sim (4, 4i, 6i)$.
(4) Show that $(1,2,3) \not\sim (3,6,8)$.

Exercise 1.4.3. Suppose that $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ and that $x_1 = x_2$. Show then that $y_1 = y_2$ and $z_1 = z_2$.

EXERCISE 1.4.4. Suppose that $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ with $z_1 \neq 0$ and $z_2 \neq 0$. Show that

$$(x_1, y_1, z_1) \sim \left(\frac{x_1}{z_1}, \frac{y_1}{z_1}, 1\right) \sim \left(\frac{x_2}{z_2}, \frac{y_2}{z_2}, 1\right) \sim (x_2, y_2, z_2).$$

Let $(x : y : z)$ denote the equivalence class of (x, y, z), i.e. $(x : y : z)$ is the following set.

$$(x : y : z) = \{(u, v, w) \in \mathbb{C}^3 - \{(0, 0, 0)\} : (x, y, z) \sim (u, v, w)\}$$

EXERCISE 1.4.5. (1) Find the equivalence class of $(0, 0, 1)$.
(2) Find the equivalence class of $(1, 2, 3)$.

EXERCISE 1.4.6. Show that the equivalence classes $(1 : 2 : 3)$ and $(2 : 4 : 6)$ are equal as sets.

DEFINITION 1.4.2. The *complex projective plane,* $\mathbb{P}^2(\mathbb{C})$, is the set of equivalence classes of the points in $\mathbb{C}^3 - \{(0, 0, 0)\}$. That is,

$$\mathbb{P}^2(\mathbb{C}) = \left(\mathbb{C}^3 - \{(0, 0, 0)\}\right) \Big/ \sim .$$

The set of points $\{(x : y : z) \in \mathbb{P}^2(\mathbb{C}) : z = 0\}$ is called the *line at infinity.* We will write $\mathbb{P}^2$ to mean $\mathbb{P}^2(\mathbb{C})$ when the context is clear.

Let $(a, b, c) \in \mathbb{C}^3 - \{(0, 0, 0)\}$. Then the complex line through this point and the origin $(0, 0, 0)$ can be defined as all points, (x, y, z), satisfying

$$x = \lambda a, \ y = \lambda b, \text{ and } z = \lambda c,$$

for any complex number λ. Here λ can be thought of as an independent parameter.

EXERCISE 1.4.7. Explain why the elements of $\mathbb{P}^2$ can intuitively be thought of as complex lines through the origin in $\mathbb{C}^3$.

EXERCISE 1.4.8. If $c \neq 0$, show, in $\mathbb{C}^3$, that the line $x = \lambda a, \ y = \lambda b, \ z = \lambda c$ intersects the plane $\{(x, y, z) : z = 1\}$ in exactly one point. Show that this point of intersection is $\left(\frac{a}{c}, \frac{b}{c}, 1\right)$.

In the next several exercises we will use

$$\mathbb{P}^2 = \{(x : y : z) \in \mathbb{P}^2 : z \neq 0\} \cup \{(x : y : z) \in \mathbb{P}^2 : z = 0\}$$

to show that $\mathbb{P}^2$ can be viewed as the union of $\mathbb{C}^2$ with the line at infinity.

EXERCISE 1.4.9. Show that the map $\phi : \mathbb{C}^2 \to \{(x : y : z) \in \mathbb{P}^2 : z \neq 0\}$ defined by $\phi(x, y) = (x : y : 1)$ is a bijection.

EXERCISE 1.4.10. Find a map from $\{(x : y : z) \in \mathbb{P}^2 : z \neq 0\}$ to $\mathbb{C}^2$ that is the inverse of the map ϕ in Exercise 1.4.9.

The maps ϕ and ϕ^{-1} in Exercises 1.4.9 and 1.4.10 show us how to view $\mathbb{C}^2$ inside $\mathbb{P}^2$. Now we show how the set $\{(x : y : z) \in \mathbb{P}^2 : z = 0\}$ corresponds to directions towards infinity in $\mathbb{C}^2$.

Exercise 1.4.11. Consider the line $\ell = \{(x, y) \in \mathbb{C}^2 : ax + by + c = 0\}$ in $\mathbb{C}^2$. Assume $a, b \neq 0$. Explain why, as $|x| \to \infty$, $|y| \to \infty$. (Here, $|x|$ is the modulus of x.)

Exercise 1.4.12. Consider again the line ℓ. We know that a and b cannot both be 0, so we will assume without loss of generality that $b \neq 0$.

(1) Show that the image of ℓ in $\mathbb{P}^2$ under ϕ is the set
$$\{(bx : -ax - c : b) : x \in \mathbb{C}\}.$$
(2) Show that this set equals the following union.
$$\{(bx : -ax - c : b) : x \in \mathbb{C}\} = \{(0 : -c : b)\} \cup \left\{ \left(1 : -\frac{a}{b} - \frac{c}{bx} : \frac{1}{x}\right) \right\}$$
(3) Show that as $|x| \to \infty$, the second set in the above union becomes
$$\{(1 : -\frac{a}{b} : 0)\}.$$

Thus, the points $(1 : -\frac{a}{b} : 0)$ are directions toward infinity and the set $\{(x : y : z) \in \mathbb{P}^2 : z = 0\}$ is the *line at infinity*.

If a point $(a : b : c)$ in $\mathbb{P}^2$ is the image of a point $(x, y) \in \mathbb{C}^2$ under the map from $\mathbb{C}^2 \xrightarrow{\phi} \mathbb{P}^2$, we say that $(a, b, c) \in \mathbb{C}^3$ are the *homogeneous coordinates* for (x, y). Notice that the homogeneous coordinates for a point $(x, y) \in \mathbb{C}^2$ are not unique. For example, the coordinates $(2 : -3 : 1)$, $(10 : -15 : 5)$, and $(2-2i : -3+3i : 1-i)$ are all homogeneous coordinates for $(2, -3)$.

In order to consider zero sets of polynomials in $\mathbb{P}^2$, a little care is needed. We start with:

Definition 1.4.3. A polynomial is *homogeneous* if every monomial term has the same total degree, that is, if the sum of the exponents in every monomial is the same. The *degree* of the homogeneous polynomial is the degree of one of its monomials. An equation is homogeneous if every nonzero monomial has the same total degree.

Exercise 1.4.13. Explain why the following polynomials are homogeneous, and find each degree.

(1) $x^2 + y^2 - z^2$
(2) $xz - y^2$
(3) $x^3 + 3xy^2 + 4y^3$
(4) $x^4 + x^2y^2$

EXERCISE 1.4.14. Explain why the following polynomials are not homogeneous.

(1) $x^2 + y^2 - z$
(2) $xz - y$
(3) $x^2 + 3xy^2 + 4y^3 + 3$
(4) $x^3 + x^2y^2 + x^2$

EXERCISE 1.4.15. Show that if the homogeneous equation $Ax + By + Cz = 0$ holds for the point (x, y, z) in $\mathbb{C}^3$, then it holds for every point of $\mathbb{C}^3$ that belongs to the equivalence class $(x : y : z)$ in $\mathbb{P}^2$.

EXERCISE 1.4.16. Show that if the homogeneous equation $Ax^2 + By^2 + Cz^2 + Dxy + Exz + Fyz = 0$ holds for the point (x, y, z) in $\mathbb{C}^3$, then it holds for every point of $\mathbb{C}^3$ that belongs to the equivalence class $(x : y : z)$ in $\mathbb{P}^2$.

EXERCISE 1.4.17. State and prove the generalization of the previous two exercises for any degree n homogeneous equation $P(x, y, z) = 0$.

EXERCISE 1.4.18. Consider the non-homogeneous equation $P(x, y, z) = x^2 + 2y + 2z = 0$. Show that $(2, -1, -1)$ satisfies this equation, but not all other points of the equivalence class $(2 : -1 : -1)$ satisfy the equation.

Thus the zero set of a non-homogeneous polynomials is not well- defined in $\mathbb{P}^2$. These exercises demonstrate that the only polynomials that are well-defined on $\mathbb{P}^2$ (and any projective space $\mathbb{P}^n$) are homogeneous polynomials.

In order to study the behavior at infinity of a curve in $\mathbb{C}^2$, we would like to extend the curve to $\mathbb{P}^2$. In order for the zero set of a polynomial over $\mathbb{P}^2$ to be well-defined we must, for any given a polynomial on $\mathbb{C}^2$, replace the original (possibly non-homogeneous) polynomial with a homogeneous one. For any point $(x : y : z) \in \mathbb{P}^2$ with $z \neq 0$ we have $(x : y : z) \sim \left(\frac{x}{z} : \frac{y}{z} : 1\right)$ which we identify, via ϕ^{-1} from Exercise 1.4.10, with the point $\left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{C}^2$. This motivates our procedure to *homogenize* polynomials.

We start with an example. With a slight abuse of notation, the polynomial $P(x, y) = y - x - 2$ maps to $P(x, y, z) = \frac{y}{z} - \frac{x}{z} - 2$. Since $P(x, y, z) = 0$ and $zP(x, y, z) = 0$ have the same zero set if $z \neq 0$ we clear the denominator and consider the polynomial $P(x, y, z) = y - x - 2z$. The zero set of $P(x, y, z) = y - x - 2z$ in $\mathbb{P}^2$ corresponds to the zero set of $P(x, y) = y - x - 2 = 0$ in $\mathbb{C}^2$ precisely when $z = 1$.

Similarly, the polynomial $x^2 + y^2 - 1$ maps to $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 - 1$. Again, clear the denominators to obtain the homogeneous polynomial $x^2 + y^2 - z^2$, whose zero set, $V(x^2 + y^2 - z^2) \subset \mathbb{P}^2$ corresponds to the zero set, $V(x^2 + y^2 - 1) \subset \mathbb{C}^2$ when $z = 1$.

Definition 1.4.4. Let $P(x,y)$ be a degree n polynomial defined over $\mathbb{C}^2$. The corresponding homogeneous polynomial defined over $\mathbb{P}^2$ is

$$P(x,y,z) = z^n P\left(\frac{x}{z}, \frac{y}{z}\right).$$

Exercise 1.4.19. Homogenize the following equations. Then find the point(s) where the curves intersect the line at infinity.

(1) $ax + by + c = 0$
(2) $x^2 + y^2 = 1$
(3) $y = x^2$
(4) $x^2 + 9y^2 = 1$
(5) $y^2 - x^2 = 1$

Exercise 1.4.20. Show that in $\mathbb{P}^2$, any two distinct lines will intersect in a point. Notice, this implies that parallel lines in $\mathbb{C}^2$, when embedded in $\mathbb{P}^2$, intersect at the line at infinity.

Exercise 1.4.21. Once we have homogenized an equation, the original variables x and y are no more important than the variable z. Suppose we regard x and z as the original variables in our homogenized equation. Then the image of the xz-plane in $\mathbb{P}^2$ would be $\{(x:y:z) \in \mathbb{P}^2 : y = 1\}$.

(1) Homogenize the equations for the parallel lines $y = x$ and $y = x + 2$.
(2) Now regard x and z as the original variables, and set $y = 1$ to sketch the image of the lines in the xz-plane.
(3) Explain why the lines in part (2) meet at the $x-$axis.

1.5. Projective Change of Coordinates

The goal of this section is to define a projective change of coordinates and then show that all ellipses, hyperbolas and parabolas are equivalent under a projective change of coordinates.

Earlier we described a complex affine change of coordinates from $\mathbb{C}^2$ with points (x,y) to $\mathbb{C}^2$ with points (u,v) by setting $u = ax + bx + e$ and $v = cx + dy + f$. We will define the analog for changing homogeneous coordinates $(x:y:z)$ for some $\mathbb{P}^2$ to homogeneous coordinates $(u:v:w)$ for another $\mathbb{P}^2$. We need the change of coordinates equations to be both homogeneous and linear:

Definition 1.5.1. A projective change of coordinates is given by

$$u = a_{11}x + a_{12}y + a_{13}z$$

$$v = a_{21}x + a_{22}y + a_{23}z$$

$$w = a_{31}x + a_{32}y + a_{33}z$$

where the $a_{ij} \in \mathbb{C}$ and

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \neq 0.$$

In matrix language

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

where $A = (a_{ij})$, $a_{ij} \in \mathbb{C}$, and $\det A \neq 0$.

DEFINITION 1.5.2. Two conics in $\mathbb{P}^2$ are *equivalent under a projective change of coordinates*, or *projectively equivalent*, if the defining homogeneous polynomial for one of the conics can be transformed into the defining polynomial for the other conic via a projective change of coordinates.

EXERCISE 1.5.1. For the complex affine change of coordinates

$$u = ax + by + e$$
$$v = cx + dy + f,$$

where $a, b, c, d, e, f \in \mathbb{C}$ and $ad - bc \neq 0$, show that

$$u = ax + by + ez$$
$$v = cx + dy + fz$$
$$w = z$$

is the corresponding projective change of coordinates.

This means that if two conics in $\mathbb{C}^2$ are equivalent under a complex affine change of coordinates, then the corresponding conics in $\mathbb{P}^2$ will still be equivalent, but now under a projective change of coordinates.

EXERCISE 1.5.2. Let $\mathcal{C}_1 = V(x^2 + y^2 - 1)$ be an ellipse in $\mathbb{C}^2$ and let $\mathcal{C}_2 = V(u^2 - v)$ be a parabola in $\mathbb{C}^2$. Homogenize the defining polynomials for $\mathcal{C}_1$ and $\mathcal{C}_2$ and show that the projective change of coordinates

$$u = ix$$
$$v = y + z$$
$$w = y - z$$

transforms the ellipse in $\mathbb{P}^2$ into the parabola in $\mathbb{P}^2$.

EXERCISE 1.5.3. Use the results of Section 1.3 together with the above problem to show that, under a projective change of coordinates, all ellipses, hyperbolas, and parabolas are equivalent in $\mathbb{P}^2$.

1.6. The Complex Projective Line $\mathbb{P}^1$

The goal of this section is to define the complex projective line $\mathbb{P}^1$ and show that it can be viewed topologically as a sphere. In the next section we will use this to show that ellipses, hyperbolas, and parabolas are also spheres in the complex projective plane $\mathbb{P}^2$.

We start with the definition of $\mathbb{P}^1$:

DEFINITION 1.6.1. Define an equivalence relation $\sim$ on points in $\mathbb{C}^2 - \{(0,0)\}$ as follows: $(x, y) \sim (u, v)$ if and only if there exists $\lambda \in \mathbb{C} - \{0\}$ such that $(x, y) = (\lambda u, \lambda v)$. Let $(x : y)$ denote the equivalence class of (x, y). The *complex projective line* $\mathbb{P}^1$ is the set of equivalence classes of points in $\mathbb{C}^2 - \{(0,0)\}$. That is,

$$\mathbb{P}^1 = \left(\mathbb{C}^2 - \{(0,0)\}\right) \Big/ \sim .$$

The point $(1 : 0)$ is called the *point at infinity*.

The next series of problems are direct analogs of problems for $\mathbb{P}^2$.

EXERCISE 1.6.1. Suppose that $(x_1, y_1) \sim (x_2, y_2)$ and that $x_1 = x_2 \neq 0$. Show that $y_1 = y_2$.

EXERCISE 1.6.2. Suppose that $(x_1, y_1) \sim (x_2, y_2)$ with $y_1 \neq 0$ and $y_2 \neq 0$. Show that

$$(x_1, y_1) \sim \left(\frac{x_1}{y_1}, 1\right) \sim \left(\frac{x_2}{y_2}, 1\right) \sim (x_2, y_2).$$

EXERCISE 1.6.3. Explain why the elements of $\mathbb{P}^1$ can intuitively be thought of as complex lines through the origin in $\mathbb{C}^2$.

EXERCISE 1.6.4. If $b \neq 0$, show, in $\mathbb{C}^2$, that the line $x = \lambda a$, $y = \lambda b$ will intersect the plane $\{(x, y) : y = 1\}$ in exactly one point. Show that this point of intersection is $\left(\frac{a}{b}, 1\right)$.

We have that

$$\mathbb{P}^1 = \{(x : y) \in \mathbb{P}^1 : y \neq 0\} \cup \{(1 : 0)\}.$$

EXERCISE 1.6.5. Show that the map $\phi : \mathbb{C} \to \{(x : y) \in \mathbb{P}^1 : y \neq 0\}$ defined by $\phi(x) = (x : 1)$ is a bijection.

EXERCISE 1.6.6. Find a map from $\{(x : y) \in \mathbb{P}^1 : y \neq 0\}$ to $\mathbb{C}$ that is the inverse of the map ϕ in Exercise 1.6.5.

The maps ϕ and ϕ^{-1} in Exercises 1.6.5 and 1.6.6 show us how to view $\mathbb{C}$ inside $\mathbb{P}^1$. Now we want to see how the extra point $(1:0)$ will correspond to the point at infinity of $\mathbb{C}$.

inverse of the map in the previous problem.

EXERCISE 1.6.7. Consider the map $\phi : \mathbb{C} \to \mathbb{P}^1$ given by $\phi(x) = (x:1)$. Show that as $|x| \to \infty$, we have $\phi(x) \to (1:0)$.

Hence we can think of $\mathbb{P}^1$ as the union of $\mathbb{C}$ and a single point at infinity. Now we want to see how we can regard $\mathbb{P}^1$ as a sphere, which means we want to find a homeomorphism between $\mathbb{P}^1$ and a sphere. A *homeomorphism* is a continuous map with a continuous inverse. Two spaces are topologically equivalent, or homeomorphic, if we can find a homeomorphism from one to the other. We know that the points of $\mathbb{C}$ are in one-to-one correspondence with the points of the real plane $\mathbb{R}^2$, so we will first work in $\mathbb{R}^2 \subset \mathbb{R}^3$. Let S^2 denote the unit sphere in $\mathbb{R}^3$ centered at the origin. This sphere is given by the equation

$$x^2 + y^2 + z^2 = 1.$$

EXERCISE 1.6.8. Let p denote the point $(0,0,1) \in S^2$, and let ℓ denote the line through p and the point $(x,y,0)$ in the xy-plane, whose parametrization is given by

$$\gamma(t) = (1-t)(0,0,1) + t(x,y,0),$$

i.e.

$$l = \{(tx, ty, 1-t) \mid t \in \mathbb{R}\}.$$

(1) ℓ clearly intersects S^2 at the point p. Show that there is exactly one other point of intersection q.
(2) Find the coordinates of q.
(3) Define the map $\psi : \mathbb{R}^2 \to S^2 - \{p\}$ to be the map that takes the point (x,y) to the point q. Show that ψ is a continuous bijection.
(4) Show that as $|(x,y)| \to \infty$, we have $\psi(x,y) \to p$.

The above argument does establish a homeomorphism, but it relies on coordinates and an embedding of the sphere in $\mathbb{R}^3$. We now give an alternative method for showing that $\mathbb{P}^1$ is a sphere that does not rely as heavily on coordinates.

If we take a point $(x:y) \in \mathbb{P}^1$, then we can choose a representative for this point of the form $\left(\frac{x}{y} : 1\right)$, provided $y \neq 0$, and a representative of the form $\left(1 : \frac{y}{x}\right)$, provided $x \neq 0$.

EXERCISE 1.6.9. Determine which point(s) in $\mathbb{P}^1$ do **not** have two representatives of the form $(x:1) = (1:\frac{1}{x})$.

Our constructions needs two copies of $\mathbb{C}$. Let U denote the first copy of $\mathbb{C}$, whose elements are denoted by x. Let V be the second copy of $\mathbb{C}$, whose elements we'll denote y. Further let $U^* = U - \{0\}$ and $V^* = V - \{0\}$.

Exercise 1.6.10. Map $U \to \mathbb{P}^1$ via $x \to (x : 1)$ and map $V \to \mathbb{P}^1$ via $y \to (1 : y)$. Show that there is a the natural one-to-one map $U^* \to V^*$.

The next two exercises have quite a different flavor than most of the problems in the book. The emphasis is not on calculations but on the underlying intuitions.

Exercise 1.6.11. A sphere can be split into a neighborhood of its northern hemisphere and a neighborhood of its southern hemisphere. Show that a sphere can be obtained by correctly gluing together two copies of $\mathbb{C}$.

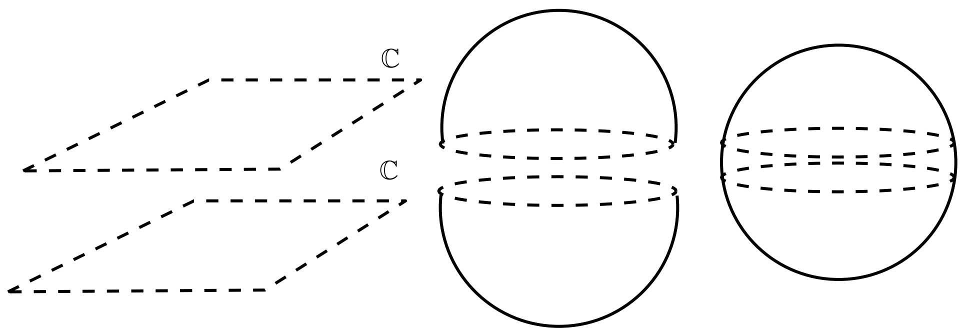


Figure 6. gluing copies of $\mathbb{C}$ together

Exercise 1.6.12. Put together the last two exercises to show that $\mathbb{P}^1$ is topologically equivalent to a sphere.

1.7. Ellipses, Hyperbolas, and Parabolas as Spheres

The goal of this section is to show that there is always a bijective polynomial map from $\mathbb{P}^1$ to any ellipse, hyperbola, or parabola. Since we showed in the last section that $\mathbb{P}^1$ is topologically equivalent to a sphere, this means that all ellipses, hyperbolas, and parabolas are spheres.

1.7.1. Rational Parameterizations of Smooth Conics. We start with rational parameterizations of conics. While we will consider conics in the complex plane $\mathbb{C}^2$, we often draw these conics in $\mathbb{R}^2$. Part of learning algebraic geometry is developing a sense for when the real pictures capture what is going on in the complex plane.

Consider a conic $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 : P(x, y) = 0\} \subset \mathbb{C}^2$ where $P(x, y)$ is a second degree polynomial. Our goal is to parametrize $\mathcal{C}$ with polynomial or rational maps.

This means we want to find a map $\phi : \mathbb{C} \to \mathcal{C} \subset \mathbb{C}^2$, given by $\phi(\lambda) = (x(\lambda), y(\lambda))$ such that $x(\lambda)$ and $y(\lambda)$ are polynomials or rational functions. In the case of a parabola, for example when $P(x, y) = x^2 - y$, it is easy to find a bijection from $\mathbb{C}$ to the conic $\mathcal{C}$.

EXERCISE 1.7.1. Find a bijective polynomial map from $\mathbb{C}$ to the conic $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 : x^2 - y = 0\}$.

On the other hand, it may be easy to find a parametrization but not a rational parametrization.

EXERCISE 1.7.2. Let $\mathcal{C} = V(x^2 + y^2 - 1)$ be an ellipse in $\mathbb{C}^2$.

(1) Find a trigonometric parametrization of $\mathcal{C}$.
(2) For any point $(x, y) \in \mathcal{C}$, express the variable x as a function of y involving a square root. Use this to find another parametrization of $\mathcal{C}$.

The exercise above gives two parameterizations for the circle but in algebraic geometry we restrict our maps to polynomial or rational maps. We develop a standard method, similar to the method developed in Exercise 1.6.8, to find such a parameterization below.

EXERCISE 1.7.3. Consider the ellipse $\mathcal{C} = V(x^2 + y^2 - 1) \subset \mathbb{C}^2$ and let p denote the point $(0, 1) \in \mathcal{C}$.

(1) Parametrize the line segment from p to the point $(\lambda, 0)$ on the complex line $y = 0$ as in Exercise 1.6.8.
(2) This line segment clearly intersects $\mathcal{C}$ at the point p. Show that if $\lambda \neq \pm i$, then there is exactly one other point of intersection. Call this point q.
(3) Find the coordinates of $q \in \mathcal{C}$.
(4) Show that if $\lambda = \pm i$, then the line segment intersects $\mathcal{C}$ at p only.

Define the map $\widetilde{\psi} : \mathbb{C} \to \mathcal{C} \subset \mathbb{C}^2$ by

$$\widetilde{\psi}(\lambda) = \left(\frac{2\lambda}{\lambda^2 + 1}, \frac{\lambda^2 - 1}{\lambda^2 + 1} \right).$$

But we want to work in projective space. This means that we have to homogenize our map.

EXERCISE 1.7.4. Show that the above map can be extended to the map $\psi : \mathbb{P}^1 \to \{(x : y : z) \in \mathbb{P}^2 : x^2 + y^2 - z^2 = 0\}$ given by

$$\psi(\lambda : \mu) = (2\lambda\mu : \lambda^2 - \mu^2 : \lambda^2 + \mu^2).$$

EXERCISE 1.7.5.

(1) Show that the map ψ is one-to-one.

(2) Show that ψ is onto. [Hint: Consider two cases: $z \neq 0$ and $z = 0$. For $z \neq 0$ follow the construction given above. For $z = 0$, find values of λ and μ to show that these point(s) are given by ψ. How does this relate to Part 4 of Exercise 1.7.3?]

Since we already know that every ellipse, hyperbola, and parabola is projectively equivalent to the conic defined by $x^2 + y^2 - z^2 = 0$, we have, by composition, a one-to-one and onto map from $\mathbb{P}^1$ to any ellipse, hyperbola or parabola.

But we can construct such maps directly. Here is what we can do for any conic $\mathcal{C}$. Fix a point p on $\mathcal{C}$, and parametrize the line segment through p and the point $(x, 0)$. We use this to determine another point on curve $\mathcal{C}$, and the coordinates of this point give us our map.

EXERCISE 1.7.6. For the following conics, for the given point p, follow what we did for the conic $x^2 + y^2 - 1 = 0$ to find a rational map from $\mathbb{C}$ to the curve in $\mathbb{C}^2$ and then a one-one map from $\mathbb{P}^1$ onto the conic in $\mathbb{P}^2$.

(1) $x^2 + 2x - y^2 - 4y - 4 = 0$ with $= (0, -2)$.
(2) $3x^2 + 3y^2 - 75 = 0$ with $p = (5, 0)$.
(3) $4x^2 + y^2 - 8 = 0$ with $p = (1, 2)$.

1.7.2. Links to Number Theory. The goal of this section is to see how geometry can be used to find all primitive Pythagorean triples, a number theory problem.

Overwhelmingly in this book we will be interested in working over the complex numbers. But if instead we work over the integers or the rational numbers, some of the deepest questions in mathematics appear. We want to see this approach in the case of conics.

In particular we want to link the last section to the search for primitive Pythagorean triples. A *Pythagorean triple* is a triple, (x, y, z), of integers that satisfies the equation

$$x^2 + y^2 = z^2.$$

EXERCISE 1.7.7. Suppose (x_0, y_0, z_0) is a solution to $x^2 + y^2 = z^2$. Show that (mx_0, my_0, mz_0) is also a solution for any scalar m.

A primitive Pythagorean triple is a Pythagorean triple that cannot be obtained by multiplying another Pythagorean triple by an integer.

The simplest example, after the trivial solution $(0, 0, 0)$, is $(3, 4, 5)$. These triples get their name from the attempt to find right triangles with integer length sides, x, y, and z. We will see that the previous section gives us a method to compute all possible primitive Pythagorean triples.

We first see how to translate the problem of finding integer solutions of $x^2+y^2 = z^2$ to finding rational number solutions to $x^2 + y^2 = 1$.

EXERCISE 1.7.8. Let $(a, b, c) \in \mathbb{Z}^3$ be a solution to $x^2 + y^2 = z^2$. Show that $c = 0$ if and only if $a = b = 0$.

This means that we can assume $c \neq 0$, since there can be only one solution when $c = 0$.

EXERCISE 1.7.9. Show that if (a, b, c) is a Pythagorean triple, with $c \neq 0$, then the pair of rational numbers $\left(\frac{a}{c}, \frac{b}{c}\right)$ is a solution to $x^2 + y^2 = 1$.

EXERCISE 1.7.10. Let $\left(\frac{a}{c_1}, \frac{b}{c_2}\right) \in \mathbb{Q}^2$ be a rational solution to $x^2 + y^2 = 1$. Find a corresponding Pythagorean triple.

Thus to find Pythagorean triples, we want to find the rational points on the curve $x^2 + y^2 = 1$. We denote these points as

$$\mathcal{C}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\}.$$

Recall, from the last section, the parameterization $\widetilde{\psi} : \mathbb{Q} \to \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\}$ given by

$$\lambda \xrightarrow{\widetilde{\psi}} \left(\frac{2\lambda}{\lambda^2 + 1}, \frac{\lambda^2 - 1}{\lambda^2 + 1}\right).$$

EXERCISE 1.7.11. Show that the above map $\widetilde{\psi}$ sends $\mathbb{Q} \to \mathcal{C}(\mathbb{Q})$.

Extend this to a map $\psi : \mathbb{P}^1(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{Q})$ by

$$(\lambda : \mu) \mapsto (2\lambda\mu : \lambda^2 - \mu^2 : \lambda^2 + \mu^2),$$

where $\lambda, \mu \in \mathbb{Z}$.

Since we know already that the map ψ is one-to-one by Exercise 1.7.5, this give us a way to produce an infinite number of integer solutions to $x^2 + y^2 = z^2$.

EXERCISE 1.7.12. Show that λ and μ are relatively prime if and only if $\psi(\lambda : \mu)$ is a primitive Pythagorean triple.

Thus it makes sense for us to work in projective space since we are only interested in primitive Pythagorean triples.

We now want to show that the map ψ is onto so that we actually obtain all primitive Pythagorean triples.

EXERCISE 1.7.13.

(1) Show that $\psi : \mathbb{P}^1(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{Q})$ is onto.
(2) Show that every primitive Pythagorean triple is of the form $(2\lambda\mu, \lambda^2 - \mu^2, \lambda^2 + \mu^2)$, where $\lambda, \mu \in \mathbb{Z}$ are relatively prime.

EXERCISE 1.7.14. Find a rational point on the conic $x^2 + y^2 - 2 = 0$. Develop a parameterization and conclude that there are infinitely many rational points on this curve.

EXERCISE 1.7.15. By mimicking the above, find four rational points on each of the following conics.

(1) $x^2 + 2x - y^2 - 4y - 4 = 0$ with $p = (0, -2)$.
(2) $3x^2 + 3y^2 - 75 = 0$ with $p = (5, 0)$.
(3) $4x^2 + y^2 - 8 = 0$ with $p = (1, 2)$.

EXERCISE 1.7.16. Show that the conic $x^2 + y^2 = 3$ has no rational points.

Diophantine problems are those where you try to find integer or rational solutions to a polynomial equation. The work in this section shows how we can approach such problems using algebraic geometry. For higher degree equations the situation is quite different and leads to the heart of a great deal of the current research in number theory.

1.8. Degenerate Conics - Crossing lines and double lines.

The goal of this section is to extend our study of conics from ellipses, hyperbolas and parabolas to the "degenerate" conics: crossing lines and double lines.

Let $f(x, y, z)$ be any homogeneous second degree polynomial with complex coefficients. The overall goal of this chapter is to understand curves

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : f(x, y, z) = 0\}.$$

Most of these curves will be various ellipses, hyperbolas and parabolas. But consider the second degree polynomial

$$f(x, y, z) = (-x + y + z)(2x + y + 3z) = -2x^2 + y^2 + 3z^2 + xy - xz + 4yz.$$

EXERCISE 1.8.1. Dehomogenize $f(x, y, z)$ by setting $z = 1$. Graph the curve

$$\mathcal{C}(\mathbb{R}) = \{(x : y : z) \in \mathbb{P}^2 : f(x, y, 1) = 0\}$$

in the real plane $\mathbb{R}^2$.

The zero set of a second degree polynomial could be the union of crossing lines.

EXERCISE 1.8.2. Consider the two lines given by

$$(a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) = 0,$$

and suppose

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \neq 0.$$

Show that the two lines intersect at a point where $z \neq 0$.

EXERCISE 1.8.3. Dehomogenize the equation in the previous exercise by setting $z = 1$. Give an argument that, as lines in the complex plane $\mathbb{C}$, they have distinct slopes.

EXERCISE 1.8.4. Again consider the two lines

$$(a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) = 0,$$

where at least one of $a_1, b_1,$ or c_1 is nonzero and at least one of $a_2, b_2,$ or c_2 is nonzero. (This is to guarantee that $(a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z)$ is actually second order.) Now suppose that

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = 0$$

and that

$$\det \begin{pmatrix} a_1 & c_1 \\ a_2 & c_2 \end{pmatrix} \neq 0 \text{ or } \det \begin{pmatrix} b_1 & c_1 \\ b_2 & c_2 \end{pmatrix} \neq 0.$$

Show that the two lines still have one common point of intersection, but that this point must have $z = 0$.

There is one other possibility. Consider the zero set

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : (ax + by + cz)^2 = 0\}.$$

As a zero set, the curve $\mathcal{C}$ is geometrically the line

$$ax + by + cz = 0$$

but due to the exponent 2, we call $\mathcal{C}$ a *double line*.

EXERCISE 1.8.5. Let

$$f(x, y, z) = (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z),$$

where at least one of $a_1, b_1,$ or c_1 is nonzero and at least one of the $a_2, b_2,$ or c_2 is nonzero. Show that the curve defined by $f(x, y, z) = 0$ is a double line if and only if

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = 0, \quad \det \begin{pmatrix} a_1 & c_1 \\ a_2 & c_2 \end{pmatrix} = 0, \quad \text{and } \det \begin{pmatrix} b_1 & c_1 \\ b_2 & c_2 \end{pmatrix} = 0.$$

We now want to show that any two crossing lines are equivalent under a projective change of coordinates to any other two crossing lines and any double line is equivalent under a projective change of coordinates to any other double line. This means that there are precisely three types of conics: the ellipses, hyperbolas, and parabolas; pairs of lines; and double lines.

For the exercises that follow, assume that at least one of $a_1, b_1,$ or c_1 is nonzero and at least one of $a_2, b_2,$ or c_2 is nonzero.

EXERCISE 1.8.6. Consider the crossing lines

$$(a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) = 0,$$

with

$$\det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \neq 0.$$

Find a projective change of coordinates from xyz-space to uvw-space so that the crossing lines become

$$uv = 0.$$

EXERCISE 1.8.7. Consider the crossing lines $(a_1x+b_1y+c_1z)(a_2x+b_2y+c_2z) = 0$, with

$$\det \begin{pmatrix} a_1 & c_1 \\ a_2 & c_2 \end{pmatrix} \neq 0.$$

Find a projective change of coordinates from xyz-space to uvw-space so that the crossing lines become

$$uv = 0.$$

EXERCISE 1.8.8. Show that there is a projective change of coordinates from xyz-space to uvw-space so that the double line $(ax + by + cz)^2 = 0$ becomes the double line

$$u^2 = 0.$$

EXERCISE 1.8.9. Argue that there are three distinct classes of conics in $\mathbb{P}^2$.

1.9. Tangents and Singular Points

The goal of this section is to develop the idea of singularity. We'll show that all ellipses, hyperbolas, and parabolas are smooth, while crossing lines and double lines are singular, but in different ways.

Thus far, we have not explicitly needed Calculus; to discuss singularities we will need to use Calculus. We have been working over both real and complex numbers throughout. For all of our differentiation we will use the familiar differentiation rules from real calculus, but we note that the underlying details involved in complex differentiation are more involved than in the differentiation of real-valued functions. See the appendix on complex analysis for further details.

Let $f(x,y)$ be a polynomial. Recall that if $f(a,b)=0$, then the normal vector for the curve $f(x,y)=0$ at the point (a,b) is given by the gradient vector

$$\nabla f(a,b) = \left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)\right).$$

A tangent vector to the curve at the point (a,b) is perpendicular to $\nabla f(a,b)$ and hence must have a dot product of zero with $\nabla f(a,b)$. This observation shows that the tangent line is given by

$$\{(x,y) \in \mathbb{C}^2 : \left(\frac{\partial f}{\partial x}(a,b)\right)(x-a) + \left(\frac{\partial f}{\partial y}(a,b)\right)(y-b) = 0\}.$$

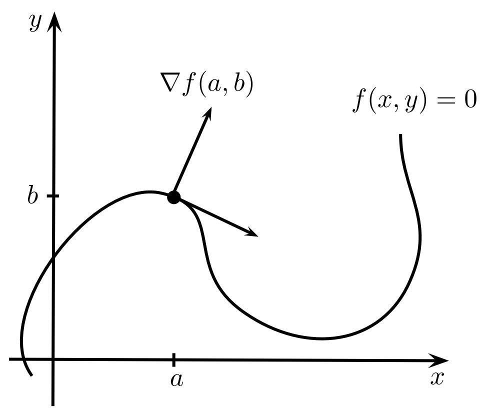


FIGURE 7. gradient versus tangent vectors

EXERCISE 1.9.1. Explain why if both $\frac{\partial f}{\partial x}(a,b)=0$ and $\frac{\partial f}{\partial y}(a,b)=0$ then the tangent line is not well-defined at (a,b).

This exercise motivates the following definition.

DEFINITION 1.9.1. A point $p=(a,b)$ on a curve $\mathcal{C} = \{(x,y) \in \mathbb{C}^2 : f(x,y)=0\}$ is said to be *singular* if

$$\frac{\partial f}{\partial x}(a,b) = 0 \text{and } \frac{\partial f}{\partial y}(a,b) = 0.$$

A point that is not singular is called *smooth.* If there is at least one singular point on $\mathcal{C}$, then curve $\mathcal{C}$ is called a *singular* curve. If there are no singular points on $\mathcal{C}$, the curve $\mathcal{C}$ is called a *smooth* curve.

EXERCISE 1.9.2. Show that the curve

$$\mathcal{C} = \{(x,y) \in \mathbb{C}^2 : x^2+y^2-1=0\}$$

is smooth.

EXERCISE 1.9.3. Show that the pair of crossing lines

$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 : (x + y - 1)(x - y - 1) = 0\}$$

has exactly one singular point. [Hint: Use the product rule.] Give a geometric interpretation of this singular point.

EXERCISE 1.9.4. Show that every point on the double line

$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 : (2x + 3y - 4)^2 = 0\}$$

is singular. [Hint: Use the chain rule.]

These definitions can also be applied to curves in $\mathbb{P}^2$.

DEFINITION 1.9.2. A point $p = (a : b : c)$ on a curve $\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : f(x, y, z) = 0\}$, where $f(x, y, z)$ is a homogeneous polynomial, is said to be *singular* if

$$\frac{\partial f}{\partial x}(a, b, c) = 0, \ \frac{\partial f}{\partial y}(a, b, c) = 0, \text{ and } \frac{\partial f}{\partial z}(a, b, c) = 0.$$

We have similar definitions, as before, for smooth point, smooth curve, and singular curve.

EXERCISE 1.9.5. Show that the curve

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : x^2 + y^2 - z^2 = 0\}$$

is smooth.

EXERCISE 1.9.6. Show that the pair of crossing lines

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : (x + y - z)(x - y - z) = 0\}$$

has exactly one singular point.

EXERCISE 1.9.7. Show that every point on the double line

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : (2x + 3y - 4z)^2 = 0\}$$

is singular.

For homogeneous polynomials, there is a clean relation between $f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}$ and $\frac{\partial f}{\partial z}$, which is the goal of the next few exercises.

EXERCISE 1.9.8. For

$$f(x, y, z) = x^2 + 3xy + 5xz + y^2 - 7yz + 8z^2,$$

show that

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

EXERCISE 1.9.9. For

$$f(x, y, z) = ax^2 + bxy + cxz + dy^2 + eyz + hz^2,$$

show that

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

EXERCISE 1.9.10. Let $f(x, y, z)$ be a homogeneous polynomial of degree n. Show that

$$n\ f = x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + z\frac{\partial f}{\partial z}.$$

(This problem is quite similar to the previous two, but to work out the details takes some work.)

EXERCISE 1.9.11. Use Exercise 1.9.10 to show that if $p = (a : b : c)$ satisfies

$$\frac{\partial f}{\partial x}(a, b, c) = \frac{\partial f}{\partial y}(a, b, c) = \frac{\partial f}{\partial z}(a, b, c) = 0,$$

then $p \in V(f)$.

The notion of smooth curves and singular curves certainly extends beyond the study of conics. We will briefly discuss higher degree curves here. Throughout, we will see that *singular* corresponds to not having a well-defined tangent.

EXERCISE 1.9.12. Graph the curve

$$f(x, y) = x^3 + x^2 - y^2 = 0$$

in the real plane $\mathbb{R}^2$. What is happening at the origin (0, 0)? Find the singular points.

EXERCISE 1.9.13. Graph the curve

$$f(x, y) = x^3 - y^2 = 0$$

in the real plane $\mathbb{R}^2$. What is happening at the origin (0, 0)? Find the singular points.

For any two polynomials, $f_1(x, y)$ and $f_2(x, y)$, let $f(x, y) = f_1(x, y)f_2(x, y)$ be the product. We have

$$V(f) = V(f_1) \cup V(f_2).$$

The picture of these curves is:

From the picture, it seems that the curve $V(f)$ should have singular points at the points of intersection of $V(f_1)$ and $V(f_2)$.

EXERCISE 1.9.14. Suppose that

$$f_1(a, b) = 0, \quad \text{and} \quad f_2(a, b) = 0$$

for a point $(a, b) \in \mathbb{C}^2$. Show that (a, b) is a singular point on $V(f)$, where $f = f_1f_2$.

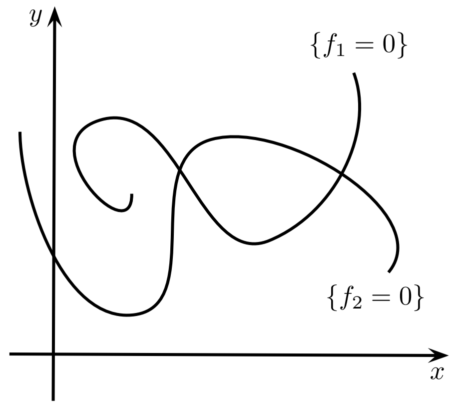


FIGURE 8. curves f_1 and f_2

EXERCISE 1.9.15. Suppose we have the projective change of coordinates given by

$$\begin{aligned} u &= x + y \\ v &= x - y \\ w &= x + y + z. \end{aligned}$$

If $f(u, v, w) = u^2 + uw + v^2 + vw$, find $\widetilde{f}(x, y, z)$.

EXERCISE 1.9.16. Given a general projective change of coordinates given by

$$\begin{aligned} u &= a_{11}x + a_{12}y + a_{13}z \\ v &= a_{21}x + a_{22}y + a_{23}z \\ w &= a_{31}x + a_{32}y + a_{33}z \end{aligned}$$

and a polynomial $f(u, v, w)$, describe how to find the corresponding $\widetilde{f}(x, y, z)$.

We now want to show, under a projective change of coordinates, that singular points go to singular points and smooth points go to smooth points.

EXERCISE 1.9.17. Let

$$\begin{aligned} u &= a_{11}x + a_{12}y + a_{13}z \\ v &= a_{21}x + a_{22}y + a_{23}z \\ w &= a_{31}x + a_{32}y + a_{33}z \end{aligned}$$

be a projective change of coordinates. Show that $(u_0 : v_0 : w_0)$ is a singular point of the curve $\mathcal{C} = \{(u : v : w) : f(u, v, w) = 0\}$ if and only if the corresponding point $(x_0 : y_0 : z_0)$ is a singular point of the corresponding curve $\widetilde{\mathcal{C}} = \{(x : y : z) : \widetilde{f}(x, y, z) = 0\}$. (This is an exercise in the multi-variable chain rule; most people are not comfortable with this chain rule without a lot of practice. Hence the value of this exercise.)

EXERCISE 1.9.18. Use the previous exercise to prove Theorem 1.2.26.

1.10. Conics via linear algebra

The goal of this section is to show how to interpret conics via linear algebra. In fact, we will see how, under projective changes of coordinates, all ellipses, hyperbolas and parabolas are equivalent; all crossing line conics are equivalent; and all double lines are equivalent follows easily from linear algebra facts about symmetric 3×3 matrices.

1.10.1. Conics via 3×3 symmetric matrices.

We start by showing how to represent conics with symmetric 3×3 matrices. Consider the second degree homogeneous polynomial

$$\begin{aligned} f(x, y, z) &= x^2 + 6xy + 5y^2 + 4xz + 8yz + 9z^2 \\ &= x^2 + (3xy + 3yx) + 5y^2 + (2xz + 2zx) + (4yz + 4zy) + 9z^2 \\ &= \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 1 & 3 & 2 \\ 3 & 5 & 4 \\ 2 & 4 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}. \end{aligned}$$

By using seemingly silly tricks such as $6xy = 3xy + 3yx$, we have written our initial second degree polynomial in terms of the symmetric 3×3 matrix

$$\begin{pmatrix} 1 & 3 & 2 \\ 3 & 5 & 4 \\ 2 & 4 & 9 \end{pmatrix}.$$

There is nothing special about this particular second degree polynomial. We can write all homogeneous second degree polynomials $f(x, y, z)$ in terms of symmetric 3×3 matrices. (Recall that a matrix $A = (a_{ij})$ is symmetric if $a_{ij} = a_{ji}$ for all i and j. Since the transpose of A simply switches the row and column entries $A^T = (a_{ji})$, another way to say A is symmetric is $A = A^T$.)

EXERCISE 1.10.1. Write the following conics in the form

$$\begin{pmatrix} x & y & z \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

That is, find a matrix A for each quadratic equation.

(1) $x^2 + y^2 + z^2 = 0$

(2) $x^2 + y^2 - z^2 = 0$
(3) $x^2 - y^2 = 0$
(4) $x^2 + 2xy + y^2 + 3xz + z^2 = 0$

Symmetric matrices can be be used to define second degree homogeneous polynomials with any number of variables.

DEFINITION 1.10.1. A *quadratic form* is a homogeneous polynomial of degree two in any given number of variables. Given a symmetric $n \times n$ matrix A and $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n$, then $f(X) = X^T A X$ is a quadratic form.

Thus conics are quadratic forms in three variables.

EXERCISE 1.10.2. Show that any conic

$$f(x, y, z) = ax^2 + bxy + cy^2 + dxz + eyz + hz^2$$

can be written as

$$\begin{pmatrix} x & y & z \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

where A is a symmetric 3×3 matrix.

1.10.2. Change of variables via matrices. We want to see that a projective change of coordinates has a quite natural linear algebra interpretation.

Suppose we have a projective change of coordinates

$$\begin{aligned} u &= a_{11}x + a_{12}y + a_{13}z \\ v &= a_{21}x + a_{22}y + a_{23}z \\ w &= a_{31}x + a_{32}y + a_{33}z. \end{aligned}$$

The matrix

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

that encodes the projective change of coordinates will be key.

Suppose $f(u, v, w)$ is a second degree homogeneous polynomial and let $\widetilde{f}(x, y, z)$ be the corresponding second degree homogeneous polynomial in the xyz-coordinate system. In the previous section, we know that there are two 3×3 symmetric matrices A and B such that

$$f(u,v,w) = \begin{pmatrix} u & v & w \end{pmatrix} A \begin{pmatrix} u \\ v \\ w \end{pmatrix}, \quad \widetilde{f}(x,y,z) = \begin{pmatrix} x & y & z \end{pmatrix} B \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

We want to find a relation between the three matrices M, A and B.

Exercise 1.10.3. Let C be a 3×3 matrix and let X be a 3×1 matrix. Show that $(CX)^T = X^T C^T$.

Exercise 1.10.4. Let M be a projective change of coordinates

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = M \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

and suppose

$$f(u,v,w) = \begin{pmatrix} u & v & w \end{pmatrix} A \begin{pmatrix} u \\ v \\ w \end{pmatrix}, \quad \widetilde{f}(x,y,z) = \begin{pmatrix} x & y & z \end{pmatrix} B \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Show that

$$B = M^T A M.$$

As a pedagogical aside, if we were following the format of earlier problems, before stating the above theorem, we would have given some concrete exercises illustrating the general principle. We have chosen not to do that here. In part, it is to allow the reader to come up with their own concrete examples, if needed. The other part is that this entire section's goal is not only to link linear algebra with conics but also to (not so secretly) force the reader to review some linear algebra.

Recall the following definitions from linear algebra.

Definition 1.10.2. We say that two $n \times n$ matrices A and B are *equivalent*, $A \sim B$, if there is an invertible $n \times n$ matrix C such that

$$A = C^{-1} B C.$$

Definition 1.10.3. An $n \times n$ matrix C is *orthogonal* if $C^{-1} = C^T$.

Definition 1.10.4. A matrix A has an eigenvalue λ if $Av = \lambda v$ for some non-zero vector v. The vector v is called an *eigenvector* with associated eigenvalue λ.

EXERCISE 1.10.5. Given a 3×3 matrix A, show that A has exactly three eigenvalues, counting multiplicity. [For this problem, it is fine to find the proof in a Linear Algebra text. After looking it up, close the book and try to reproduce the proof on your own. Repeat as necessary until you get it. This is of course another attempt by the authors to coax the reader into reviewing linear algebra.]

EXERCISE 1.10.6.
(1) Let A and B be two symmetric matrices, neither of which has as zero eigenvalue. Show there is an invertible 3×3 matrix C such that
$$A = C^T BC.$$
(2) Let A and B be two symmetric matrices, each of which has exactly one zero eigenvalue (with the other two eigenvalues being non-zero). Show that there is an invertible 3×3 matrix C such that
$$A = C^T BC.$$
(3) Now let A and B be two symmetric matrices, each of which has a zero eigenvalue with multiplicity two (and hence the remaining eigenvalue must be non-zero). Show that there is an invertible 3×3 matrix C such that
$$A = C^T BC.$$

(Again, it is fine to look up this deep result in a linear algebra text. Just make sure that you can eventually reproduce it on your own.)

EXERCISE 1.10.7.
(1) Show that the 3×3 matrix associated to the ellipse $V(x^2 + y^2 - z^2)$ has three non-zero eigenvalues.
(2) Show that the 3×3 matrix associated to the two lines $V(xy)$ has one zero eigenvalue and two non-zero eigenvalues.
(3) Finally show that the 3×3 matrix associated to the double line $V((x-y)^2)$ has a zero eigenvalue of multiplicity two and a non-zero eigenvalue.

EXERCISE 1.10.8. Based on the material of this section, give another proof that under projective changes of coordinates all ellipses, hyperbolas and parabolas are the same, all "two line" conics are the same, and all double lines are the same.

1.10.3. Conics in $\mathbb{R}^2$. We have shown that all smooth conics can be viewed as the same in the complex projective plane $\mathbb{P}^2$. But certainly ellipses, hyperbolas and parabolas are quite different in the real plane $\mathbb{R}^2$, as we saw earlier. But there is a more linear-algebraic approach that captures these differences.

Let $f(x, y, z) = ax^2 + bxy + cy^2 + dxz + eyz + hz^2 = 0$, with $a, b, c, d, e, h \in \mathbb{R}$. Dehomogenize by setting $z = 1$, so that we are looking at the polynomial
$$f(x, y) = ax^2 + bxy + cy^2 + dx + ey + h,$$

which can be written as

$$f(x,y) = \begin{pmatrix} x & y & 1 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & h \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.$$

In $\mathbb{P}^2$, the coordinates x, y and z all play the same role. That is no longer the case, after setting $z = 1$. The second order term of f,

$$ax^2 + bxy + cy^2$$

determines whether we have an ellipse, hyperbola, or parabola.

Exercise 1.10.9. Explain why we only need to consider the second order terms. [Hint: We have already answered this question earlier in this chapter.]

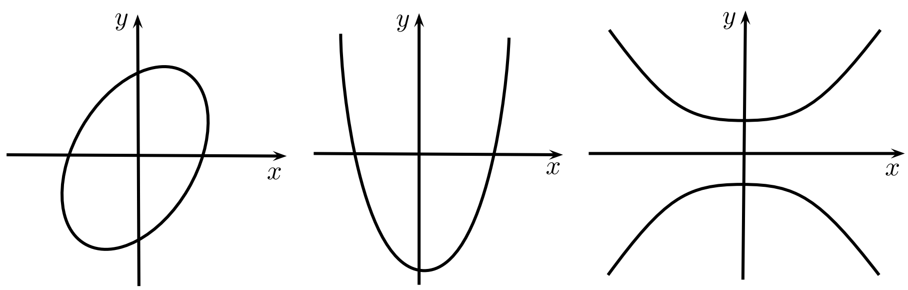


Figure 9. three types of conics

This suggests that the matrix

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

might be worth investigating.

Definition 1.10.5. The *discriminant* of a conic over $\mathbb{R}^2$ is

$$\Delta = -4 \det \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

Exercise 1.10.10. Find the discriminant of each of the following conics:

(1) $9x^2 + 4y^2 = 1$
(2) $9x^2 - 4y^2 = 1$
(3) $9x^2 - y = 0$.

Exercise 1.10.11. Based on the previous exercise, describe the conic obtained if $\Delta = 0$, $\Delta < 0$, or $\Delta > 0$. State what the general result ought to be. To rigorously prove it should take some time. In fact, if you have not seen this before, this type of problem will have to be spread out over a few days. (We do not mean for you spend all of your time on this problem; no, we mean for you to work on it for a thirty minutes to an hour, put it aside and then come back to it.)

Exercise 1.10.12. Consider the equation $ax^2 + bxy + cy^2 = 0$, where all coefficients are real numbers. Dehomogenize the equation by setting $y = 1$. Solve the resulting quadratic equation for x. You should see a factor involving Δ in your solution. How does Δ relate to the discriminant used in the quadratic formula?

Exercise 1.10.13. The discriminant in the quadratic formula tells us how many (real) solutions a given quadratic equation in a single variable has. Classify a conic $V(f(x,y))$ based on the number of solutions to the dehomogenized quadratic equation.

1.11. Duality

1.11.1. Duality in $\mathbb{P}^2$ between points and lines. The goal of this subsection is show that there is a duality between points and lines in the projective plane.

Given a triple of points $a, b, c \in \mathbb{C}$, not all zero, we have a line

$$\mathcal{L} = \{(x : y : z) \in \mathbb{P}^2 : ax + by + cz = 0\}.$$

Exercise 1.11.1. Show that the line associated to $a_1 = 1, b_1 = 2, c_1 = 3$ is the same line as that associated to $a_2 = -2, b_2 = -4, c_2 = -6$.

Exercise 1.11.2. Show that the line associated to a_1, b_1, c_1 is the same line as the line associated to a_2, b_2, c_2 if and only if there is a non-zero constant $\lambda \in \mathbb{C}$ such that $a_1 = \lambda a_2,\ b_1 = \lambda b_2,\ c_1 = \lambda c_2$.

Hence any representative in the equivalence class for $(a : b : c) \in \mathbb{P}^2$ defines the same line.

Exercise 1.11.3. Show that the set of all lines in $\mathbb{P}^2$ can be identified with $\mathbb{P}^2$ itself.

Even though the set of lines in $\mathbb{P}^2$ can be thought of as another $\mathbb{P}^2$, we want notation to be able to distinguish $\mathbb{P}^2$ as a set of points and $\mathbb{P}^2$ as the set of lines. Let $\mathbb{P}^2$ be our set of points and let $\widetilde{\mathbb{P}}^2$ denote the set of lines in $\mathbb{P}^2$. To help our notation, given $(a : b : c) \in \mathbb{P}^2$, let

$$\mathcal{L}_{(a:b:c)} = \{(x : y : z) \in \mathbb{P}^2 : ax + by + cz = 0\}.$$

Then we define the map $\mathcal{D} : \widetilde{\mathbb{P}}^2 \to \mathbb{P}^2$ by

$$\mathcal{D}(\mathcal{L}_{(a:b:c)}) = (a : b : c).$$

The $\mathcal{D}$ stands for *duality*.

Let us look for a minute at the equation of a line:

$$ax + by + cz = 0.$$

Though it is traditional to think of a, b, c as constants and x, y, z as variables, this is only a convention. Think briefly of x, y, z as fixed, and consider the set

$$\mathcal{M}_{(x:y:z)} = \{(a : b : c) \in \widetilde{\mathbb{P}}^2 : ax + by + cz = 0.\}$$

Exercise 1.11.4. Explain in your own words why, given a $(x_0 : y_0 : z_0) \in \mathbb{P}^2$, we can interpret $\mathcal{M}_{(x_0:y_0:z_0)}$ as the set of all lines containing the point $(x_0 : y_0 : z_0)$.

We are beginning to see a duality between lines and points.

Let

$$\Sigma = \{((a : b : c), (x_0 : y_0 : z_0)) \in \widetilde{\mathbb{P}}^2 \times \mathbb{P}^2 : ax_0 + by_0 + cz_0 = 0\}.$$

There are two natural projection maps:

$$\pi_1 : \Sigma \to \widetilde{\mathbb{P}}^2$$

given by

$$\pi_1(((a : b : c), (x_0 : y_0 : z_0))) = (a : b : c)$$

and

$$\pi_2 : \Sigma \to \mathbb{P}^2$$

given by

$$\pi_2(((a : b : c), (x_0 : y_0 : z_0))) = (x_0 : y_0 : z_0).$$

Exercise 1.11.5. Show that both maps π_1 and π_2 are onto.

Exercise 1.11.6. Given a point $(a : b : c) \in \widetilde{\mathbb{P}}^2$, consider the set

$$\pi_1^{-1}(a : b : c) = \{((a : b : c), (x_0 : y_0 : z_0)) \in \Sigma\}.$$

Show that the set $\pi_2(\pi_1^{-1}(a : b : c))$ is identical to a set in $\mathbb{P}^2$ that we defined near the beginning of this section.

In evidence for a type of duality, show:

Exercise 1.11.7. Given a point $(x_0 : y_0 : z_0) \in \mathbb{P}^2$, consider the set

$$\pi_2^{-1}(x_0 : y_0 : z_0) = \{((a : b : c), (x_0 : y_0 : z_0)) \in \Sigma\}.$$

Show that the set $\pi_1(\pi_2^{-1}(x_0 : y_0 : z_0))$ is identical to a set in $\widetilde{\mathbb{P}}^2$ that we defined near the beginning of this section.

EXERCISE 1.11.8. Let $(1:2:3),(2:5:1)\in\widetilde{\mathbb{P}}^2$. Find

$$\pi_2(\pi_1^{-1}(1:2:3))\cap\pi_2(\pi_1^{-1}(2:5:1)).$$

Explain why this is just a fancy way for finding the point of intersection of the two lines

$$x+2y+3z=0$$

$$2x+5y+z=0.$$

As another piece of evidence for duality, show:

EXERCISE 1.11.9. Let $(1:2:3),(2:5:1)\in\mathbb{P}^2$. Find

$$\pi_1(\pi_2^{-1}(1:2:3))\cap\pi_1(\pi_2^{-1}(2:5:1)).$$

Explain that this is just a fancy way for finding the unique line containing the two points $(1:2:3),(2:5:1)$.

PRINCIPLE 1.11.1. The duality principle for points and lines in the complex projective plane is that for any theorem for points and lines there is a corresponding different theorem obtained by interchanging words the "points" and "lines".

EXERCISE 1.11.10. Use the duality principle to find the corresponding theorem to:

THEOREM 1.11.11. *Any two distinct points in $\mathbb{P}^2$ are contained on a unique line.*

This duality extends to higher dimensional projective spaces.

The following is a fairly open ended exercise:

EXERCISE 1.11.12. For points $(x_0,y_0,z_0,w_0),(x_1,y_1,z_1,w_1)\in\mathbb{C}^4-\{(0,0,0,0)\}$, define

$$(x_0,y_0,z_0,w_0)\sim(x_1,y_1,z_1,w_1)$$

if there exists a non-zero λ such that

$$x_0=\lambda x_1,y_0=\lambda y_1,z_0=\lambda z_1,w_0=\lambda w_1.$$

Define

$$\mathbb{P}^3=\mathbb{C}^4-\{(0,0,0,0)\}/\sim.$$

Show that the set of all planes in $\mathbb{P}^3$ can be identified with another copy of $\mathbb{P}^3$. Explain how the duality principle can be used to link the fact that three non-collinear points define a unique plane to the fact three planes with linearly independent normal vectors intersect in a unique point.

1.11.2. Dual Curves to Conics. The goal of this subsection is to show how to map any smooth curve in $\mathbb{P}^2$ to another curve via duality.

Let $f(x, y, z)$ be a homogeneous polynomial and let

$$\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2 : f(x, y, z) = 0\},$$

We know that the normal vector at a point $p = (x_0 : y_0 : z_0) \in \mathcal{C}$ is

$$\nabla(f)(p) = \left(\frac{\partial f}{\partial x}(p), \frac{\partial f}{\partial y}(p), \frac{\partial f}{\partial z}(p)\right).$$

Further the tangent line at $p = (x_0 : y_0 : z_0) \in \mathcal{C}$ is defined as

$$T_p(\mathcal{C}) = \{(x : y : z) \in \mathbb{P}^2 : x\frac{\partial f}{\partial x}(p) + y\frac{\partial f}{\partial y}(p) + z\frac{\partial f}{\partial z}(p) = 0\}.$$

Recall from Section 1.9, that if f has degree n, then

$$nf(x, y, z) = x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + z\frac{\partial f}{\partial z}.$$

EXERCISE 1.11.13. Show that for any $p = (x_0 : y_0 : z_0) \in \mathcal{C}$, we have

$$T_p(\mathcal{C}) = \{(x : y : z) \in \mathbb{P}^2 : (x - x_0)\frac{\partial f}{\partial x}(p) + (y - y_0)\frac{\partial f}{\partial y}(p) + (z - z_0)\frac{\partial f}{\partial z}(p) = 0\}.$$

Recall that $p \in \mathcal{C}$ is smooth if the gradient

$$\nabla f(p) \neq (0, 0, 0).$$

DEFINITION 1.11.1. For a smooth curve $\mathcal{C}$, the dual curve $\widetilde{\mathcal{C}}$ is the composition of the map, for $p \in \mathcal{C}$,

$$p \to T_p(\mathcal{C})$$

with the dual map from last section

$$\mathcal{D} : \widetilde{\mathbb{P}}^2 \to \mathbb{P}^2.$$

We denote this map also by $\mathcal{D}$. Then

$$\mathcal{D}(p) = \left(\frac{\partial f}{\partial x}(p) : \frac{\partial f}{\partial y}(p) : \frac{\partial f}{\partial z}(p)\right).$$

To make sense out of this, we of course need some examples.

EXERCISE 1.11.14. For $f(x, y, z) = x^2 + y^2 - z^2$, let $\mathcal{C} = V(f(x, y, z))$. Show for any $(x_0 : y_0 : z_0) \in \mathcal{C}$ that

$$\mathcal{D}(x_0 : y_0 : z_0) = (2x_0 : 2y_0 : -2z_0).$$

Show that in this case the dual curve $\widetilde{\mathcal{C}}$ is the same as the original $\mathcal{C}$.

EXERCISE 1.11.15. Consider $f(x,y,z) = x^2 - yz = 0$. Then for any $(x : y : z) \in \mathcal{C}$, where $\mathcal{C} = V(f)$, show that

$$\begin{aligned} \mathcal{D}(x,y,z) &= (\frac{\partial f}{\partial x} : \frac{\partial f}{\partial y} : \frac{\partial f}{\partial z}) \\ &= (2x : -z : -y) \end{aligned}$$

Show that the image is indeed in $\widetilde{\mathbb{P}}^2$ by showing that $(2x : -z : -y) \neq (0 : 0 : 0)$. Let $(u : v : w) = (2x : -z : -y)$. Using $x^2 - yz = 0$ on $\mathcal{C}$ as a motivator, show that $u^2 - 4vw = 4x^2 - 4yz = 4(x^2 - yz) = 0$. Relabeling $(u : v : w)$ as $(x : y : z)$, show that the curve $\widetilde{\mathcal{C}}$ is given by $x^2 - 4yz = 0$. Note that here $\widetilde{\mathcal{C}} \neq \mathcal{C}$.

EXERCISE 1.11.16. For $\mathcal{C} = V(x^2 + 4y^2 - 9z^2)$, show that the dual curve is

$$\widetilde{\mathcal{C}} = \{(x : y : z) \in \mathbb{P}^2 : x^2 + \frac{1}{4}y^2 - \frac{1}{9}z^2 = 0\}.$$

EXERCISE 1.11.17. For $\mathcal{C} = V(5x^2 + 2y^2 - 8z^2)$, find the dual curve.

EXERCISE 1.11.18. For a line $\mathcal{L} = \{(x : y : z) \in \mathbb{P}^2 : ax + by + cz\}$, find the dual curve. Explain why calling this set the "dual curve" might seem strange.

CHAPTER 2

Cubic Curves and Elliptic Curves

The goal of this chapter is to provide an introduction to cubic curves (smooth cubic curves are also known as elliptic curves). Cubic curves have a far richer structure than that of conics. Many of the deepest questions in mathematics still involve questions about cubics. After a few preliminaries, we will show how each smooth cubic curve is a group, meaning that its points can be added together. No other type of curve has this property. We will then see that there are many different cubics, even up to projective change of coordinates. In fact, we will see that there are a complex numbers worth of different cubics. That is, we can parametrize cubics up to isomorphism by the complex numbers. (This is in marked contrast to conics, since all smooth conics are the same up to projective change of coordinates.). Next, we will see that, as surfaces, all smooth cubics are toruses. Finally, we see how all cubics can be viewed as the quotient $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$.

2.1. Cubics in $\mathbb{C}^2$

A cubic curve $\mathrm{V}(P)$ is simply the zero set of a degree three polynomial P. If P is in two variables, then $\mathrm{V}(P)$ will be a cubic in $\mathbb{C}^2$ while if P is homogeneous in three variables, then $\mathrm{V}(P)$ is a cubic in the projective plane $\mathbb{P}^2$.

Exercise 2.1.1. Sketch the following cubics in the real plane $\mathbb{R}^2$.

(1) $y^2 = x^3$
(2) $y^2 = x(x-1)^2$
(3) $y^2 = x(x-1)(x-2)$
(4) $y^2 = x(x^2+x+1)$

Of course, we are only sketching these curves in the real plane to get a feel for cubics.

Exercise 2.1.2. Consider the cubics in the above exercise.

(1) Give the homogeneous form for each cubic, which extends each of the above cubics to the complex projective plane $\mathbb{P}^2$.
(2) For each of the above cubics, dehomogenize by setting $x = 1$, and graph the resulting cubic in $\mathbb{R}^2$ with coordinates y and z.

Recall that a point $(a:b:c) \in \mathrm{V}(P)$ on a curve is *singular* if

$$\begin{aligned}\frac{\partial P}{\partial x}(a,b,c) &= 0\\ \frac{\partial P}{\partial y}(a,b,c) &= 0\\ \frac{\partial P}{\partial z}(a,b,c) &= 0\end{aligned}$$

If a curve has a singular point, then we call the curve singular. If a curve has no singular points, it is smooth.

Exercise 2.1.3. Show that the following cubics are singular:

(1) $\mathrm{V}(xyz)$
(2) $\mathrm{V}(x(x^2+y^2-z^2))$
(3) $\mathrm{V}(x^3)$

The only singular conics are unions of two lines or double lines. The above singular cubics are similar, in that they are all the zero sets of reducible polynomials $P(x,y,z)$. Unlike for conics, though, there are singular cubics that do not arise from reducible P.

Exercise 2.1.4. Sketch the cubic $y^2 = x^3$ in the real plane $\mathbb{R}^2$. Show that the corresponding cubic $\mathrm{V}(x^3 - y^2 z)$ in $\mathbb{P}^2$ has a singular point at $(0:0:1)$. Show that this is the only singular point on this cubic.

Exercise 2.1.5. Show that the polynomial $P(x,y,z) = x^3 - y^2 z$ is irreducible, i.e. cannot be factored into two polynomials. (This is a fairly brute force high-school algebra problem.)

2.2. Inflection Points

The goal of this section is to show that every smooth cubic curve must have exactly nine points of inflection.

2.2.1. Intuitions about Inflection Point. One of the strengths of algebraic geometry is the ability to move freely between the symbolic language of algebra and the visual capabilities of geometry. We would like to use this flexibility to convert what initially is a geometric problem into an algebraic one. While we can sometimes imagine what is happening geometrically, this will help us in situations that may be difficult to visualize.

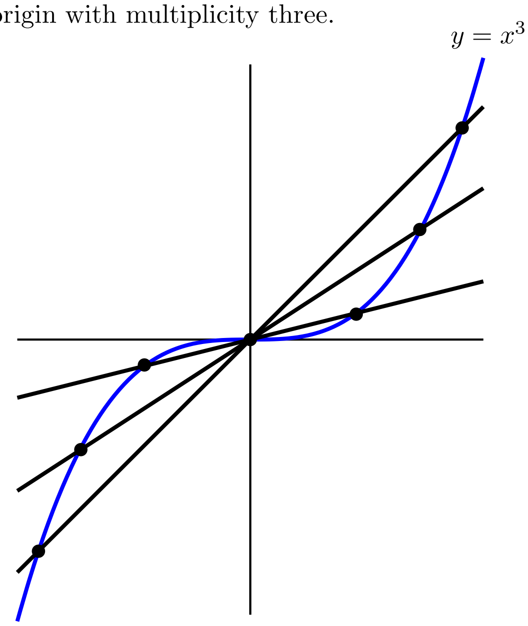
We have seen that a line will intersect a smooth conic in two points. If the points are distinct, then the line will cut through the conic. However, there may be a line which has only one point in common with the conic, namely the tangent line. In this case, if we consider that the point of tangency is to be counted twice, then the line will intersect the conic in "two" points.

If we now consider a line intersecting a cubic, we may have more points of intersection to consider. Intuitively, they can not cross in too many places. In fact, the Fundamental Theorem of Algebra shows that a line intersects a cubic in at most three points. As in the case of the conics, points may need to be counted more than once. Since we may have more possible points of intersection, the number of times a point in common to the line and cubic can be either one, two or three.

If a line intersects a cubic in a single point (counted thrice), we call such a point a point of inflection or flex point. An *inflection point* of a curve $\mathrm{V}(P)$ is a non-singular point $p \in \mathrm{V}(P)$ where the tangent line to the curve at p intersects $\mathrm{V}(P)$ with multiplicity 3 (or greater).

We define below what it means for the tangent line at a point to intersect the curve with multiplicity 3 (or greater), but the idea can be illustrated with some examples.

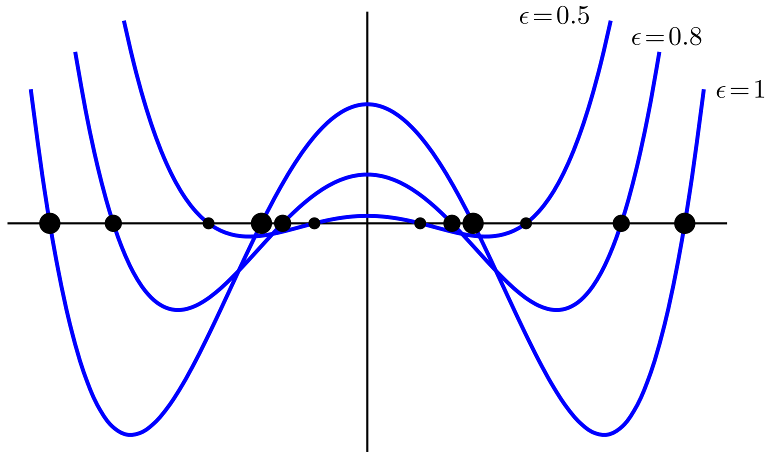
(1) Consider the cubic curve $y = x^3$, that is, $\mathrm{V}(P)$ where $P(x, y) = x^3 - y$. Let the point p be the origin, and consider the line $y = \epsilon x$, where $\epsilon > 0$. This line intersects the curve in three distinct points no matter how small ϵ is, but as ϵ approaches zero, the three points of intersection coalesce into just one point. We say that the tangent line $y = 0$ intersects the cubic $y = x^3$ at the origin with multiplicity three.



(2) If we look at the behavior of the quartic (fourth-degree) curve

$$y = (x - \epsilon)(x - \epsilon/3)(x + \epsilon/3)(x + \epsilon),$$

we see that the curve and the line $y = 0$ intersect at four points whenever $\epsilon > 0$. But as ϵ approaches zero, the four points of intersection become one point, the origin. Here we say that the tangent line $y = 0$ intersects this curve at the origin with multiplicity four.



$y = (x - \epsilon)(x - \epsilon/3)(x + \epsilon/3)(x + \epsilon)$

(3) We will see later that the tangent line ℓ to a curve $\mathrm{V}(P)$ at a point p always intersects the curve with multiplicity at least 2.

2.2.2. Multiplicity of Roots. For a moment we will look at one-variable polynomials (which correspond to homogeneous two-variable polynomials).

DEFINITION 2.2.1. Given a polynomial $P(x)$, a *root* or *zero* is a point a such that $P(a) = 0$.

EXERCISE 2.2.1. If $(x - a)$ divides $P(x)$, show that a is a root of $P(x)$.

EXERCISE 2.2.2. If a is a root of $P(x)$, show that $(x - a)$ divides $P(x)$. [Hint: use the Division Algorithm for polynomials.]

DEFINITION 2.2.2. Let a be a root of the polynomial $P(x)$. This root has *multiplicity* k if $(x - a)^k$ divides $P(x)$ but $(x - a)^{k+1}$ does not divide $P(x)$.

EXERCISE 2.2.3. Suppose that a is a root of multiplicity two for $P(x)$. Show there is a polynomial $g(x)$ such that

$$P(x) = (x - a)^2 g(x)$$

with $g(a) \neq 0$.

EXERCISE 2.2.4. Suppose that a is a root of multiplicity two for $P(x)$. Show that $P(a) = 0$ and $P'(a) = 0$ but $P''(a) \neq 0$.

EXERCISE 2.2.5. Suppose that a be a root of multiplicity k for $P(x)$. Show there is a polynomial $g(x)$ such that

$$P(x) = (x-a)^k g(x)$$

with $g(a) \neq 0$.

EXERCISE 2.2.6. Suppose that a is a root of multiplicity k for $P(x)$. Show that $P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$ but that $P^{(k)}(a) \neq 0$.

The homogeneous version is the following.

DEFINITION 2.2.3. Let $P(x, y)$ be a homogeneous polynomial. A *root* or *zero* is a point $(a : b) \in \mathbb{P}^1$ such that $P(a, b) = 0$. If $(a : b)$ is a root of $P(x, y)$, then $(bx - ay)$ divides $P(x, y)$. This root has *multiplicity* k if $(bx - ay)^k$ divides $P(x, y)$ but $(bx - ay)^{k+1}$ does not divide $P(x, y)$.

EXERCISE 2.2.7. Suppose that $(a : b)$ is a root of multiplicity two for $P(x, y)$. Show that

$$P(a, b) = \frac{\partial P}{\partial x}(a, b) = \frac{\partial P}{\partial y}(a, b) = 0,$$

but at least one of the second partials does not vanish at $(a : b)$.

EXERCISE 2.2.8. Suppose that $(a : b)$ is a root of multiplicity k for $P(x, y)$. Show that

$$P(a, b) = \frac{\partial P}{\partial x}(a, b) = \frac{\partial P}{\partial y}(a, b) = \cdots = \frac{\partial^{k-1} P}{\partial x^i \partial y^j}(a, b) = 0,$$

where $i + j = k - 1$ but that

$$\frac{\partial^k P}{\partial x^i \partial y^j}(a, b) \neq 0,$$

for at least one pair $i + j = k$. This means that the first partials, second partials, etc. up to the $k - 1$ partials all vanish at $(a : b)$, but that at least one of the k^{th} partials does not vanish at $(a : b)$.

2.2.3. Inflection Points. Let $P(x, y, z)$ be a homogeneous polynomial. We want to understand what it means for a line to intersect $\mathrm{V}(P)$ in a point with multiplicity three or more. Let

$$l(x, y, z) = ax + by + cz$$

be a linear polynomial and let $\ell = \mathrm{V}(l)$ be the corresponding line in $\mathbb{P}^2$. We are tacitly assuming that not all of a, b, c are zero. We might as well assume that $b \neq 0$. That is, by a projective change of coordinates we may assume that $b \neq 0$. We can multiply l by any nonzero constant and still have the same line, meaning that for $\lambda \neq 0$, we have $\mathrm{V}(l) = \mathrm{V}(\lambda l)$. So, we can assume that $b = -1$. The reason for the -1 is that we now know that all points on the line have the property that $y = ax + cz$.

EXERCISE 2.2.9. Let $(x_0 : y_0 : z_0) \in \mathrm{V}(P) \cap \mathrm{V}(l)$. Show that $(x_0 : z_0)$ is a root of the homogeneous two-variable polynomial $P(x, ax + cz, z)$ and that $y_0 = ax_0 + cz_0$.

DEFINITION 2.2.4. The *intersection multiplicity* of $\mathrm{V}(P)$ and $\mathrm{V}(l)$ at $(x_0 : y_0 : z_0)$ is the multiplicity of the root $(x_0 : z_0)$ of $P(x, ax + cz, z)$.

EXERCISE 2.2.10. Let $P(x, y, z) = x^2 - yz$ and $l(x, y, z) = \lambda x - y$. Show that the intersection multiplicity of $\mathrm{V}(P)$ and $\mathrm{V}(l)$ at $(0 : 0 : 1)$ is one when $\lambda \neq 0$ and is two when $\lambda = 0$.

The key to the definition above is that, when $b = -1$, the system $x = x, y = ax + cz, z = z$ gives a parametrization of the line $\mathrm{V}(l)$ and the intersection multiplicity of $\mathrm{V}(P)$ and $\mathrm{V}(l)$ at $(x_0 : y_0 : z_0)$ is found by considering P evaluated as a function of these two parameters. The next exercise proves the important fact that the intersection multiplicity is independent of the choice of parametrization of the line $\mathrm{V}(l)$ used.

EXERCISE 2.2.11. Let $(x_0 : y_0 : z_0) \in \mathrm{V}(P) \cap \mathrm{V}(l)$. Let $x = a_1 s + b_1 t, y = a_2 s + b_2 t, z = a_3 s + b_3 t$ and $x = c_1 u + d_1 v, y = c_2 u + d_2 v, z = c_3 u + d_3 v$ be two parametrizations of the line $\mathrm{V}(l)$ such that $(x_0 : y_0 : z_0)$ corresponds to $(s_0 : t_0)$ and $(u_0 : v_0)$, respectively. Show that the multiplicity of the root $(s_0 : t_0)$ of $P(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t)$ is equal to the multiplicity of the root $(u_0 : v_0)$ of $P(c_1 u + d_1 v, y = c_2 u + d_2 v, z = c_3 u + d_3 v)$. Conclude that our definition of the intersection multiplicity of $\mathrm{V}(P)$ and $\mathrm{V}(l)$ is independent of the parametrization of the line $\mathrm{V}(l)$ used.

EXERCISE 2.2.12. Let $P(x, y, z) = x^2 + 2xy - yz + z^2$. Show that the intersection multiplicity of $\mathrm{V}(P)$ and any line ℓ at a point of intersection is at most two.

EXERCISE 2.2.13. Let $P(x, y, z)$ be an irreducible second degree homogeneous polynomial. Show that the intersection multiplicity of $\mathrm{V}(P)$ and any line ℓ at a point of intersection is at most two.

EXERCISE 2.2.14. Let $P(x, y, z) = x^2 + y^2 + 2xz - yz$.

(1) Find the tangent line $\ell = \mathrm{V}(l)$ to $\mathrm{V}(P)$ at $(-2 : 1 : 1)$.
(2) Show that the intersection multiplicity of $\mathrm{V}(P)$ and ℓ at $(-2 : 1 : 1)$ is two.

EXERCISE 2.2.15. Let $P(x, y, z) = x^3 - y^2 z + z^3$.

(1) Find the tangent line to $\mathrm{V}(P)$ at $(2 : 3 : 1)$ and show directly that the intersection multiplicity of $\mathrm{V}(P)$ and its tangent at $(2 : 3 : 1)$ is two.

(2) Find the tangent line to $\mathrm{V}(P)$ at $(0 : 1 : 1)$ and show directly that the intersection multiplicity of $\mathrm{V}(P)$ and its tangent at $(0 : 1 : 1)$ is three.

Exercise 2.2.16. Redo the previous two exercises using Exercise 2.2.8.

Exercise 2.2.17. Show that for any non-singular curve $\mathrm{V}(P) \subset \mathbb{P}^2$, the intersection multiplicity of $\mathrm{V}(P)$ and its tangent line ℓ at the point of tangency is at least two.

Exercise 2.2.18.

(1) Let $P(x, y, z)$ be an irreducible degree three homogeneous polynomial. Show that the intersection multiplicity of $\mathrm{V}(P)$ and any line ℓ at a point of intersection is at most three.

(2) Let $P(x, y, z)$ be an irreducible homogeneous polynomial of degree n. Show that the intersection multiplicity of $\mathrm{V}(P)$ and any line ℓ at a point of intersection is at most n.

Definition 2.2.5. Let $P(x, y, z)$ be an irreducible homogeneous polynomial of degree n. A non-singular point $p \in \mathrm{V}(P) \subset \mathbb{P}^2$ is called a *point of inflection* or a *flex* of the curve $\mathrm{V}(P)$ if the tangent line to the curve at p intersects $\mathrm{V}(P)$ with multiplicity at least three.

Exercise 2.2.19. Let $P(x, y, z) = x^3 + yz^2$. Show that $(0 : 0 : 1)$ is an inflection point of $\mathrm{V}(P)$.

Exercise 2.2.20. Let $P(x, y, z) = x^3 + y^3 + z^3$ (the Fermat curve). Show that $(1 : -1 : 0)$ is an inflection point of $V(P)$.

2.2.4. Hessians. We have just defined what it means for a point $p \in \mathrm{V}(P)$ to be a point of inflection. Checking to see whether a given point $p \in \mathrm{V}(P)$ is an inflection point can be tedious, but finding inflection points can be extremely difficult task with our current tools. How did we know to check $(1 : -1 : 0)$ in Exercise 2.2.20? As we know $\mathrm{V}(P)$ has an infinite number of points, so it would be impossible to find the tangent at every point and to check the intersection multiplicity. Moreover, if these inflection points are related to the inflection points of calculus, where are the second derivatives? The Hessian curve will completely solve these difficulties. We will first define the Hessian curve, then determine how it can be used to find the points of inflection.

Definition 2.2.6. Let $P(x, y, z)$ be a homogeneous polynomial of degree n. The *Hessian* $H(P)$ is

$$H(P)(x, y, z) = \det \begin{pmatrix} P_{xx} & P_{xy} & P_{xz} \\ P_{xy} & P_{yy} & P_{yz} \\ P_{xz} & P_{yz} & P_{zz} \end{pmatrix},$$

where

$$\begin{aligned} P_x &= \frac{\partial P}{\partial x} \\ P_{xx} &= \frac{\partial^2 P}{\partial x^2} \\ P_{xy} &= \frac{\partial^2 P}{\partial x \partial y}, \quad \text{etc.} \end{aligned}$$

The *Hessian curve* is $\mathrm{V}(H(P))$.

EXERCISE 2.2.21. Compute $H(P)$ for the following cubic polynomials.

(1) $P(x, y, z) = x^3 + yz^2$
(2) $P(x, y, z) = y^3 + z^3 + xy^2 - 3yz^2 + 3zy^2$
(3) $P(x, y, z) = x^3 + y^3 + z^3$

EXERCISE 2.2.22. Let $P(x, y, z)$ be an irreducible homogeneous polynomial of degree three. Show that $H(P)$ is also a third degree homogeneous polynomial.

We want to link the Hessian curve with inflection points.

EXERCISE 2.2.23. Let $P(x, y, z) = x^3 + y^3 + z^3$ (the Fermat curve). Show that $(1 : -1 : 0) \in \mathrm{V}(P) \cap \mathrm{V}(H(P))$.

EXERCISE 2.2.24. Let $P(x, y, z) = y^3 + z^3 + xy^2 - 3yz^2 + 3zy^2$. Show that $(-2 : 1 : 1) \in \mathrm{V}(P) \cap \mathrm{V}(H(P))$.

EXERCISE 2.2.25. Let $P(x, y, z) = x^3 + yz^2$. Show that $(0 : 0 : 1) \in \mathrm{V}(P) \cap \mathrm{V}(H(P))$.

These exercises suggest a link between inflection points of $\mathrm{V}(P)$ and points in $\mathrm{V}(P) \cap \mathrm{V}(H(P))$, but we need to be careful.

EXERCISE 2.2.26. Let $P(x, y, z) = x^3 + yz^2$.

(1) Show that $(0 : 1 : 0) \in \mathrm{V}(P) \cap \mathrm{V}(H(P))$.
(2) Explain why $(0 : 1 : 0)$ is not an inflection point of $\mathrm{V}(P)$.

We can now state the relationship we want.

THEOREM 2.2.27. Let $P(x, y, z)$ be a homogeneous polynomial of degree d. If $\mathrm{V}(P)$ is smooth, then $p \in \mathrm{V}(P) \cap \mathrm{V}(H(P))$ if and only if p is a point of inflection of $\mathrm{V}(P)$.

We will prove this theorem through a series of exercises.[1] The first thing we need to show is that the vanishing of the Hessian $\mathrm{V}(H(P))$ is invariant under a projective change of coordinates.

[1] The following exercises are based on the proof taken from C. G. Gibson's "Elementary Geometry of Algebraic Curves." [**Gib98**]

EXERCISE 2.2.28. Consider the following projective change of coordinates

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

where

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Suppose that under the projective transformation A the polynomial $P(x, y, z)$ becomes the polynomial $Q(u, v, w)$.

(1) Show that the Hessian matrices of P and Q are related by

$$\begin{pmatrix} P_{xx} & P_{xy} & P_{xz} \\ P_{xy} & P_{yy} & P_{yz} \\ P_{xz} & P_{yz} & P_{zz} \end{pmatrix} = A^T \begin{pmatrix} Q_{uu} & Q_{uv} & Q_{uw} \\ Q_{uv} & Q_{vv} & Q_{vw} \\ Q_{uw} & Q_{vw} & Q_{ww} \end{pmatrix} A.$$

(2) Conclude that $H(P)(x, y, z) = 0$ if and only if $H(Q)(u, v, w) = 0$.

Next we need to show that inflection points are mapped to inflection points under a projective change of coordinates.

EXERCISE 2.2.29. Suppose p is a point of inflection of $\mathrm{V}(P)$, and that under a projective change of coordinates the polynomial P becomes the polynomial Q and $p \mapsto q$. Show that q is a point of inflection of $\mathrm{V}(Q)$.

In the next exercise, we will reduce the proof of Theorem 2.2.27 to the case where $p = (0 : 0 : 1) \in \mathrm{V}(P)$ and the tangent line to $\mathrm{V}(P)$ at p is $\ell = \mathrm{V}(y)$.

EXERCISE 2.2.30. Use Exercises 2.2.28 and 2.2.29 to explain why to prove Theorem 2.2.27 it is enough to show that p is a point of inflection if and only if $H(P)(p) = 0$ in the case where $p = (0 : 0 : 1) \in \mathrm{V}(P)$ and the tangent line ℓ to $\mathrm{V}(P)$ at p is $y = 0$, i.e. $\ell = \mathrm{V}(y)$.

Thus we will assume that the point $p = (0 : 0 : 1) \in \mathrm{V}(P)$ and that the tangent line to $\mathrm{V}(P)$ at p is $y = 0$ from now until the end of Exercise 2.2.34.

EXERCISE 2.2.31. Explain why in the affine patch $z = 1$ the dehomogenized curve is

$$\lambda y + (ax^2 + bxy + cy^2) + \text{higher order terms},$$

where $\lambda \neq 0$. [Hint: We know that $p \in \mathrm{V}(P)$ and p is non-singular.]

From this we can conclude that $P(x, y, z)$ is given by

$$P(x, y, z) = \lambda y z^{d-1} + (ax^2 + bxy + cy^2) z^{d-2} + \text{higher order terms} \tag{2.1}$$

where $d = \deg P$.

EXERCISE 2.2.32. Explain why the intersection of $\mathrm{V}(P)$ with the tangent $\mathrm{V}(y)$ at p corresponds to the root $(0:1)$ of the equation

$$P(x,0,z) = ax^2z^{d-2} + \text{higher order terms} = 0.$$

EXERCISE 2.2.33. Show that p is a point of inflection of $\mathrm{V}(P)$ if and only if $a = 0$. [Hint: For p to be an inflection point, what must the multiplicity of $(0:1)$ be in the equation in Exercise 2.2.32?]

We have now established that p is a point of inflection if and only if $a = 0$ in Equation (2.1). All that remains is to show that $p \in \mathrm{V}(H(P))$ if and only if $a = 0$.

EXERCISE 2.2.34.

(1) Show that

$$H(P)(p) = \det \begin{pmatrix} 2a & b & 0 \\ b & 2c & \lambda(d-1) \\ 0 & \lambda(d-1) & 0 \end{pmatrix}.$$

(2) Conclude that $p \in \mathrm{V}(H(P))$ if and only if $a = 0$.

This completes our proof of Theorem 2.2.27. In practice, we use the Hessian to locate inflection points even if $\mathrm{V}(P)$ is not smooth by finding the points of intersection of $\mathrm{V}(P)$ and $\mathrm{V}(H(P))$ and eliminating those that are singular on $\mathrm{V}(P)$.

EXERCISE 2.2.35. Let $P(x,y,z)$ be an irreducible second degree homogeneous polynomial. Using the Hessian curve, show that $\mathrm{V}(P)$ has no points of inflection.

We conclude this section with the following theorem, which we state without proof. Theorem 2.2.36 is a direct result of Bézout's theorem, which we will prove in Section 3.3.27.

THEOREM 2.2.36. *Two cubic curves in $\mathbb{P}^2$ will intersect in exactly $3 \times 3 = 9$ points, counted up to intersection multiplicities.*

EXERCISE 2.2.37. Use Exercise 2.2.22 and Theorem 2.2.27 to show that if $\mathrm{V}(P)$ is a smooth cubic curve, then $\mathrm{V}(P)$ has exactly nine inflection points.

EXERCISE 2.2.38. Find all nine points of inflection of the Fermat curve, $P(x,y,z) = x^3 + y^3 + z^3$.

2.3. Group Law

The goal of this section is to illustrate that, as a consequence of their geometric structure, smooth cubic curves are abelian groups. While the group law can be stated algebraically, in this section we will develop it geometrically to see why it is important for the curve to have degree three.

2.3.1. Adding points on smooth cubics. Let $\mathcal{C}$ denote a smooth cubic curve in the projective plane, $\mathbb{P}^2(\mathbb{C})$. We will develop a geometric method for adding points so that $\mathcal{C}$ is an abelian group under this operation. First, we define an abelian group.

DEFINITION 2.3.1. A *group* is a set G equipped with a binary operation $\star$ satisfying the following axioms:

(G1) The binary operation is associative, i.e.,

$$g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3$$

for all $g_1, g_2, g_3 \in G$.

(G2) There is an (unique) identity element $e \in G$ such that $e \star g = g = g \star e$ for all $g \in G$.

(G3) For each $g \in G$, there is an (unique) inverse element $g' \in G$ satisfying $g \star g' = e = g' \star g$.

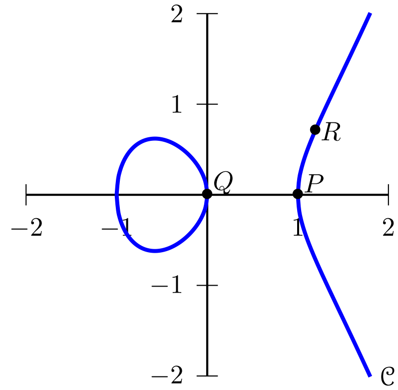
A group G is said to be an *abelian group* if, in addition, the binary operation $\star$ is commutative, i.e., $g_1 \star g_2 = g_2 \star g_1$ for all $g_1, g_2 \in G$.

For points P and Q on $\mathcal{C}$, let $\ell(P, Q)$ denote the line in $\mathbb{P}^2$ through P and Q. In case P and Q are the same point, let $\ell(P, P)$ be the line tangent to $\mathcal{C}$ at P. (This is why we must assume the cubic curve $\mathcal{C}$ is smooth, in order to ensure there is a well-defined tangent line at every point.) In Section 2.2.3 we saw that the Fundamental Theorem of Algebra ensures there are exactly three points of intersection of $\ell(P, Q)$ with the cubic curve $\mathcal{C}$, counting multiplicities. Let PQ denote this unique third point of intersection, so that the three points of intersection of $\mathcal{C}$ with $\ell(P, Q)$ are P, Q and PQ. In the event that a line ℓ is tangent to $\mathcal{C}$ at P, then the multiplicity of P is at least two by Exercise 2.2.17. Therefore, if $P \neq Q$ and $\ell(P, Q)$ is tangent to $\mathcal{C}$ at P, then $PQ = P$, for P counted the second time is the third point of intersection of $\ell(P, Q)$ with $\mathcal{C}$. The rule $(P, Q) \mapsto PQ$ gives a binary operation on $\mathcal{C}$, which is called the *chord-tangent composition law*.

EXERCISE 2.3.1. Explain why the chord-tangent composition law is commutative, i.e., $PQ = QP$ for all points P, Q on $\mathcal{C}$.

While this is a well-defined, commutative binary operation on $\mathcal{C}$, the following exercises illustrate that the chord-tangent composition law lacks the properties required of a group law.

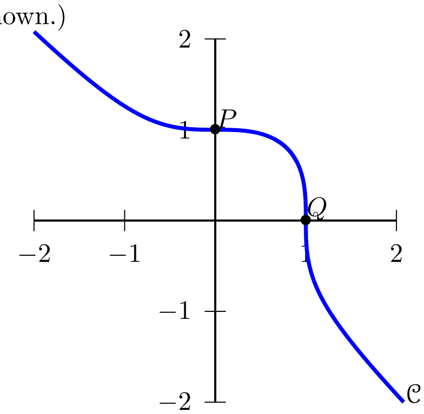
EXERCISE 2.3.2. Consider the cubic curve $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 - x\}$ and the points P, Q, R on $\mathcal{C}$, as shown below. (Note that only the real part of $\mathcal{C}$ is shown.)



Using a straightedge, locate PQ and then $(PQ)R$ on the curve $\mathcal{C}$. Now locate the point QR and the point $P(QR)$ on the curve $\mathcal{C}$. Is it true that $P(QR) = (PQ)R$? That is, is the chord-tangent composition law associative for these points on $\mathcal{C}$?

The preceding exercise demonstrates that the chord-tangent composition law is not associative. The next exercise illustrates that associativity is not the only group axiom that fails for the chord-tangent composition law.

Exercise 2.3.3. Consider the cubic curve $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid x^3 + y^3 = 1\}$. and the points $P = (0, 1)$ and $Q = (1, 0)$ on $\mathcal{C}$, as shown below. (Again, we note that only the real part is shown.)



(1) Using the equation of the cubic curve $\mathcal{C}$ and its Hessian, verify that P and Q are inflection points of $\mathcal{C}$.
(2) Verify that $PP = P$. Conclude that if $\mathcal{C}$ has an identity element e, then $e = P$.
(3) Verify that $QQ = Q$. Conclude that if $\mathcal{C}$ has an identity element e, then $e = Q$.
(4) Conclude that $\mathcal{C}$ does not have an identity element for the chord-tangent composition law.

Therefore, the chord-tangent composition law will not serve as a binary operation for the group structure on $\mathcal{C}$ because it violates both axioms (G1) and (G2).

However, we can find a way to make this work. By using the chord-tangent composition law twice in combination with a fixed inflection point, we will construct the group law on $\mathcal{C}$ in the next subsection.

2.3.2. Group Law with an Inflection Point. Let $\mathcal{C}$ denote a smooth cubic curve in the projective plane, $\mathbb{P}^2(\mathbb{C})$. As we showed in Exercise 2.2.37 , there are nine points of inflection (counting multiplicity) on $\mathcal{C}$. These are the points of intersection of the cubic curve, $\mathcal{C}$, with its Hessian curve.

Select a point of inflection O on $\mathcal{C}$. We define our binary operation, $+$, relative to this specific point O. For points P, Q on $\mathcal{C}$, define $P+Q$ to be the unique third point of intersection of $\ell(O, PQ)$ with $\mathcal{C}$, where PQ denotes the chord-tangent composition of P and Q. That is, $P+Q = O(PQ)$, using the chord-tangent composition law notation. We claim that with this binary operation $+$, $\mathcal{C}$ is an abelian group, and we call this operation addition, i.e. we can "add" points on $\mathcal{C}$.

We will prove that for a given choice of inflection point, O, the cubic curve $\mathcal{C}$ with addition of points relative to O is an abelian group. Before we verify this claim, let's consider a specific example.

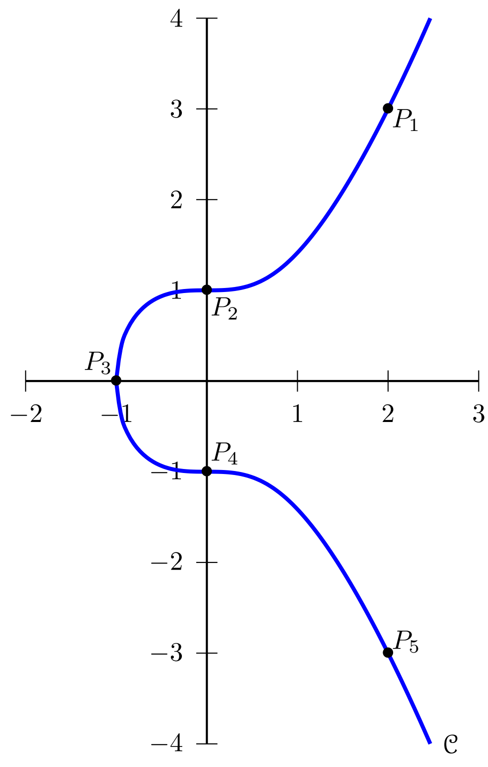


FIGURE 1. The cubic curve $\mathcal{C} = V(x^3 - y^2z + z^3)$ in the affine patch $z = 1$

Consider the cubic curve $\mathcal{C} = V(x^3 - y^2z + z^3) \subset \mathbb{P}^2$, and the points $P_1 = (2 : 3 : 1)$, $P_2 = (0 : 1 : 1)$, $P_3 = (-1 : 0 : 1)$, $P_4 = (0 : -1 : 1)$, $P_5 = (2 : -3 : 1)$ on $\mathcal{C}$. Figure 2.3.2 shows $\mathcal{C}$ in the affine patch $z = 1$.

Exercise 2.3.4. Use the equations of the cubic curve $\mathcal{C}$ and its Hessian to verify that P_2 and P_4 are inflection points of $\mathcal{C}$.

Exercise 2.3.5. Let $O = P_2$ be the specified inflection point so that $+$ is defined relative to P_2, i.e. $Q + R = P_2(QR)$ for points Q, R on $\mathcal{C}$.

(1) Compute $P_1 + P_2$, $P_2 + P_2$, $P_3 + P_2$, $P_4 + P_2$, and $P_5 + P_2$.
(2) Explain why P_2 is the identity element for $\mathcal{C}$.
(3) Find the inverses of P_1, P_2, P_3, P_4 and P_5 on $\mathcal{C}$.
(4) Verify that $P_1 + (P_3 + P_4) = (P_1 + P_3) + P_4$. In general, addition of points on $\mathcal{C}$ is associative.

Exercise 2.3.6. Now let $O = P_4$ be the specified inflection point so that $+$ is defined relative to P_4, i.e. $Q + R = P_4(QR)$ for points Q, R on $\mathcal{C}$.

(1) Compute $P_1 + P_2$, $P_2 + P_2$, $P_3 + P_2$, $P_4 + P_2$, and $P_5 + P_2$. [Hint: For $P_4 + P_2$ and $P_5 + P_2$ find the equations of the lines $\ell(P_4, P_2)$ and $\ell(P_5, P_2)$, respectively, to find the third points of intersection with $\mathcal{C}$.] Are the answers the same as they were in part (1) of Exercise 2.3.5? Is P_2 still the identity element for $\mathcal{C}$?
(2) Now compute $P_1 + P_4$, $P_2 + P_4$, $P_3 + P_4$, $P_4 + P_4$, and $P_5 + P_4$. Explain why P_4 is now the identity element for $\mathcal{C}$.
(3) Using the fact that P_4 is now the identity element on $\mathcal{C}$, find the inverses of P_1, P_2, P_3, P_4 and P_5 on $\mathcal{C}$. [Hint: See the hint on part (1).] Are these the same as the inverses found in part (3) of Exercise 2.3.5?

Now we will prove that the cubic curve $\mathcal{C}$ with addition of points relative to a fixed inflection point O is an abelian group. First, we verify that the binary operation $+$ is commutative.

Exercise 2.3.7. Explain why $P + Q = Q + P$ for all points P, Q on $\mathcal{C}$. This establishes that $+$ is a commutative binary operation on $\mathcal{C}$.

In Exercises 2.3.5 and 2.3.6, the inflection point used to define the addition also served as the identity element for the curve $\mathcal{C} = V(x^3 - y^2z + z^3)$. In the exercise below, you will show this is true for any cubic curve.

Exercise 2.3.8. Let $\mathcal{C}$ be a smooth cubic curve and let O be one of its inflection points. Define addition, $+$, of points on $\mathcal{C}$ relative to O. Show that $P + O = P$ for all points P on $\mathcal{C}$ and that there is no other point on $\mathcal{C}$ with this property. Thus O is the identity element for $+$ on $\mathcal{C}$.

Thus $(\mathcal{C}, O, +)$ satisfies group axiom (G2). Next, we verify that every point P on $\mathcal{C}$ has an inverse, so that $\mathcal{C}$ with $+$ also satisfies group axiom (G3).

EXERCISE 2.3.9. Let $\mathcal{C}$ be a smooth cubic curve and let O be one of its inflection points. Define addition, $+$, of points on $\mathcal{C}$ relative to the identity O.

(1) Suppose that P, Q, R are collinear points on $\mathcal{C}$. Show that $P+(Q+R) = O$ and $(P+Q)+R = O$.
(2) Let P be any point on $\mathcal{C}$. Assume that P has an inverse element P^{-1} on $\mathcal{C}$. Prove that the points P, P^{-1}, and O must be collinear.
(3) Use the results of parts (1) and (2) to show that for any P on $\mathcal{C}$ there is an element P' on $\mathcal{C}$ satisfying $P + P' = P' + P = O$, i.e. every element P has an inverse P^{-1}. Then show this inverse is unique.

So far we have shown that $(\mathcal{C}, O, +)$ has an identity, inverses, and is commutative. All that remains in order to prove that $\mathcal{C}$ is an abelian group is to show that $+$ is an associative operation. Establishing this fact is more involved than verifying the other axioms.

The following three exercises are based on [**Ful69**], pages 124-125. We will first develop some results regarding families of cubic curves.

EXERCISE 2.3.10. Start with two cubic curves, $\mathcal{C} = V(f)$ and $\mathcal{D} = V(g)$. By Theorem 2.2.36, there are exactly nine points of intersection, counting multiplicities, of $\mathcal{C}$ and $\mathcal{D}$. Denote these points by $P_1, P_2, \ldots, P_9$.

(1) Let $\lambda, \mu \in \mathbb{C}$ be arbitrary constants. Show that $P_1, P_2, \ldots, P_9$ are points on the cubic curve defined by $\lambda f + \mu g = 0$.
(2) Let $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{C}$ be arbitrary constants. Show that $P_1, P_2, \ldots, P_9$ are the nine points of intersection of the cubic curves $\mathcal{C}_1 = V(\lambda_1 f + \mu_1 g)$ and $\mathcal{C}_2 = V(\lambda_2 f + \mu_2 g)$.

Let $F(x, y, z) = a_1x^3 + a_2x^2y + a_3x^2z + a_4xy^2 + a_5xyz + a_6xz^2 + a_7y^3 + a_8y^2z + a_9yz^2 + a_{10}z^3$ be a cubic whose coefficients, $a_1, a_2, \ldots, a_{10}$, are viewed as unknowns. Then, for any point $P = (x_0 : y_0 : z_0)$ in $\mathbb{P}^2$, the equation $F(P) = 0$ gives a linear equation in the unknown coefficients, a_i. Explicitly, we obtain the linear equation

$$\begin{gathered} a_1x_0^3 + a_2x_0^2y_0 + a_3x_0^2z_0 + a_4x_0y_0^2 + a_5x_0y_0z_0 + \\ a_6x_0z_0^2 + a_7y_0^3 + a_8y_0^2z_0 + a_9y_0z_0^2 + a_{10}z_0^3 = 0. \end{gathered}$$

Recall that the coordinates of P are only determined up to non-zero scalar multiple. Since $F(x, y, z)$ is homogeneous of degree three, we have $F(\lambda x_0, \lambda y_0, \lambda z_0) = \lambda^3 F(x_0, y_0, z_0)$. Therefore, the zero set of the equation in the ten unknowns $a_1, a_2, \ldots, a_{10}$ is uniquely determined by P.

EXERCISE 2.3.11. Consider eight distinct points in $\mathbb{P}^2$, say $P_1, P_2, \ldots, P_8$, that are in *general position*, which for us means that no four are collinear and no seven are on a single conic. Let F be a generic cubic polynomial with unknown coefficients $a_1, a_2, \ldots, a_{10}$. The system of simultaneous equations $F(P_1) = F(P_2) = \cdots = F(P_8) = 0$ is a system of eight linear equations in the ten unknowns $a_1, a_2, \ldots, a_{10}$.

(1) Show that if the eight points $P_1, P_2, \ldots, P_8$ are in general position, then the rank of the linear system $F(P_1) = F(P_2) = \cdots = F(P_8) = 0$ is equal to 8.
(2) Use the Rank-Nullity theorem from linear algebra to show that there are two "linearly independent" cubics $F_1(x, y, z)$ and $F_2(x, y, z)$ such that any cubic curve passing through the eight points $P_1, P_2, \ldots, P_8$ has the form $\lambda F_1 + \mu F_2$.
(3) Conclude that for any collection of eight points in general position, there is a *unique* ninth point P_9 such that *every* cubic curve passing through the eight given points must also pass through P_9.

In this next exercise, we prove the associativity of the newly defined addition of points on a smooth cubic curve.

EXERCISE 2.3.12. Let $\mathcal{C}$ be a smooth cubic curve in $\mathbb{P}^2$ and let P, Q, R be three points on $\mathcal{C}$. We will show that $P + (Q + R) = (P + Q) + R$.

- Let $V(l_1) = \ell(P, Q)$ and $S_1 = PQ$, so $V(l_1) \cap \mathcal{C} = \{P, Q, S_1\}$.
- Let $V(l_2) = \ell(S_1, O)$ and $S_2 = OS_1 = P + Q$, so $V(l_2) \cap \mathcal{C} = \{S_1, O, S_2\}$.
- Let $V(l_3) = \ell(S_2, R)$ and $S_3 = (P + Q)R$, so $V(l_3) \cap \mathcal{C} = \{S_2, R, S_3\}$.

Similarly,

- Let $V(m_1) = \ell(Q, R)$ and $T_1 = QR$, so $V(m_1) \cap \mathcal{C} = \{Q, R, T_1\}$.
- Let $V(m_2) = \ell(T_1, O)$ and $T_2 = OT_1 = Q + R$, so $V(m_2) \cap \mathcal{C} = \{T_1, O, T_2\}$.
- Let $V(m_3) = \ell(T_2, P)$ and $T_3 = P(Q + R)$, so $V(m_3) \cap \mathcal{C} = \{T_2, P, T_3\}$.

(1) Notice that $\mathcal{C}' = V(l_1 m_2 l_3)$ is a cubic. Find $\mathcal{C}' \cap \mathcal{C}$.
(2) Likewise, $\mathcal{C}'' = V(m_1 l_2 m_3)$ is a cubic. Find $\mathcal{C}'' \cap \mathcal{C}$.
(3) Using parts (1) and (2) together with Exercise 2.3.11, deduce that $(P + Q)R = P(Q + R)$.
(4) Explain why $(P+Q)R = P(Q+R)$ implies that $(P+Q)+R = P+(Q+R)$. Conclude that the addition of points on cubics is associative.

Therefore, a cubic curve $\mathcal{C}$ with a selected inflection point O determines a binary operation, $+$, in such a way that $(\mathcal{C}, O, +)$ is an abelian group under addition.[2]

[2]We defined addition on $\mathcal{C}$ relative to an inflection point, O, but we could define addition on $\mathcal{C}$ relative to any point O on $\mathcal{C}$. See Husemöller, "Elliptic Curves", Theorem 1.2 for details.

Since $(\mathcal{C}, O, +)$ is a group, it is natural to ask group theoretic questions about $\mathcal{C}$, such as questions regarding the orders of its elements. First we define an integer multiple of a point and the order of a point.

Definition 2.3.2. Let $(\mathcal{C}, O, +)$ be a smooth cubic curve and let $P \neq O$ be a point on the curve. For $n \in \mathbb{Z}$ we define $n \cdot P$ as follows:

- $0 \cdot P = O$ and $1 \cdot P = P$
- For $n \geq 2$, we have $n \cdot P = (n-1)\,P + P$
- For $n < 0$, we set $n \cdot P$ to be the inverse of $-n \cdot P$.

Definition 2.3.3. Let $(\mathcal{C}, O, +)$ be a smooth cubic curve and let $P \neq O$ be a point on the curve. If there exists a positive integer n so that $n \cdot P = O$ and for $1 \leq m \leq n-1$ we have $m \cdot P \neq O$, then the point P has *order* n. If no such positive integer exists, then the point is said to have *infinite order*.

We can now examine points of finite order. In particular, we are interested here in points of order two and three. Many areas of mathematics are concerned with the computation of the order of various points on a cubic curve.

2.3.3. Points of Order Two and Three. Let $\mathcal{C}$ be a smooth cubic curve with $+$ defined relative to the inflection point O, the group identity. Let P be a point on $\mathcal{C}$.

Exercise 2.3.13. Show that $2P = O$ if and only if $\ell(O, P)$ is tangent to $\mathcal{C}$ at P.

Exercise 2.3.14. Show that if P and Q are two points on $\mathcal{C}$ of order two, then PQ, the third point of intersection of $\mathcal{C}$ with $\ell(P, Q)$, is also a point of order two on $\mathcal{C}$.

Exercise 2.3.15. Let $\mathcal{C}$ be the cubic curve defined by $y^2 z = x^3 - xz^2$. Graph $\mathcal{C}$ in the affine patch $z = 1$, and find three points of order two.

Let $\mathcal{C}$ be a smooth cubic curve with $+$ defined relative to the inflection point O.

Exercise 2.3.16. Let P be any inflection point on $\mathcal{C}$. Show that $3P = O$.

Exercise 2.3.17. Suppose P is point on $\mathcal{C}$ and $3P = O$. Conclude that $PP = P$. From this, deduce that P is a point of inflection on $\mathcal{C}$.

We will return to points of finite order in section 2.4.3 after we have developed a more convenient way to express our smooth cubic curves.

2.4. Normal forms of cubics

The goal of this section[3] is to show that every smooth cubic is projectively equivalent to one of the form $y^2 = x^3 + Ax + B$, the Weierstrass normal form, where the coefficients A and B are determined uniquely. See Equation (2.7). We will also show that every smooth cubic is projectively equivalent to the canonical form $y^2 = x(x-1)(x-\lambda)$. See Equation 2.4.24. The value of λ, however, is not uniquely determined, as there are six values of λ for the same cubic. We associate to each cubic a complex number and vice versa showing that we can parametrize all cubics by the complex numbers. Using this, in the next section we will give an algebraic characterization of the group law, which may then be used not only in characteristic zero, but for positive characteristics and even over non-algebraically closed fields such as $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}_p$.

2.4.1. Weierstrass Normal Form.

One set of problems will be to achieve the goals outlined above for a general cubic curve $\mathcal{C}$. The other set of problems consists of carrying out the computations with a concrete example, the curve $\{x^3 + y^3 - z^3 = 0\}$.

Let $\mathcal{C}$ be a smooth cubic curve in $\mathbb{P}^2$ given by the homogeneous equation $f(x, y, z) = 0$. Select an inflection point, $O = (a_0 : b_0 : c_0)$, on $\mathcal{C}$ and let ℓ denote the tangent line to $\mathcal{C}$ at O, where ℓ is defined by the linear equation l(x,y,z)=0. Recall that we can projectively change coordinates with an invertible 3×3 matrix M.

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} = M \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

We choose M so that

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = M \begin{pmatrix} a_0 \\ b_0 \\ c_0 \end{pmatrix}$$

and ℓ is transformed to the line defined by $l_1(x_1, y_1, z_1) = z_1$, i.e. the inflection point O becomes and $(0 : 1 : 0)$ and the tangent line ℓ becomes the line $\{z_1 = 0\}$ under the projective change of coordinates M. Recall, that we actually carry out the computations of changing coordinates by using the inverse M^{-1} of M and replacing x, y, and z with expressions involving x_1, y_1, and z_1.

Exercise 2.4.1. Consider the smooth cubic curve $\mathcal{C}$ defined by $x^3+y^3-z^3 = 0$.

(1) Show that $O = (1 : 0 : 1)$ is an inflection point of $\mathcal{C}$.

[3] The development in this section follows the first two sections of chapter three of J. Silverman's *The Arithmetic of Elliptic Curves*.

(2) Show that $x - z = 0$ is the equation of the tangent line to $\mathcal{C}$ at O.

(3) Find a 3×3 matrix M such that, under the change of variables

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = M^{-1} \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix},$$

we have $(1 : 0 : 1) \mapsto (0 : 1 : 0)$ and $l(x, y, z) = x - z$ becomes $l_1(x_1, y_1, z_1) = z_1$.

(4) Find the equation, $f_1(x_1, y_1, z_1) = 0$, for the curve $\mathcal{C}_1$ that is associated to this projective change of coordinates.

Now we have transformed our original smooth cubic curve $\mathcal{C}$ into another smooth cubic curve $\mathcal{C}_1$, which is projectively equivalent to $\mathcal{C}$. Let's now work with the new curve $\mathcal{C}_1$ that is defined by the equation $f_1(x_1, y_1, z_1) = 0$ in $\mathbb{P}^2$ with coordinates $(x_1 : y_1 : z_1)$.

Exercise 2.4.2.

(1) Explain why the homogeneous polynomial $f_1(x_1, y_1, z_1)$ can be expressed as

$$f_1(x_1, y_1, z_1) = \alpha x_1^3 + z_1 F(x_1, y_1, z_1),$$

where $\alpha \neq 0$ and $F(0, 1, 0) \neq 0$.

(2) Explain why the highest power of y_1 in the homogeneous polynomial $f_1(x_1, y_1, z_1)$ is two.

(3) Explain how by rescaling we can introduce new coordinates $(x_2 : y_2 : z_2)$ so that the coefficient of x_2^3 is 1 and the coefficient of $y_2^2 z_2$ is -1 in the new homogeneous polynomial $f_2(x_2, y_2, z_2) = 0$.

We can now rearrange the equation $f_2(x_2, y_2, z_2) = 0$ to be of the form

$$y_2^2 z_2 + a_1 x_2 y_2 z_2 + a_3 y_2 z_2^2 = x_2^3 + a_2 x_2^2 z_2 + a_4 x_2 z_2^2 + a_6 z_2^3. \tag{2.2}$$

Exercise 2.4.3. Refer to the curve defined in Exercise 2.4.1 for the following.

(1) Show that the matrix

$$M^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

does what we want for part (3) of Exercise 2.4.1.

(2) Find the homogeneous polynomial $f_1(x_1, y_1, z_1)$ that corresponds to this projective change of coordinates.

(3) Verify that f_1 is of the form $f_1(x_1, y_1, z_1) = \alpha x_1^3 + z_1 F(x_1, y_1, z_1)$, where $\alpha \neq 0$ and $F(0, 1, 0) \neq 0$.

(4) Rescale, if necessary, so that the coefficient of x_2 is 1 and the coefficient of $y_2^2 z_2$ is -1.
(5) Rearrange $f_2(x_2, y_2, z_2) = 0$ to be in the form of equation (2.2).

Let's now work in the affine patch $z_2 = 1$, that is, in the affine (x_2, y_2) plane, and consider the nonhomogeneous form of equation (2.2),

$$y_2^2 + a_1 x_2 y_2 + a_3 y_2 = x_2^3 + a_2 x_2^2 + a_4 x_2 + a_6, \tag{2.3}$$

keeping in mind that there is an extra point at infinity. We can treat the left-hand side of equation (2.3) as a quadratic expression in y_2. This means we can complete the square to remove some of the terms.

Consider the following concrete examples.

Exercise 2.4.4.

(1) Complete the square on the left hand side of the following equation.

$$y^2 + 2y = 8x^3 + x - 1$$

(2) Find an affine change of coordinates so that $y^2 + 2y = 8x^3 + x - 1$ becomes $v^2 = f(u)$.

Exercise 2.4.5.

(1) Complete the square (with respect to y) on the left hand side of the following equation.

$$y^2 + 4xy + 2y = x^3 + x - 3$$

(2) Find an affine change of coordinates such that $y^2 + 2y = 8x^3 + x - 1$ becomes $v^2 = f(u)$.

Now we can do this in general.

Exercise 2.4.6. Complete the square on the left-hand side of equation (2.3) and verify that the affine change of coordinates

$$x_3 = x_2$$
$$y_3 = a_1 x_2 + 2y_2 + a_3$$

gives the new equation

$$y_3^2 = 4x_3^3 + (a_1^2 + 4a_2)x_3^2 + 2(a_1 a_3 + 2a_4)x_3 + (a_3^2 + 4a_6) \tag{2.4}$$

To simplify notation, we introduce the following.

$$b_2 = a_1^2 + 4a_2$$
$$b_4 = a_1 a_3 + 2a_4$$
$$b_6 = a_3^2 + 4a_6$$

so that equation (2.4) becomes

$$y_3^2 = 4x_3^3 + b_2 x_3^2 + 2b_4 x_3 + b_6. \tag{2.5}$$

We are now ready to make the final affine change of coordinates to achieve the Weierstrass normal form. Our goal is to scale the coefficient of x_3^3 to 1 and to eliminate the x_3^2 term. [4]

Consider the following concrete examples.

EXERCISE 2.4.7.

(1) Suppose we have the equation

$$y^2 = x^3 + 6x^2 - 2x + 5.$$

Show that the affine change of coordinates

$$u = x + 2$$
$$v = y$$

eliminates the quadratic term on the right hand side.

(2) Suppose we have the equation

$$y^2 = 4x^3 + 12x^2 + 4x - 6.$$

Show that the affine change of coordinates

$$u = 36x + 36$$
$$v = 108y$$

eliminates the quadratic term and rescales the coefficient of the cubic term to one on the right hand side.

EXERCISE 2.4.8. Verify that the affine change of coordinates

$$u = 36x_3 + 3b_2$$
$$v = 108y_3$$

gives the Weierstrass normal form

$$v^2 = u^3 - 27(b_2^2 - 24b_4)u - 54(b_2^3 + 36b_2b_4 - 216b_6).$$

[4] This change of coordinates is similar to completion of the square, but with cubics. This was first used by Cardano in *Ars Magna* (in 1545) to achieve a general solution to the cubic equation $x^3+\alpha x^2+\beta x+\gamma = 0$. He needed to eliminate the x^2 term then, as we do now. Since the coefficient of the cubic term inhis equation is already one, he simply made the substitution $u = x - \alpha/3$.

Again we can introduce the following to simplify notation.

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Then we have the following for our Weierstrass normal form.

$$v^2 = u^3 - 27c_4u - 54c_6 \tag{2.6}$$

Let's collect all of the coefficient substitutions that we have made. Recall that the a_i's are the coefficients from equation (2.3). Then we have the following.

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

For upcoming computations it is convenient to introduce the following as well.

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= \frac{c_4^3}{\Delta} \end{aligned}$$

Exercise 2.4.9. Show the following relationships hold.

(1) $4b_8 = b_2b_6 - b_4^2$
(2) $1728\Delta = c_4^3 - c_6^2$
(3) $j = \dfrac{1728c_4^3}{c_4^3 - c_6^2}$

These are simply brute-force computations.

Δ is called the discriminant of the cubic curve. The discriminant of a polynomial is an expression in the coefficients of a polynomial which is zero if and only if the polynomial has a multiple root. For example, the quadratic equation $ax^2 + bx + c = 0$ has a multiple root if and only if $b^2 - 4ac = 0$. Similarly, the cubic equation $\alpha x^3 + \beta x^2 + \gamma x + \delta = 0$ has a multiple root if and only if

$$\beta^2\gamma^2 - 4\alpha\gamma^3 - 4\beta^3\delta - 27\alpha^2\delta^2 + 18\alpha\beta\gamma\delta = 0.$$

The discriminant Δ given above is the discriminant (up to a factor of 16) of the right hand side cubic in equation (2.5). The number j defined above is called the j-invariant of the cubic curve. We will see its significance soon.

EXERCISE 2.4.10. Follow the procedure outlined above to write the following cubics in Weierstrass normal form and use part (3) of Exercise 2.4.9 to calculate their j- invariants.

(1) $y^2 + 2y = 8x^3 + x - 1$
(2) $y^2 + 4xy + 2y = x^3 + x - 3$

To avoid even more cumbersome notation, let's "reset" our variables. Consider the Weierstrass normal form of a smooth cubic $\mathcal{C}$:

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{2.7}$$

Notice that with the specific example $x^3 + y^3 - z^3 = 0$ in $\mathbb{P}^2$ in exercises 2.4.1 and 2.4.3, we chose the initial change of coordinates, the transformation M, so that the inflection point is $(0 : 1 : 0)$ with tangent line given by $z = 0$, but this is not a unique transformation. Suppose we had chosen a different transformation. That is, suppose instead of having the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

we obtained the equation

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'.$$

How different would our Weierstrass normal form have been?

EXERCISE 2.4.11. Show that the only (affine) transformation that takes

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

to

$$v^2 + a_1'uv + a_3'v = u^3 + a_2'u^2 + a_4'u + a_6'$$

is given by

$$\begin{aligned} x &= \alpha^2u + r \\ y &= \alpha^2su + \alpha^3v + t, \end{aligned}$$

with $\alpha, r, s, t \in \mathbb{C}$ and $\alpha \neq 0$. [Hint: Start with the projective transformation, which is also affine,

$$\begin{aligned} x &= a_{11}u + a_{12}v + a_{13}w \\ y &= a_{21}u + a_{22}v + a_{23}w \\ z &= w \end{aligned}$$

and show that the only way to satisfy the condition in this exercise is for the specific a_{ij} to have the form above.]

Using this change of coordinates, we can compute the following relationships[5] between equivalent cubic curves with coefficients a_i in equation (2.2) with coordinates $(x : y : z)$ and coefficients a'_i with coordinates $(u : v : w)$.

$$
\begin{aligned}
\alpha a'_1 &= a_1 + 2s \\
\alpha^2 a'_2 &= a_2 - sa_1 + 3r - s^2 \\
\alpha^3 a'_3 &= a_3 + ra_1 + 2t \\
\alpha^4 a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
\alpha^6 a'_6 &= a_6 + ra_4 - ta_3 + r^2 a_2 - rta_1 + r^3 - t^2
\end{aligned}
$$

$$
\begin{aligned}
\alpha^2 b'_2 &= b_2 + 12r \\
\alpha^4 b'_4 &= b_4 + rb_2 + 6r^2 \\
\alpha^6 b'_6 &= b_6 + 2rb_4 + r^2 b_2 + 4r^3 \\
\alpha^6 b'_8 &= b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4
\end{aligned}
$$

$$
\begin{aligned}
\alpha^4 c'_4 &= c_4 \\
\alpha^6 c'_6 &= c_6 \\
\alpha^{12} \Delta' &= \Delta \\
j' &= j
\end{aligned}
$$

Notice that if two smooth cubic plane curves are projectively equivalent, then the value j for each is the same, which is why we call this number the j-invariant. Let $\mathcal{C}$ and $\mathcal{C}'$ be two cubic plane curves, written in Weierstrass normal form.

$$
\begin{aligned}
\mathcal{C} &: y^2 = x^3 + Ax + B \\
\mathcal{C}' &: y^2 = x^3 + A'x + B'
\end{aligned}
$$

EXERCISE 2.4.12. Suppose $\mathcal{C}$ and $\mathcal{C}'$ have the same j-invariant.

(1) Show that this implies
$$\frac{A^3}{4A^3 + 27B^2} = \frac{A'^3}{4A'^3 + 27B'^2}.$$
(2) Show that from the previous part we have $A^3 B'^2 = A'^3 B^2$.

In the next exercises we construct the transformations that send $\mathcal{C}$ to $\mathcal{C}'$. We need to consider three cases: $A = 0$, $B = 0$, $AB \neq 0$.

[5] This is Table 1.2 in Silverman's book.

Exercise 2.4.13. Suppose $A = 0$.

(1) Show that if $A = 0$, then $B \neq 0$. [Hint: Recall, $\mathcal{C}$ is smooth.]
(2) What is j if $A = 0$?
(3) Explain why $B' \neq 0$.
(4) Show that the following change of coordinates takes $\mathcal{C}$ to $\mathcal{C}'$.

$$x = (B/B')^{1/3}u$$
$$y = (B/B')^{1/2}v$$

Exercise 2.4.14. Suppose $B = 0$.

(1) What is j if $B = 0$?
(2) Explain why $A' \neq 0$.
(3) Show that the following change of coordinates takes $\mathcal{C}$ to $\mathcal{C}'$.

$$x = (A/A')^{1/2}u$$
$$y = (A/A')^{3/4}v$$

Exercise 2.4.15. Suppose $AB \neq 0$. Find a change of coordinates that takes $\mathcal{C}$ to $\mathcal{C}'$. [Hint: See the two previous problems.]

We can summarize the preceding discussion with the following theorem.

Theorem 2.4.16. Two smooth cubic curves are projectively equivalent if and only if their j-invariants are equal.

The following exercises yield a characterization of smooth cubics via the j-invariant.

Exercise 2.4.17. Let γ be any complex number except 0 or 1728, and consider the cubic curve $\mathcal{C}$ defined as follows.

$$y^2 + xy = x^3 - \frac{36}{\gamma - 1728}x - \frac{1}{\gamma - 1728}$$

Compute j for this cubic.

Exercise 2.4.18. Compute j for the following cubics.

(1) $y^2 + y = x^3$
(2) $y^2 = x^3 + x$

Exercise 2.4.19. Use Theorem 2.4.16 and Exercises 2.4.10 and 2.4.18 to show that $V(x^3+xz^2-y^2z)$ and $V(8x^3+xz^2-y^2z-2yz^2-z^3)$ are projectively equivalent.

Exercises (2.4.17) and (2.4.18) establish the following theorem.

Theorem 2.4.20. If γ is any complex number, then there exists a plane cubic curve whose j-invariant is γ.

2.4.2. Canonical Form. As we have just seen the Weierstrass normal form is very useful and provides a nice way to characterize smooth plane cubics. Another form that is equally useful is the canonical form of the cubic. Consider equation (2.5) from above.

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

EXERCISE 2.4.21. Rewrite equation (2.5) on page 67 in (x_1, y_1) using the change of coordinates below.

$$x = x_1$$

$$y = 2y_1$$

The change of coordinates in Exercise 2.4.21 scales the cubic coefficient on the right hand side to one. Now we can factor the resulting equation from to obtain

$$y_1^2 = (x_1 - e_1)(x_1 - e_2)(x_1 - e_3). \tag{2.8}$$

EXERCISE 2.4.22. Show that e_1, e_2, e_3 are distinct. [Hint: Recall, the cubic curve $V((x - e_1z)(x - e_2z)(x - e_3z) - y^2z)$is smooth.]

Consider the following example.

EXERCISE 2.4.23. In Exercise 2.4.10 we found the Weierstrass normal form of $y^2 + 2y = 8x^3 + x - 1$ to be $y^2 = x^3 + \frac{1}{2}x$. Factor the right hand side to find values for e_1, e_2, and e_3.

Now we can do this in general.

EXERCISE 2.4.24. Rewrite equation (2.8) in (x_2, y_2) using the change of coordinates below.

$$x_1 = (e_2 - e_1)x_2 + e_1$$

$$y_1 = (e_2 - e_1)^{3/2}y_2$$

EXERCISE 2.4.25. Show that if we make the substitution

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1} \tag{2.9}$$

in the equation we found in Exercise 2.4.24, we get

$$y_2^2 = x_2(x_2 - 1)(x_2 - \lambda).$$

We say a smooth cubic is in canonical form if we can write

$$y^2 = x(x - 1)(x - \lambda). \tag{2.10}$$

EXERCISE 2.4.26. Find an affine transformation that puts $y^2 + 2y = 8x^3 + x - 1$ in canonical form. What is λ?

We digress for a moment here. By now we have become comfortable working in $\mathbb{P}^2$ and in various affine patches. We have seen that the context often determines when it is most advantageous to work in an affine patch. We usually work in the affine xy-plane, i.e. the $z = 1$ patch, but we need to be sure that we are not missing anything that happens "at infinity."

Exercise 2.4.27. Let $\mathcal{C} \subset \mathbb{P}^2$ be the smooth cubic defined by the homogeneous equation $y^2 z = x(x-z)(x-\lambda z)$. Show that the only "point at infinity" $(x_1 : y_1 : 0)$ on $\mathcal{C}$ is the point $(0 : 1 : 0)$. We will see the significance of the point $(0 : 1 : 0)$ in section 2.5.

In equation (2.8) we factored the right hand side and called the roots e_1, e_2, and e_3, but these labels are just labels. We could just as easily have written e_2, e_3, and e_1. In other words, we should get the same cubic curve no matter how we permuted the e_i's. There are $3! = 6$ distinct permutations of the set $\{e_1, e_2, e_3\}$, so we expect that there would be six equivalent ways to express our cubic in canonical form. Recall that we defined λ as a ratio in equation (2.9). Changing the roles of e_2 and e_3 would give $1/\lambda$ rather than λ. The two cubics

$$y^2 = x(x-1)(x-\lambda)$$

and

$$y^2 = x(x-1)(x-1/\lambda)$$

should still be equivalent.

Exercise 2.4.28. Suppose we have the following canonical cubic

$$y^2 = x(x-1)(x-\lambda),$$

where λ corresponds to the order e_1, e_2, e_3 of the roots in (2.8). Show that the other five arrangements of $\{e_1, e_2, e_3\}$ yield the following values in place of λ.

$$\frac{1}{\lambda} \qquad 1-\lambda \qquad \frac{1}{1-\lambda} \qquad \frac{\lambda-1}{\lambda} \qquad \frac{\lambda}{\lambda-1}$$

As we have seen the value of λ in a canonical form of $\mathcal{C}$ is almost uniquely determined by $\mathcal{C}$. The correspondence between complex numbers $\lambda \neq 0, 1$ and smooth cubic curves $\mathcal{C}$ is a six-to-one correspondence , where if λ is a complex number assigned to $\mathcal{C}$, then all of the complex numbers in exercise (2.4.28) are assigned to $\mathcal{C}$. Though λ is not uniquely determined, the j-invariant, as we would expect, is unique.

Exercise 2.4.29. Show that if a smooth cubic curve $\mathcal{C}$ has an equation in canonical form

$$y^2 = x(x-1)(x-\lambda),$$

then its j-invariant is

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

[Hint: Write the equation $y^2 = x(x-1)(x-\lambda)$ in Weirstrass normal form and use Exercise 2.4.9 to compute j.]

EXERCISE 2.4.30. Use the λ found in Exercise 2.4.26 to compute the j-invariant of $y^2 + 2y = 8x^3 + x - 1$. [Hint: Use the expression in Exercise 2.4.29.] Check that this agrees with the computation of j in Exercise 2.4.10.

EXERCISE 2.4.31. Show that the j-invariant of a smooth cubic curve $\mathcal{C}$ can be written as

$$2^7 \left[\sum_{i=1}^{6} \mu_i^2 - 3 \right],$$

where the μ_i range over the six values $\lambda, 1/\lambda, \ldots$ from exercise 2.4.28.

Exercise 2.4.31 demonstrates that the value of the j-invariant, while expressed in terms of a particular choice of λ associated to $\mathcal{C}$, is independent of which λ corresponding to $\mathcal{C}$ we select. When we combine Exercise 2.4.31 and Theorem 2.4.16 we see that, as we would expect, the six values in Exercise 2.4.28 really do give the same smooth cubic.

EXERCISE 2.4.32. Verify that the values of a_λ and b_λ are the same no matter which of the six options of λ is selected in the canonical form.

EXERCISE 2.4.33. I conjecture that $j(\lambda)$ is some natural invariant expressed in terms of a_λ and b_λ. Find this expression.

2.4.3. An Application: Points of Finite Order. As we have seen it is often convenient to express a smooth cubic in canonical form. For our final application in this section we will prove that there are exactly three points of order two on a smooth cubic. We showed in Exercise 2.3.14, that if we have two points P and Q of order two, then there is a third point PQ also of order two, but we are not assured of the existence of the two points P and Q or that there is not another point R, of order two, not collinear with P and Q. Exercise 2.3.15 suggests there are exactly three such points and now we set about proving this in general. Recall, in Exercise 2.3.13 we showed that a point $P \in \mathcal{C}$ has order two if and only if the tangent to $\mathcal{C}$ at P passes through the identity element O.

EXERCISE 2.4.34. Let $\mathcal{C} = V(x(x-1)(x-\lambda) - y^2)$ be a smooth cubic curve with $+$ defined relative to the inflection point $O = (0:1:0)$.

(1) Homogenize Equation 2.10 and find the equation of the tangent line $V(l)$ to $\mathcal{C}$ at the point $P = (x_0 : y_0 : z_0)$.

(2) Show that $(0:1:0) \in V(l)$ if and only if either $z_0 = 0$ or $y_0 = 0$.
(3) Show that O is the only point in $\mathcal{C} \cap V(l)$ with $z_0 = 0$.
(4) Show that $(0:0:1)$, $(1:0:1)$, and $(\lambda:0:1)$ are the only points in $\mathcal{C} \cap V(l)$ with $y_0 = 0$.
(5) Conclude that there are exactly three points of order two on $\mathcal{C}$.

We have just shown that any cubic $\mathcal{C}$ has exactly three points of order two. In fact, we have found these points explicitly, but we can say even more.

EXERCISE 2.4.35. (1) Show that the points of order two on $\mathcal{C}$, together with $O = (0:1:0)$, form a subgroup of $\mathcal{C}$.
(2) Show that this subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We showed in Exercises 2.3.16 and 2.3.17 that a point $P \in \mathcal{C}$ satisfies $3P = O$ if and only if P is an inflection point. By Exercise 2.2.37 there are exactly nine inflection points on $\mathcal{C}$, but O has order one. Thus there are eight points of order three on $\mathcal{C}$.

In general, there are n^2 points on $\mathcal{C}$ whose order divides n. Hence there are twelve points of order four on $\mathcal{C}$, as there will be sixteen whose order divides four, but four of these are already counted among the three points of order two and O.

2.5. The Group Law for a Smooth Cubic in Canonical Form

The goal of this section is to reformulate the group law for a smooth cubic that it is already expressed in canonical form $y^2 = x(x-1)(x-\lambda)$. By doing so, we will see that the group law for cubics is valid not only over $\mathbb{C}$, but over fields of positive characteristic[6] and non-algebraically closed fields, too.

We have already shown that the set of points of a smooth cubic curve $\mathcal{C}$ forms a group under the binary operation $+$ we defined in Section 2.3.2. In what follows we will use the canonical form developed in Section 2.4 to determine the (affine) coordinates of the point $P + Q$ given coordinates of P and Q. We will use the point at infinity $(0:1:0)$ as our identity O on $\mathcal{C}$. When we work in the affine patch $z = 1$, we will see that the line $\ell(O, PQ)$ that we use to determine $P+Q$ will correspond to the vertical line through PQ.

2.5.1. The Identity, Addition, and Inverses. First, we need to establish that $O \in \mathcal{C}$ and that any vertical line in the affine xy-plane does indeed pass through O.

[6] We would need to modify our calculations from the previous sections for fields of characteristic two or three.

EXERCISE 2.5.1. Consider the cubic curve $\mathcal{C}$ in homogeneous canonical form given by $y^2z = x(x-z)(x+z)$, i.e. $\mathcal{C} = V(x^3 - xz^2 - y^2z)$.

(1) Show that the point at infinity $(0:1:0) \in \mathcal{C}$.
(2) Show that $(0:1:0) \in V(H(x^3 - xz^2 - y^2z))$, the Hessian curve of $\mathcal{C}$, and conclude that $O = (0:1:0)$ is an inflection point.
(3) Show that every vertical line in the affine xy-plane meets $\mathcal{C}$ at $(0:1:0)$.
(4) Sketch the graph of the real affine part of $\mathcal{C}$, $y^2 = x^3 - x$.
(5) Let P and Q be two points on the real affine curve. Show geometrically that if the line $\ell(P,Q)$ through P and Q intersects $\mathcal{C}$ a third time at the point $PQ = (a,b)$, then $P + Q = (a,-b)$.
(6) Now suppose that $R = (a:b:1)$ is a point on $\mathcal{C}$. Show that the line $\ell(O,R)$ is given by the equation $x - az = 0$, which is the vertical line $x = a$ in the xy-plane.

EXERCISE 2.5.2. Let $\lambda \neq 0, 1$ be a complex number and consider the cubic curve $\mathcal{C}$ in homogeneous canonical form given by $y^2z = x(x-z)(x-\lambda z)$, i.e. $\mathcal{C} = V(x(x-z)(x-\lambda z) - y^2z)$.

(1) Show that the point at infinity, $(0:1:0) \in \mathcal{C}$.
(2) Show that $(0:1:0) \in V(H(x(x-z)(x-\lambda z) - y^2z))$, the Hessian curve of $\mathcal{C}$, and conclude that $O = (0:1:0)$ is an inflection point.
(3) Show that every vertical line in the affine xy-plane meets $\mathcal{C}$ at O.
(4) Suppose that $P = (a:b:1)$ is a point on $\mathcal{C}$. Show that the line $\ell(O,P)$ is given by the equation $x - az = 0$, which is the vertical line $x = a$ in the (x,y)-plane.

Now we have established that if $\mathcal{C} = V(x(x-z)(x-\lambda z) - y^2z)$ is given in canonical form, then $(0:1:0)$ is an inflection point, so henceforth we let $O = (0:1:0)$ be our identity element. Since any vertical line ℓ in the affine xy-plane intersects $\mathcal{C}$ at O, we define $+$ relative to O and ℓ. Before we develop an algebraic expression for the coordinates of $P+Q$, we first consider the coordinates of P^{-1}, the inverse of the point P. Recall, that if $P \in \mathcal{C}$ then the inverse P^{-1} of P is the third point of intersection of $\mathcal{C}$ and $\ell(O,P)$.

EXERCISE 2.5.3. First, we want to work in the affine patch $z = 1$, so we dehomogenize our cubic equation, $y^2 = x(x-1)(x-\lambda)$. Let $P = (x_1, y_1)$ be a point in the xy-plane on $\mathcal{C}$ with $y_1 \neq 0$.

(1) Find the linear equation that defines $\ell(O,P)$.
(2) Find the point $P' = (x_2, y_2)$ that is the third point of intersection of $\ell(O,P)$ and $\mathcal{C}$ in the xy-plane.
(3) Show that $P + P' = O$. Conclude that $P' = P^{-1}$.

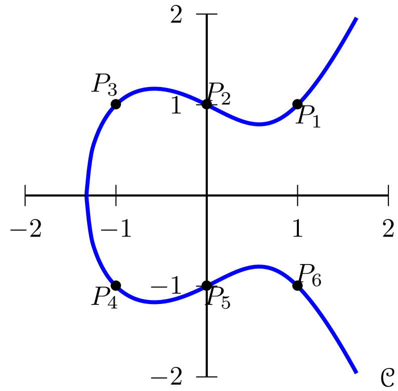


FIGURE 2. $\mathcal{C}$ in the affine xy-plane

Therefore, if $P = (x_1 : y_1 : 1)$ is a point on $\mathcal{C}$, the additive inverse of P is the point $P^{-1} = (x_1 : -y_1 : 1)$ on $\mathcal{C}$. Notice in Exercise 2.5.3 we assumed $y_1 \neq 0$ for our point P. Now we see what the inverse of a point on the x-axis in the affine xy-plane is.

EXERCISE 2.5.4. Let $P = (x_1, 0)$ be a point in the xy-plane on $\mathcal{C}$ defined by $y^2 = x(x-1)(x-\lambda)$.

(1) Show that $2P = O$, so that $P = P^{-1}$.
(2) Show that this agrees with Exercise 2.3.13, that is, show that the tangent to $\mathcal{C}$ at $P = (x_1, y_1)$ in the xy-plane is a vertical line if and only if $y_1 = 0$.

2.5.2. The Group Law. Our goal in this section is to obtain an algebraic formula for the sum of two points on a cubic in canonical form.

EXERCISE 2.5.5. Consider the cubic curve $\mathcal{C} = V(x^3 - xz^2 + z^3 - y^2 z)$ and the points $P_1 = (1 : 1 : 1)$, $P_2 = (0 : 1 : 1)$, $P_3 = (-1 : 1 : 1)$, $P_4 = (-1 : -1 : 1)$, $P_5 = (0 : -1 : 1)$, $P_6 = (1 : -1 : 1)$ on $\mathcal{C}$. Figure 2.5.5 shows $\mathcal{C}$ in the affine $z = 1$ patch.

(1) Use a straightedge and figure 2.5.5 to find $P_1 + P_2$, $P_1 + P_3$, $P_1 + P_4$, and $P_3 + P_4$ geometrically. [Hint: $O = (0 : 1 : 0)$, the point at infinity, is the identity and we use the vertical line through $P_i P_j$ to find $P_i + P_j$.]
(2) Find the coordinates of $P_1 + P_2$, $P_1 + P_3$, $P_1 + P_4$, and $P_3 + P_4$. [Hint: Use the equation of the line through P_i and P_j to find the coordinates of the point $P_i P_j$. Now find the coordinates of $P_i + P_j$ using the equation of the vertical line through $P_i P_j$.]

EXERCISE 2.5.6. Let $\mathcal{C}$ be the affine cubic curve defined by the equation $y^2 = x^3 + x^2 - 2x$. Let P denote the point $(-1/2, -3\sqrt{2}/4)$ and Q denote the point $(0, 0)$.

(1) Write the defining equation of $\mathcal{C}$ in canonical form and verify that P and Q are on $\mathcal{C}$.
(2) Find the equation of $\ell(P, Q)$, the line through P and Q.
(3) Find the coordinates of the point PQ on $\mathcal{C}$, that is, the coordinates of the third point of intersection of $\mathcal{C}$ and $\ell(P, Q)$.
(4) Let O denote the inflection point $(0 : 1 : 0)$ and find the coordinates of the point $P + Q$ on $\mathcal{C}$ using O as the identity element.
(5) Find the coordinates of $2P$ on $\mathcal{C}$.
(6) Find the coordinates of the point P^{-1} on $\mathcal{C}$ using O as the identity element.
(7) Show that $2Q = O$. [Hint: Show that the tangent to $\mathcal{C}$ at Q passes through O and invoke Exercise 2.3.13.]
(8) Find the coordinates of all three points of the points of order 2 on $\mathcal{C}$.

Now we carry out these computations in a more general setting to derive an expression for the coordinates of $P + Q$. Let $\mathcal{C} = V(x(x - z)(x - \lambda z) - y^2 z)$ be a smooth cubic curve. Dehomogenize the defining equation $x(x-z)(x-\lambda z)-y^2 z = 0$ to get the affine equation $y^2 = f(x)$, where $f(x) = x(x - 1)(x - \lambda)$.

EXERCISE 2.5.7. Suppose $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$ are two points on $\mathcal{C}$, with $Q \neq P^{-1}$ (that is $x_1 \neq x_2$), and let $y = \alpha x + \beta$ be the equation of line $\ell(P, Q)$ through the points P and Q.

(1) Suppose $P \neq Q$. Express α in terms of x_1, x_2, y_1, y_2.
(2) Suppose $P = Q$ (in which case $\ell(P, Q)$ is the tangent line to $\mathcal{C}$ at P). Use implicit differentiation to express α in terms of x_1, y_1.
(3) Substitute $\alpha x + \beta$ for y in the equation $y^2 = f(x)$ to get a new equation in terms of x only. Write the resulting equation of x in the form $x^3 + Bx^2 + Cx + D = 0$.
(4) If $P + Q$ has coordinates $(x_3 : y_3 : 1)$, explain why $x^3 + Bx^2 + Cx + D$ must factor as $(x - x_1)(x - x_2)(x - x_3)$.
(5) By equating coefficients of x^2 in parts (4) and (5), conclude that
$$x_3 = -x_1 - x_2 + \alpha^2 + \lambda + 1,$$
where α is the slope of the line $\ell(P, Q)$.
(6) We now have an expression for the x-coordinate of $P + Q$. Use this to conclude that
$$P + Q = \bigl(-x_1 - x_2 + \alpha^2 + \lambda + 1 : y_1 + \alpha(x_3 - x_1) : 1\bigr)$$
where α is the slope of $\ell(P, Q)$. [Hint: Use the relationship between the y-coordinates of PQ and $P + Q$ along with the fact that (x_1, y_1) lies on the line defined by $y = \alpha x + \beta$.]

Therefore, if $P = (x_1 : y_1 : 1), P = (x_2 : y_2 : 1)$ are points on $\mathcal{C} = V(x(x-1)(x-\lambda) - y^2)$, then $P+Q$ has coordinates $(x_3 : y_3 : 1)$ given by

$$\begin{aligned} x_3 &= \begin{cases} -x_1 - x_2 + \lambda + 1 + \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 & \text{if } P \neq Q \\ \\ -2x_1 + \lambda + \left(\dfrac{f'(x_1)}{2y_1}\right)^2 & \text{if } P = Q \end{cases} \\ y_3 &= y_1 + \alpha(x_3 - x_1). \end{aligned}$$

Exercise 2.5.8. Verify the results in Exercise 2.5.6 using the above formula.

We may perform a similar sequence of calculations for a cubic in general form. Let $\mathcal{C}$ be the cubic curve defined by $y^2z = ax^3 + bx^2z + cxz^2 + dz^3$, where $a, b, c, d \in \mathbb{C}$. Dehomogenize this defining equation to get the affine equation $y^2 = f(x)$, where $f(x) = ax^3 + bx^2 + cx + d$ and f has distinct roots.

Exercise 2.5.9. Suppose $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$ be two points on $\mathcal{C}$, with $Q \neq P^{-1}$, and let $y = \alpha x + \beta$ be the equation of line $\ell(P, Q)$ through the points P and Q.

(1) Suppose $P \neq Q$. Express α in terms of x_1, x_2, y_1, y_2.
(2) Suppose $P = Q$ (in which case $\ell(P, Q)$ is the tangent line to $\mathcal{C}$ at P). Use implicit differentiation to express α in terms of x_1, y_1.
(3) Substitute $\alpha x + \beta$ for y in the equation $y^2 = f(x)$ to get a new equation in terms of x only. Write the resulting equation of x in the form $x^3 + Bx^2 + Cx + D = 0$.
(4) If $P + Q$ has coordinates $P + Q = (x_3 : y_3 : 1)$, explain why $Ax^3 + Bx^2 + Cx + D$ must factor as $a(x - x_1)(x - x_2)(x - x_3)$.
(5) By equating coefficients of x^2, conclude that

$$x_3 = -x_1 - x_2 + \frac{\alpha^2 - b}{a},$$

where α is the slope of the line $\ell(P, Q)$.
(6) We now have an expression for the x-coordinate of $P + Q$. Use this to conclude that

$$P + Q = \left(-x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\alpha^2 : y_1 + \alpha(x_3 - x_1) : 1\right)$$

where α is the slope of $\ell(P, Q)$.

Therefore, if $P = (x_1 : y_1 : 1), P = (x_2 : y_2 : 1)$ are points on $\mathcal{C} = V(ax^3 + bx^2 + cx + d - y^2)$, then $P + Q$ has coordinates $(x_3 : y_3 : 1)$ given by

$$
\begin{aligned}
x_3 &= \begin{cases} -x_1 - x_2 - \dfrac{b}{a} + \dfrac{1}{a}\left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 & \text{if } P \neq Q \\[2ex] -2x_1 - \dfrac{b}{a} + \dfrac{1}{a}\left(\dfrac{f'(x_1)}{2y_1}\right)^2 & \text{if } P = Q \end{cases} \\
y_3 &= y_1 + \alpha(x_3 - x_1).
\end{aligned}
$$

2.5.3. Rational Points on Cubics. Of particular importance to number theory and the theory of elliptic curves is the following property of the group law for elliptic curves.

Definition 2.5.1. Let $y^2 = f(x)$ be an affine equation of a smooth cubic curve, where $f(x)$ is a polynomial with rational coefficients. A point $P = (x, y)$ is a *rational point* if x, $y \in \mathbb{Q}$.

Once we have a rational point, a natural follow-up would be to ask how many rational points exist on a given curve. We first note the following property of rational points.

Exercise 2.5.10. Let $y^2 = f(x)$ be an affine equation of a smooth cubic curve, where $f(x)$ is a degree three polynomial with rational coefficients. Suppose P and Q are rational points on this curve, so that $P, Q \in \mathbb{Q}^2$ and $Q \neq P^{-1}$. Prove that $P + Q$ is also a rational point.

What happens if $Q = P^{-1}$? In this case $P + Q$ would be equal to the point at infinity $O = [0 : 1 : 0]$. While this point does have rational coordinates, this point is technically not on this particular affine chart. How can we address this?

2.5.4. Cubics over Other Fields. Another important consequence of our algebraic formulation for the group law is that the operations involved are independent of the field of definition. With this addition law, we can define the group law for cubic curves not only over $\mathbb{C}$, but also over $\mathbb{R}$, $\mathbb{Q}$, and even over finite fields. However, there is one subtlety that we need to be aware of. Some of the calculations need to be modified if the characteristic of the field is equal to 2.

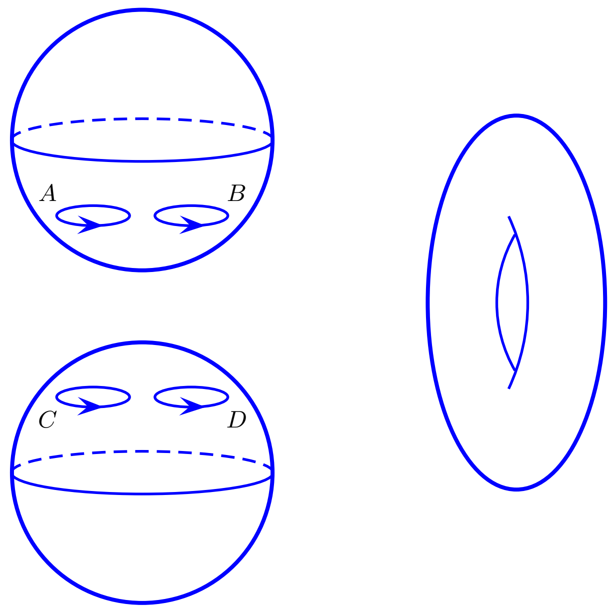
Exercise 2.5.11. This is inspired by [**AG06**], pages 105–109. Let $\mathcal{C}$ be the cubic curve given by $y^2 = x^3 + 1$.

(1) Show that $(0, 4)$ and $(2, 3)$ are points of $\mathcal{C}$ over $\mathbb{F}_5$.
(2) Use the formulas for addition above to compute $(0, 4) + (2, 3)$.
(3) Find all of the points on $\mathcal{C}$ that are defined over $\mathbb{F}_5$.

2.6. Cubics as Tori

The goal of this problem set is to realize a smooth cubic curve in $\mathbb{P}^2(\mathbb{C})$ as a torus.

Exercise 2.6.1. Draw a sequence of diagrams to show that if we attach the circle A to the circle $\mathcal{C}$ and the circle B to circle D, we obtain a torus.

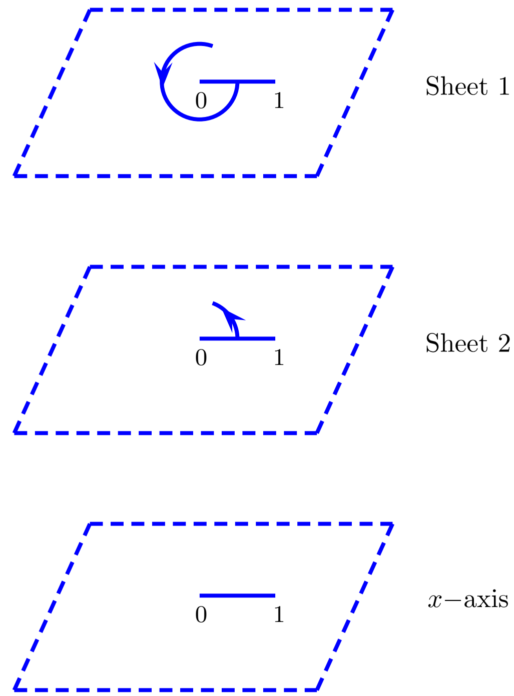


Exercise 2.6.2. Let $T : [0, 2\pi] \to \mathbb{C}$ be defined by $T(\theta) = e^{i\theta}$ and let $f : \mathbb{C} \to \mathbb{C}$ be defined by $f(x) = \sqrt{x}$.

(1) Show that $T([0, 2\pi])$ is a unit circle in $\mathbb{C}$.
(2) Show that $f \circ T([0, 2\pi])$ is a half circle.

Exercise 2.6.3. Now let $T : [0, 2\pi] \to \mathbb{C}$ be defined by $T(\theta) = 2e^{i\theta}$ and let $f : \mathbb{C} \to \mathbb{C}$ be defined by $f(x) = \sqrt{x(x-1)}$.

(1) Show that $T([0, 2\pi])$ is a circle of radius 2 in $\mathbb{C}$.
(2) Show that $f \circ T(0) = f \circ T(2\pi)$.
(3) Show that $f \circ T([0, 2\pi])$ is a closed curve in $\mathbb{C} - [0, 1]$.
(4) Sketch an intuitive argument for $f(x) = \sqrt{x(x-1)}$ being well-defined on $\mathbb{C} - [0, 1]$ in two ways: (i) by setting $\sqrt{2(2-1)} = +\sqrt{2}$, and then (ii) by setting $\sqrt{2(2-1)} = -\sqrt{2}$. This construction establishes a 2 sheeted cover of $\mathbb{C}$.

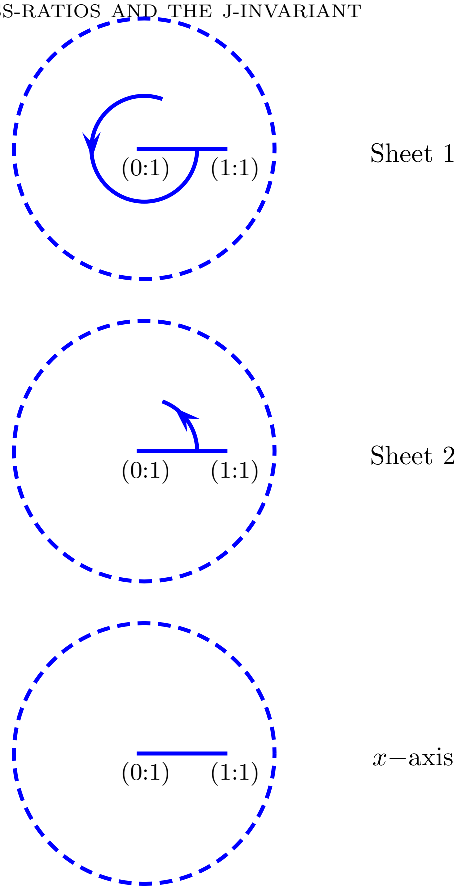


EXERCISE 2.6.4. Let $T : [0, 2\pi] \to \mathbb{C}$ be defined by $T(\theta) = \frac{1}{2}e^{i(\theta+\pi/2)}$ and let $f : \mathbb{C} \to \mathbb{C}$ be defined by $f(x) = \sqrt{x(x-1)}$.

(1) Show that $T([0, 2\pi])$ is the circle of radius $\frac{1}{2}$, with center 0, starting at the point $\frac{1}{2}i$, in the counterclockwise direction.
(2) Show that $f \circ T(0)$ and $f \circ T(2\pi)$ give different values and that these exist on each of the two sheets.
(3) Justify intuitively why $f \circ T([0, 2\pi])$ can be viewed as illustrated where Sheet 1 corresponds to $\sqrt{2}$ and Sheet 2 corresponds to $-\sqrt{2}$ as in the previous problem.

EXERCISE 2.6.5. Consider $V(y^2 - x(x-z))$ in $\mathbb{P}^2$. Now instead of considering two $\mathbb{C}$ sheets, we include the point at infinity, so we have two $\mathbb{P}^1$ sheets, i.e. our two sheets are now spheres rather than planes.

(1) Show that for each $(x : z) \in \mathbb{P}^1$ there are two possible values for y, except at $(0 : 1)$ and $(1 : 1)$.
(2) Consider the following figure in which the bottom sphere corresponds to the $(x : z)$-axis, which is really $\mathbb{P}^1$, the projective line. Show that sitting over this projective line are two sheets, each of which is $\mathbb{P}^1$.



(3) Replace the segments in $[(0:1),(1:1)]$ in Sheets 1 and 2 with circles A and B. Draw a sequence of diagrams to show that if we attach circle A in Sheet 1 to circle B in Sheet 2, then we obtain a sphere.
(4) Conclude that $V(y^2 - x(x-z)) \subset \mathbb{P}^2$ is a sphere.

Exercise 2.6.6. Now consider $f : \mathbb{C} \to \mathbb{C}$ defined by $f(x) = \sqrt{x(x-1)(x-\lambda)}$.

(1) Justify that f is well-defined on two possible sheets.
(2) Show that f is a 2-to-1 cover of the x-axis except at $x = 0$, $x = 1$, and $x = \lambda$.
(3) Homogenize $y^2 = x(x-1)(x-\lambda)$ to show that we now have a two-to-one cover of $\mathbb{P}^1$ except at $(0:1)$, $(1:1)$, $(\lambda:1)$, and $(1:0)$, where each of the two sheets is itself a $\mathbb{P}^1$. Explain how this is related to (b). What is the extra ramified point?
(4) Use the earlier exercises to draw a sequence of diagrams illustrating how $y^2 = x(x-z)(x-\lambda z)$ in $\mathbb{P}^2$ is a torus.

2.7. Cross-Ratios and the j-Invariant

We have seen that every smooth cubic curve can be thought of as a two-to-one cover of $\mathbb{P}^1$, branched at exactly four points. This section will show how we can always assume, via a change of coordinates, that three of these four branch points are $(1:0), (1:1)$ and $(0:1)$. We will start with a series of exercises that explicitly give these changes of coordinates. We then will have a series of exercises putting these changes of coordinates into changes of coordinates of $\mathbb{C}$. It is here that the *cross ratio* is made explicit. The key behind all of this is that two ordered sets of four points are projectively equivalent if and only if they have the same cross-ratio. The cross ratio will then return us to the j-invariant for a cubic curve.

2.7.1. Projective Changes of Coordinates for $\mathbb{P}^1$. Given any three points $(x_1 : y_1), (x_2 : y_2), (x_3 : y_3) \in \mathbb{P}^1$, we want to find a projective change of coordinates $T : \mathbb{P}^1 \to \mathbb{P}^1$ such that

$$\begin{aligned} T(x_1 : y_1) &= (1:0) \\ T(x_2 : y_2) &= (0:1) \\ T(x_3 : y_3) &= (1:1) \end{aligned}$$

We will see that not only does such a map always exist, but that it is unique.

We first have to define what we mean by a projective change of coordinates for $\mathbb{P}^1$. In Section 1.5, we gave a definition for project change of coordinates for $\mathbb{P}^2$. The definition for $\mathbb{P}^1$ is similar, namely that a projective change of coordinates is given by

$$\begin{aligned} u &= ax + by \\ v &= cx + dy, \end{aligned}$$

where $ad - bc \neq 0$. We write this as

$$T(x : y) = (ax + by : cx + dy).$$

Now, we could write $(x : y) \in \mathbb{P}^1$ as a column vector

$$\begin{pmatrix} x \\ y \end{pmatrix}.$$

If we let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then we can think of $T(x : y) = (ax + by : cx + dy)$ in terms of the matrix multiplication

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

In $\mathbb{P}^1$, we have that $(x : y) = (\lambda x : \lambda y)$ for any constant $\lambda \neq 0$. This suggests the following:

Exercise 2.7.1. Show that the matrices

$$A = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 6 & 4 \\ 2 & 8 \end{pmatrix} = 2 \cdot A$$

give rise to the same change of coordinates of $\mathbb{P}^1 \to \mathbb{P}^1$.

Exercise 2.7.2. Show that the matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix},$$

for any $\lambda \neq 0$, give rise to the same change of coordinates of $\mathbb{P}^1 \to \mathbb{P}^1$.

This means that the projective change of coordinates

$$(x : y) \to (ax + by : cx + dy)$$

and

$$(x : y) \to (\lambda ax + \lambda by : \lambda cx + \lambda dy)$$

are the same.

Our desired projective change of coordinates T such that

$$T(x_1 : y_1) = (1 : 0),\ T(x_2 : y_2) = (0 : 1),\ T(x_3 : y_3) = (1 : 1)$$

is

$$T(x : y) = ((x_2 y - y_2 x)(x_1 y_3 - x_3 y_1) : (x_1 y - y_1 x)(x_2 y_3 - x_3 y_2)).$$

(It should not be at all clear how this T was created.)

Exercise 2.7.3. Let

$$(x_1 : y_1) = (1 : 2),\ (x_2 : y_2) = (3 : 4),\ (x_3 : y_3) = (6 : 5).$$

Show that

(1) $T(x : y) = (28x - 21y : 18x - 9y)$
(2) $T(1 : 2) = (1 : 0),\ T(3 : 4) = (0 : 1),\ T(6 : 5) = (1 : 1)$

These problems give no hint as to how anyone could have known how to create T; the goal of these last problems was to show that this T actually does work.

We now want to start looking at uniqueness questions.

EXERCISE 2.7.4. Let $T(x:y) = (ax+by : cx+dy)$ be a projective change of coordinates such that $T(1:0) = (1:0),\ T(0:1) = (0:1),\ T(1:1) = (1:1)$. Show that

$$a = d \neq 0$$

and that

$$b = c = 0.$$

Explain why T must be the same as the projective change of coordinates given by $T(x:y) = (x:y)$.

Part of showing uniqueness will be in finding a decent, easy to use formula for the inverse of our map T.

EXERCISE 2.7.5. Let $T(x:y) = (ax+by : cx+dy)$ be a projective change of coordinates and let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be its associated matrix. Let

$$B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Show that

$$A \cdot B = \det(A) I,$$

where I is the two-by-two identity matrix.

EXERCISE 2.7.6. Let $(x_1 : y_1),\ (x_2 : y_2),\ (x_3 : y_3) \in \mathbb{P}^1$ be three distinct points. Let T_1 and T_2 be two projective change of coordinates such that

$$T_1(x_1 : y_1) = (1:0),\ T_1(x_2 : y_2) = (0:1),\ T_1(x_3 : y_3) = (1:1)$$

and

$$T_2(x_1 : y_1) = (1:0),\ T_2(x_2 : y_2) = (0:1),\ T_2(x_3 : y_3) = (1:1).$$

Show that $T_1 \circ T_2^{-1}$ is a projective change of coordinates such that

$$T_1 \circ T_2^{-1}(1:0) = (1:0),\ T_1 \circ T_2^{-1}(0:1) = (0:1),\ T_1 \circ T_2^{-1}(1:1) = (1:1).$$

Show that T_1 and T_2 must be the same projective change of coordinates.

Thus our desired map T is unique.

EXERCISE 2.7.7. Mathematicians will say that any three points in $\mathbb{P}^1$ can be sent to any other three points, but any fourth point's image must be fixed. Using the results of this section, explain what this means. (This problem is not so much a typical math exercise but is instead an exercise in exposition.)

Finally, we can see how anyone ever came up with the map

$$T(x:y) = ((x_2y - y_2x)(x_1y_3 - x_3y_1) : (x_1y - y_1x)(x_2y_3 - x_3y_2)).$$

We just have to find a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that

$$A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; A\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \; A\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Solving for the coefficients for A is now just a (somewhat brutal) exercise in algebra.

2.7.2. Working in $\mathbb{C}$. Algebraic geometers like to work in projective space $\mathbb{P}^n$. Other mathematicians prefer to keep their work in affine spaces, such as $\mathbb{C}^n$, allowing for points to go off, in some sense, to infinity. In this subsection we interpret the projective change of coordinates $T : \mathbb{P}^1 \to \mathbb{P}^1$ in the previous section as a map $T : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$.

Given three points x_1, x_2 and x_3 in $\mathbb{C}$, we want to find a map $T : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ such that

$$\begin{aligned} T(x_1) &= \infty \\ T(x_2) &= 0 \\ T(x_3) &= 1 \end{aligned}$$

For now, set

$$T(x) = \frac{(x_2 - x)(x_1 - x_3)}{(x_1 - x)(x_2 - x_3)}.$$

The next three exercises are in parallel with those in the previous subsection.

Exercise 2.7.8. Let $x_1 = 1/2$, $x_2 = 3/4$, and $x_3 = 6/5$. (Note that these correspond to the dehomogenization of the three points $(x_1 : y_1) = (1 : 2)$, $(x_2 : y_2) = (3 : 4)$ in the previous subsections first problem.) Show that

(1) $T(x) = \dfrac{28x - 21}{18x - 9}$.
(2) $T(1/2) = \infty, T(3/4) = 0, T(6/5) = 1$.

The next exercise will link the map $T : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ with the map $T : \mathbb{P}^1 \to \mathbb{P}^1$. Recall in $\mathbb{P}^1$ that

$$(x : y) = (\frac{x}{y} : 1),$$

provided that $y \neq 0$. By a slight abuse of notation, we can think of dehomogenizing as just setting all of the y's equal to one.

EXERCISE 2.7.9. Show that the map $T : \mathbb{P}^1 \to \mathbb{P}^1$ given by

$$T(x : y) = (ax + by : cx + dy)$$

will correspond to a map $T : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ given by

$$T(x) = \frac{ax+b}{cx+d}.$$

EXERCISE 2.7.10. Show that the map $T : \mathbb{P}^1 \to \mathbb{P}^1$ given by

$$T(x : y) = ((x_2y - y_2x)(x_1y_3 - x_3y_1) : (x_1y - y_1x)(x_2y_3 - x_3y_2))$$

will correspond to the map $T : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ given by

$$T(x) = \frac{(x_2 - x)(x_1 - x_3)}{(x_1 - x)(x_2 - x_3)}.$$

Here the dehomogenization is the map achieved by setting $y = 1$.

2.8. Cross Ratio: A Projective Invariant

Suppose we are given some points in $\mathbb{P}^1$. We can label these points in many ways, by choosing different coordinate systems. This is the same as studying the points under projective changes of coordinates. We would like to associate to our points something (for us, a number) that will not change, no matter how we write the points. We call such numbers *invariants*.

If we start with three points $p_1 = (x_1 : y_1), p_2 = (x_2 : y_2), p_3 = (x_3 : y_3) \in \mathbb{P}^1$, no such invariant number can exist, since any three points can be sent to any other three points. But we cannot send any four points to any other four points. This means that any collection of four points has some sort of intrinsic geometry. So add a fourth point $p_4 = (x_4 : y_4) \in \mathbb{P}^1$. Then

DEFINITION 2.8.1. The *cross ratio* of the four distinct points p_1, p_2, p_3, p_4 is

$$[p_1, p_2, p_3, p_4] = \frac{(x_2y_4 - y_2x_4)(x_1y_3 - x_3y_1)}{(x_1y_4 - y_1x_4)(x_2y_3 - x_3y_2)}.$$

We need to show that this number does not change under projective change of coordinates.

EXERCISE 2.8.1. Let

$$p_1 = (1 : 2), p_2 = (3 : 1), p_3 = (1 : 1), p_4 = (5 : 6).$$

(1) Calculate the cross ratio $[p_1, p_2, p_3, p_4]$.
(2) Let $T : \mathbb{P}^1 \to \mathbb{P}^1$ be

$$T(x : y) = (3x + 2y : 2x + y).$$

Find $T(p_1), T(p_2), T(p_3), T(p_4)$.

(3) Show
$$[T(p_1), T(p_2), T(p_3), T(p_4)] = [p_1, p_2, p_3, p_4].$$

EXERCISE 2.8.2. Let $p_1 = (x_1 : y_1), p_2 = (x_2 : y_2), p_3 = (x_3 : y_3), p_4 = (x_4 : y_4)$ be any collection of four distinct points in $\mathbb{P}^1$ and let $T(x, y) = (ax + by : cx + dy)$ be any projective change of coordinates. Show
$$[T(p_1), T(p_2), T(p_3), T(p_4)] = [p_1, p_2, p_3, p_4].$$
(This is a long exercise in algebra, but at the end, there should be satisfaction at seeing everything being equal.)

The above cross ratio depends, though, on how we ordered our four points $p_1, p_2, p_3 p_4$. If we change the order, the cross ratio might change.

EXERCISE 2.8.3. Let p_1, p_2, p_3, p_4 be any four distinct points in $\mathbb{P}^1$. Show
$$[p_1, p_2, p_3, p_4] = \frac{1}{[p_2, p_1, p_3, p_4]}.$$

EXERCISE 2.8.4. Let $p_1 = (x_1 : y_1), p_2 = (x_2 : y_2), p_3 = (x_3 : y_3), p_4 = (x_4 : y_4)$ such that $[p_1, p_2, p_3, p_4] \neq \pm 1$. Show that there is no projective change of coordinate $T(x : y) = (ax + by : cx + dy)$ such that T interchanges p_1 with p_2 but leave p_3 and p_4 alone. In other words, show there is no T such that
$$T(p_1) = p_2,\ T(p_2) = p_1,\ T(p_3) = p_3,\ T(p_4) = p_4.$$

EXERCISE 2.8.5. Let $p_1 = (x_1 : y_1), p_2 = (x_2 : y_2), p_3 = (x_3 : y_3), p_4 = (x_4 : y_4)$ be any collection of four distinct points in $\mathbb{P}^1$. Show that
$$[p_2, p_1, p_4, p_3] = [p_1, p_2, p_3, p_4].$$

EXERCISE 2.8.6. Using the notation from the previous problem, find two other permutations of the points p_1, p_2, p_3, p_4 so that the cross ratio does not change.

Let
$$[p_1, p_2, p_3, p_4] = \lambda.$$
We have shown that there are four permutations of the p_1, p_2, p_3, p_4 that do not change the cross ratio but we have also shown
$$[p_2, p_1, p_3, p_4] = \frac{1}{\lambda}.$$

EXERCISE 2.8.7. Using the above notation, find permutations of the p_1, p_2, p_3, p_4 so that all of the following cross ratios occur:
$$\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, 1-\lambda, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}.$$

EXERCISE 2.8.8. Given any four distinct points $p_1,\ p_2,\ p_3,\ p_4$ in $\mathbb{P}^1$, show that the j-invariant of the cross ratio does not change under any reordering of the four points and under any projective linear change of coordinates. (This is why we are justified in using the term "invariant" in the name j-invariant.)

Thus given a smooth cubic curve, we can put the curve into Weierstrass normal form and associate to this curve a singe number j. A natural question is if two different curves could have the same j invariant. The next exercises will show that this is not possible.

EXERCISE 2.8.9. Suppose that

$$j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} = a$$

for some constant a.

(1) Show that any solution μ of the equation

$$2^8(\lambda^2 - \lambda + 1)^3 - a\lambda^2(\lambda - 1)^2 = 0$$

has the property that

$$j(\mu) = a.$$

(2) Show that the above equation can have only six solutions.
(3) Show that if λ is a solution, then the other five solutions are $\frac{1}{\lambda},\ \frac{1}{1-\lambda},\ 1 - \lambda,\ \frac{\lambda}{\lambda-1},\ \frac{\lambda-1}{\lambda}$.
(4) Show that if we have two curves $zy^2 = x(x - z)(x - \lambda z)$ and $zy^2 = x(x - z)(x - \mu z)$ with

$$j(\lambda) = j(\mu),$$

then there is a projective change of coordinates of $\mathbb{P}^1$ with coordinates $(x : z)$ taking the first curve to the second.

2.9. Torus as $\mathbb{C}/\Lambda$

We will begin this section with background material from abstract algebra to make clear what a quotient group is. After that material is developed, we will expeditiously proceed to the goal of this problem set, namely to realize a torus as the quotient group $\mathbb{C}/\Lambda$.

2.9.1. Quotient Groups. Given a group G with binary operation $\star$, a subset S of G is said to be a *subgroup* if, equipped with the restriction of $\star$ to $S \times S$, S itself is a group. Given a known group G, a way to generate examples of groups is to look at all its subgroups. Another way of generating examples is to "collapse" a certain type of subgroup N of the group G into the identity element of a new "quotient group" G/N. In order for this "quotient" construction to yield a group, N must satisfy certain properties that make it a so-called *normal subgroup* of G.

Notation: Let G be a group with binary operation $\star$. This binary operation $\star$ induces an operation $\star$ (by abuse of notation) on subsets of G defined as follows: if S and T are subsets of G, then $S \star T := \{s \star t : s \in S, t \in T\}$. If $S = \{s\}$ is a singleton, then we write sT for $\{s\} \star T$; likewise, we write St for $S \star \{t\}$.

DEFINITION 2.9.1. Given a nonempty set A, we say that a collection P of subsets of A is a *partition* of A if P consists of nonempty, pairwise disjoint sets whose union is A. This means that if

$$P = \{U_\alpha\}_{\alpha \in I},$$

where I is an indexing set, then the elements of P satisfy the following two conditions.

(1) $P_\alpha \cap P_\beta =$ for all $\alpha, \beta \in I$;
(2) $A = \cup_{\alpha \in I} U_\alpha$.

EXERCISE 2.9.1. Let A be a nonempty set.

(1) Let $\sim$ be an equivalence relation on the set A. Show that the set of equivalence classes of $\sim$ is a partition of A.
(2) Suppose P is a partition of A. Show that the relation $\sim$, defined by $x \sim y$ if and only if x and y belong to the same element of P, is an equivalence relation.

The previous exercise shows that partitions give natural equivalence relations and that equivalence relations are natural ways of generating partitions.

DEFINITION 2.9.2. Let G be a group. A quotient group of G is a partition of G that is a group under the subset operation induced by the binary operation on G.

EXERCISE 2.9.2. For $i = 0, 1, 2$, let $3\mathbb{Z} + i := \{3n + i : n \in \mathbb{Z}\}$. Show that $\{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\}$ is a quotient group of the additive group $\mathbb{Z}$.

EXERCISE 2.9.3. Suppose Q is a quotient group of a group G. Prove the following.

(1) Let e be the identity of G and let E be the unique element of Q with $e \in E$. Then E is the identity in the group Q.
(2) Let $A \in Q$, $a \in A$, and a^{-1} the inverse to a in G. Let A' be the unique element of Q containing a^{-1}. Then A' is the inverse to A in Q.
(3) Let $A \in Q$. For any $a \in A$, $A = aE = Ea$.

DEFINITION 2.9.3. Let G be a group. A *normal subgroup* N of G is a subgroup of G that is the identity element of some quotient group Q of G. The subsets of G in Q are called the *cosets* of N. If N is a normal subgroup by virtue of being the identity element of the quotient group Q, we write $Q = G/N$ and say that Q is the group $G \mod N$.

EXERCISE 2.9.4. Identify all possible normal subgroups of the additive group $\mathbb{Z}$. (Hint: start by analyzing the previous exercise.)

Recall, from above, that $gN = \{gn : n \in N\}$. In the next exercise we will establish that N is normal if and only if $gN = Ng$. gN and Ng are two sets and we will show equality *as sets*. In particular, we show that every element of gN is in Ng and vice versa, but it is not necessarily true that $gn = ng$ for a particular $n \in N$, i.e. the group need not be abelian.

EXERCISE 2.9.5. Show that a subgroup N of a group G is normal if and only if $gN = Ng$ for all $g \in G$. [Hint: If $gN = Ng$ for all $g \in G$, define $Q = \{gN : g \in G\}$. Show that the operation on subsets of G is well-defined on Q and makes Q into a group.]

EXERCISE 2.9.6. Given a quotient group Q of a group G, show that the element of Q containing e (the identity element of G) is a normal subgroup of G.

EXERCISE 2.9.7. Suppose G is an abelian group. Show that every subgroup is normal.

In the discussion above, we have produced some ways of generating examples of groups: finding subgroups and taking quotients. (To be sure, there are more ways of generating groups from given ones: for instance, one can take direct products, or ultraproducts, but that's not useful to us at this point.) But how do we compare groups? One way of doing this is to look for maps between groups that preserve group structure.

DEFINITION 2.9.4. Suppose $(G, \star_G)$ and $(H, \star_H)$ are two groups. A map $\varphi : G \to H$ is said to be a *homomorphism* if $\varphi(x \star_G y) = \varphi(x) \star_H \varphi(y)$ for all $x, y \in G$. If a homomorphism is bijective, we call it an *isomorphism* and say that the groups G and H are *isomorphic*. We denote this by $G \cong H$.

If two groups are isomorphic, they are essentially "the same." If there is a homomorphism between two groups there is still a nice relationship between G and H.

EXERCISE 2.9.8. Let $\varphi : G \to H$ be a homomorphism, and let e be the identity element of H. Let $\ker(\varphi) := \{g \in G : \varphi(g) = e\}$. (We call $\ker(\varphi)$ the *kernel* of φ.)

(1) Show that $\ker(\varphi)$ is a subgroup of G.
(2) Show that $\ker(\varphi)$ is a normal subgroup of G.
(3) Show that if $\varphi : G \to H$ is onto, then the quotient group $G/\ker(\varphi)$ is isomorphic to H.

The previous exercise gives us a way to check whether a subset S of a group G is a normal subgroup. If we can realize the subset S as the kernel of a homomorphism, then it must be a normal subgroup.

EXERCISE 2.9.9. Let G be the multiplicative group of all invertible 2×2 matrices over the real numbers, and let N be the subset of G consisting of matrices having determinant equal to 1. Prove that N is a normal subgroup of G.

2.9.2. The Torus. In order to understand some of the geometry of a torus, we need to determine how a torus is formed. We will begin by using a little group theory to realize a circle, S^1, as the quotient group $\mathbb{R}/\mathbb{Z}$.

EXERCISE 2.9.10.

(1) Show that $\mathbb{R}$ is an abelian group under addition.
(2) Show that $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ and conclude that $\mathbb{Z}$ is a normal subgroup.

EXERCISE 2.9.11. Define a relation on $\mathbb{R}$ by $x \sim y$ if and only if $x - y \in \mathbb{Z}$.

(1) Verify that $\sim$ an equivalence relation.
(2) Let $[x]$ denote the equivalence class of x, that is, $[x] = \{y \in \mathbb{R} \mid x \sim y\}$. Find the following equivalence classes: $[0]$, $[\frac{1}{2}]$, and $[\sqrt{2}]$.
(3) The equivalence relation $\sim$ gives a partition of $\mathbb{R}$. Explain how this partition $\mathbb{R}/\mathbb{Z}$ is the realization of a circle. [Hint: Explain how progressing from 0 to 1 is the same as going around a circle once.]

We can also use Exercise 2.9.8 to give an isomorphism between $\mathbb{R}/\mathbb{Z}$ and the circle. Let S^1 denote the unit circle centered at the origin in $\mathbb{R}^2$. As we have already seen $\mathbb{R}^2$ is in one-to-one correspondence with $\mathbb{C}$, so we can regard S^1 as the set $S^1 = \{x \in \mathbb{C} \mid |x| = 1\}$. Recall, that any complex number has a polar representation $x = r(\cos\theta + i\sin\theta)$, so we can express S^1 as $S^1 = \{\cos\theta + i\sin\theta : \theta \in \mathbb{R}\} \subset \mathbb{C}$.

EXERCISE 2.9.12. Show that S^1 is a group under (complex) multiplication.

EXERCISE 2.9.13. Define a map $\phi : \mathbb{R} \to S^1$ by $\phi(\theta) = \cos 2\pi\theta + i \sin 2\pi\theta$.

(1) Show that ϕ is onto.
(2) Show that ϕ is a homomorphism, i.e. show that $\phi(\alpha + \beta) = \phi(\alpha)\phi(\beta)$ for all $\alpha, \beta \in \mathbb{R}$.
(3) Find $\ker \phi$ and conclude that $\mathbb{R}/\mathbb{Z} \cong S^1$.

We now want to extend the ideas in the previous exercises to the complex plane. Let ω_1 and ω_2 be complex numbers such that $\frac{\omega_1}{\omega_2}$ is not purely real. Let the integer lattice Λ be defined as $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$. We will call the parallelogram formed by joining 0, ω_1, $\omega_1 + \omega_2$, ω_2, and 0 in succession the fundamental period-parallelogram. We will realize a torus as a quotient group $\mathbb{C}/\Lambda$.

EXERCISE 2.9.14. (1) Sketch the lattice generated by $\omega_1 = 1$ and $\omega_2 = i$. [Hint: Sketch the fundamental period-parallelogram of this lattice.]
(2) Sketch the lattice generated by $\omega_1 = 1 + i$ and $\omega_2 = i$.

EXERCISE 2.9.15. (1) Show that $\mathbb{C}$ is an abelian group under addition.
(2) Show that Λ is a subgroup of $\mathbb{C}$ and conclude that Λ is a normal subgroup.

EXERCISE 2.9.16. Define a relation on $\mathbb{C}$ by $x \sim y$ if and only if $x - y \in \Lambda$. Show that $\sim$ is an equivalence relation.

Since $\sim$ is an equivalence relation, it is natural to ask about the quotient group $\mathbb{C}/\Lambda$.

EXERCISE 2.9.17. Let $\Lambda \subset \mathbb{C}$ be the integer lattice generated by $\{\omega_1 = 1, \omega_2 = i\}$ and let $a, b \in \mathbb{R}$.

(1) Find all points in $\mathbb{C}$ equivalent to $\frac{1}{2} + \frac{1}{2}i$ in the group $\mathbb{C}/\Lambda$.
(2) Find all points in $\mathbb{C}$ equivalent to $\frac{1}{3} + \frac{1}{4}i$ in $\mathbb{C}/\Lambda$.
(3) Show that $a \sim a + i$ in $\mathbb{C}/\Lambda$.
(4) Show that $bi \sim 1 + bi$ in $\mathbb{C}/\Lambda$.

EXERCISE 2.9.18. Sketch a sequence of diagrams to show that $\mathbb{C}/\Lambda$ is a torus. [Hint: Construct a torus using $\omega_1 = 1$ and $\omega_2 = i$ by identifying the horizontal and vertical sides of the fundamental period-parallelogram as in the previous problem. Now repeat with any lattice.]

EXERCISE 2.9.19. Let $\Lambda \subset \mathbb{C}$ be the integer lattice generated by $\{\omega_1 = 1, \omega_2 = i\}$.

(1) Sketch a vertical segment in the fundamental period-parallelogram and illustrate to what this corresponds on our torus. Sketch a horizontal line in the fundamental period-parallelogram and illustrate to what this corresponds on our torus.

(2) Show that $\frac{1}{4}+i \in \mathbb{C}/\Lambda$ has order 4 and write all of the elements of $\langle \frac{1}{4}+i\rangle$.
(3) Represent the fact that $\frac{1}{4}+i$ has order 4 geometrically on the fundamental period-parallelogram by sketching a line in $\mathbb{C}$ that has slope $\frac{1}{4}$ and considering its image in $\mathbb{C}/\Lambda$.
(4) Sketch the paths traced by these segments on the torus. What do you notice about this path on the torus?
(5) Pick any element $\alpha \in \mathbb{C}/\Lambda$ and show that if α has finite order, then the path on the torus represented by the line through 0 and α is a closed path.
(6) Suppose an element α has infinite order. What can you say about the slope of the line through 0 and α. Illustrate this phenomenon on the fundamental period-parallelogram in $\mathbb{C}$ and on the torus.

2.10. Mapping $\mathbb{C}/\Lambda$ to a Cubic

The goal of this problem set is construct a map from $\mathbb{C}/\Lambda$ to a cubic curve.

In this section we assume some knowledge about complex variables and analysis. For a quick outline of the basics that we are going to use, please refer to Appendix A or your favorite introductory complex variables textbook.

We have established that given any smooth cubic curve $\mathcal{C}$ we can realize $\mathcal{C}$ topologically as a torus. We have also seen that given any integer lattice $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\} \subset \mathbb{C}$, with ω_1/ω_2 not purely real, we can construct a torus $\mathbb{C}/\Lambda$. Our goal in this section is to generate a smooth cubic curve given a lattice Λ. Hence, we will construct a map from the quotient group $\mathbb{C}/\Lambda$ to $\mathbb{C}^2$ whose image is the zero locus of a non-singular cubic polynomial. In order to do this we will use the Weierstrass $\wp$-function $\wp : \mathbb{C}/\Lambda \to \mathbb{C}$ defined by

$$\wp(x) = \frac{1}{x^2} + \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(x - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2}.$$

Then our map $\mathbb{C}/\Lambda \to \mathbb{C}^2$ will be given by the map $x \mapsto (\wp(x), \wp'(x))$, and the smooth cubic will be defined by the differential equation $[\wp'(x)]^2 = 4[\wp(x)]^3 + A\wp(x) + B$.

At this point it is not at all clear how we arrived at the function $\wp$. We begin by considering the minimal properties that are essential for our map $\mathbb{C}/\Lambda \to \mathbb{C}$. We will then show that $\wp$ has these properties and gives us our desired cubic.

Exercise 2.10.1. Show that for a function $f : \mathbb{C}/\Lambda \to \mathbb{C}$ to be well-defined, the function $f : \mathbb{C} \to \mathbb{C}$ must be doubly-periodic, that is,

$$f(x + \omega_1) = f(x) \quad \text{and} \quad f(x + \omega_2) = f(x),$$

for all x in the domain of f.

To define the function f we seek we need only consider what happens on the fundamental period-parallelogram. Our first hope is that f is analytic on its fundamental period-parallelogram, i.e. f has a Taylor series, $f(x) = \sum_{n=0}^{\infty} a_n x^n$. This will not work.

EXERCISE 2.10.2. Show that if a doubly-periodic function f is analytic on its fundamental period-parallelogram, then f is constant. (Hint: Use Liouville's Theorem.)

We see then that f cannot be analytic on its entire fundamental period-parallelogram. The next hope is that f is be analytic except with a single pole at 0, and hence at the other lattice points by double periodicity. Furthermore, we hope that the pole at 0 is not too bad. We can do this, but 0 will be a pole of order two, as the next two exercises illustrate.

It is inconvenient to integrate over these parallelograms if the singularities are on the boundaries, but we can translate the vertices, without rotating, so that the singularities are in the interior. The translated parallelograms will be called *cells*.

EXERCISE 2.10.3. Show that the sum of the residues of f at its poles in any cell is zero.

EXERCISE 2.10.4. Show that if f has a single pole at 0 in its fundamental period-parallelogram, not including the other vertices, then 0 must be a pole of order at least two.

We have now established that a candidate for our function could have the form

$$f(x) = \frac{a_{-2}}{x^2} + a_0 + a_1 x + a_2 x^2 + \dots$$

EXERCISE 2.10.5. Show that if

$$f(x) = \frac{a_{-2}}{x^2} + a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

is doubly-periodic, then f is an even function, i.e. $a_1 = a_3 = \cdots = 0$. [Hint: Consider the function $f(x) - f(-x)$.]

We can change coordinates to eliminate a_0 so that f is now of the form

$$f(x) = \frac{a_{-2}}{x^2} + a_2 x^2 + a_4 x^4 + \dots$$

Now we are ready to introduce the Weierstrass $\wp$-function.

$$\wp(x) = \frac{1}{x^2} + \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(x - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2}, \tag{2.11}$$

A series $\sum_{n=0}^{\infty} a_n$ is *absolutely convergent* whenever $\sum_{n=0}^{\infty} |a_n| < \infty$.

A series of functions f_n is *uniformly convergent* with limit f if for all $\epsilon > 0$, there exists a natural number N such that for all x in the domain and all $n \geq N$, $|f_n(x) - f(x)| < \epsilon$.

EXERCISE 2.10.6. Show that $\wp(x)$ converges uniformly and absolutely except near its poles. Conclude that $\wp(x)$ is analytic on the complex plane except at the lattice points $\Lambda = \{m\omega_1 + n\omega_2\}$.

Since $\wp(x)$ converges uniformly and absolutely, we can differentiate term-by-term to find $\wp'(x)$, and the order of summation does not affect the value of the function, so we can rearrange the terms.

EXERCISE 2.10.7. Find $\wp'(x)$ and show that $\wp'(x)$ is doubly-periodic.

EXERCISE 2.10.8. Show that $\wp(x)$ is doubly-periodic. (Hint: Consider the functions $F_i(x) = \wp(x + \omega_i) - \wp(x)$ for $i = 1, 2$.)

Consider the function $F(x) = \wp(x) - x^{-2}$.

EXERCISE 2.10.9. Show that F is analytic in a neighborhood of 0.

EXERCISE 2.10.10. Find the Taylor series expansion of F at 0.

EXERCISE 2.10.11. From above we know that $\wp(x)$ is even, so F is also even. Show that the odd powers of x vanish in the Taylor expansion of F at 0.

EXERCISE 2.10.12. Now we can rewrite $\wp(x) = x^{-2} + F(x)$. Find the coefficients of x^2 and x^4 in this expression for $\wp(x)$.

EXERCISE 2.10.13. Let

$$g_2 = 60 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^4}$$

and

$$g_3 = 140 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^6}.$$

Find the x^2 and x^4 coefficients of $\wp(x)$ in terms of g_2 and g_3.

EXERCISE 2.10.14. Find the coefficients of x and x^3 in $\wp'(x)$ in terms of g_2 and g_3.

We will now establish a cubic relationship between $\wp(x)$ and $\wp'(x)$. In the previous exercises we found the following expressions for $\wp(x)$ and $\wp'(x)$.

$$\wp(x) = \frac{1}{x^2} + \frac{1}{20} g_2 x^2 + \frac{1}{28} g_3 x^4 + O(x^6)$$

$$\wp'(x) = -\frac{2}{x^3} + \frac{1}{10} g_2 x + \frac{1}{7} g_3 x^3 + O(x^5)$$

EXERCISE 2.10.15. Compute $\wp(x)^3$ and $\wp'(x)^2$, and only consider terms up to first order, that is, find f and g such that $\wp(x)^3 = f(x) + O(x^2)$ and $\wp'(x)^2 = g(x) + O(x^2)$.

EXERCISE 2.10.16. Show that $\wp'(x)^2 = 4\wp(x)^3 - g_2\wp(x) - g_3$.

CHAPTER 3

Higher Degree Curves

The goal of this chapter is to explore higher degree curves in $\mathbb{P}^2$. There are six parts. In the first, we define what is meant by an irreducible curve and its degree. We next show how curves in $\mathbb{P}^2$ can be thought of as real surfaces, similar to our observations for conics (Section 1.7) and cubics (Section 2.6). In the third part, we develop Bézout's Theorem, which tells us the number of points of intersection of two curves. We then introduce the ring of regular functions and the function field of a curve. In the fourth part, we develop Riemann-Roch, an amazing theorem that links functions on the curve, the degree of the curve and the genus (the number of holes) of the curve into one formula. In the last section, we consider singular points on a curve and develop methods for resolving them.

3.1. Higher Degree Polynomials and Curves

The goals of this section are to define what it means for a curve to be irreducible and to define the degree of a curve.

In Chapter 1 we dealt with conics, which are the zero sets of second degree polynomials. In Chapter 2, we looked at cubics, which are the zero sets of third degree polynomials. It is certainly natural to consider zero sets of higher degree polynomials.

By now, we know that it is most natural to work in the complex projective plane, $\mathbb{P}^2$, which means in turn that we want our zero sets to be the zero sets of homogeneous polynomials. Suppose that $P(x, y, z) \in \mathbb{C}[x, y, z]$ is a homogeneous polynomial. We denote this polynomial's zero set by

$$\mathrm{V}(P) = \{(a : b : c) \in \mathbb{P}^2 : P(a, b, c) = 0\}.$$

Exercise 3.1.1. Let $P(x, y, z) = (x + y + z)(x^2 + y^2 - z^2)$. Show that $\mathrm{V}(P)$ is the union of the two curves $\mathrm{V}(x + y + z)$ and $\mathrm{V}(x^2 + y^2 - z^2)$.

Thus, if we want to understand $\mathrm{V}(P)$, we should start with looking at its two components: $\mathrm{V}(x + y + z)$ and $\mathrm{V}(x^2 + y^2 - z^2)$. In many ways, this reminds us of working with prime factorization of numbers. If we understand these building blocks—those numbers that cannot be broken into a product of two smaller numbers—then we start to understand the numbers formed when they are strung together.

EXERCISE 3.1.2. Let $P(x, y, z) = (x+y+z)^2$. Show that $\mathrm{V}(P) = \mathrm{V}(x+y+z)$.

Both $(x + y + z)(x^2 + y^2 - z^2)$ and $(x + y + z)^2$ are *reducible*, meaning that both can be factored. We would prefer, for now, to restrict our attention to curves that are the zero sets of irreducible homogeneous polynomials.

DEFINITION 3.1.1. If the defining polynomial P cannot be factored, we say the curve $\mathrm{V}(P)$ is *irreducible*.

When we are considering a factorization, we do not consider trivial factorizations, such as $P = 1 \cdot P$. *For the rest of this chapter, all polynomials used to define curves will be irreducible unless otherwise indicated.*

DEFINITION 3.1.2. The *degree* of the curve $\mathrm{V}(P)$ is the degree of its defining polynomial, P[1].

The degree of a curve is the most basic number associated to a curve that is invariant under change of coordinates. The following is an example of this phenomenon.

EXERCISE 3.1.3. Let $P(x, y, z) = x^3 + y^3 - z^3$. Then $\mathrm{V}(P)$ is a degree three curve. Consider the projective change of coordinates

$$\begin{aligned} x &= u - w \\ y &= iv \\ z &= u + v \end{aligned}$$

Find the polynomial $\widetilde{P}(u, v, w)$ whose zero set $\mathrm{V}(\widetilde{P})$ maps to $\mathrm{V}(P)$. Show that $\mathrm{V}(\widetilde{P})$ also has degree three.

3.2. Higher Degree Curves as Surfaces

The goal of this section is to generalize our work in Sections 1.7 and 2.6, where we realized smooth conics and cubics over $\mathbb{C}$ as topological surfaces over $\mathbb{R}$.

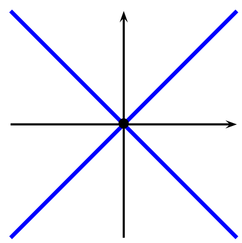
[1]Recall that we are assuming that all polynomials used to define curves are irreducible. There will be times when we will define the degree as the degree of P even if P is not irreducible but then we have to alter slightly the definition of V(P).

3.2.1. Topology of a Curve. Suppose $f(x, y, z)$ is a homogeneous polynomial, so $\mathrm{V}(f)$ is a curve in $\mathbb{P}^2$. Recall that the degree of $\mathrm{V}(f)$ is, by definition, the degree of the homogeneous polynomial f. We will see that this algebraic invariant of the curve is closely linked to the topology of the curve viewed as a surface over $\mathbb{R}$. Specifically, it is related to the "genus" of the curve, which counts the number of holes in the surface.

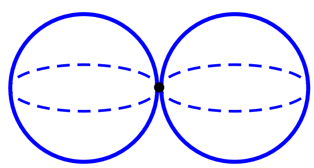
Before we proceed to higher degree curves, we return to our previous experience with conics and cubics.

Exercise 3.2.1. Consider the conics defined by the homogeneous equation $x^2 - y^2 = \lambda z^2$, where λ is a parameter. Sketch affine patches of these in the chart $z = 1$ for $\lambda = 4, 1, 0.25$.

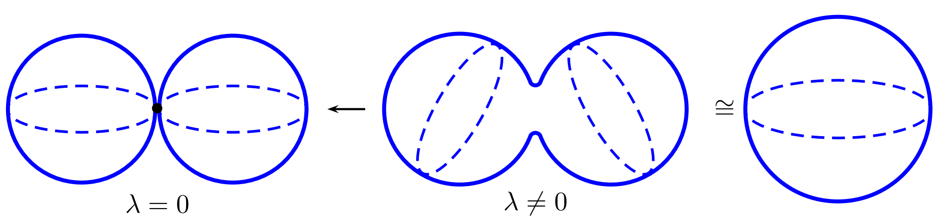
As $\lambda \to 0$, we get $x^2 - y^2 = 0$, or $(x - y)(x + y) = 0$. In $\mathbb{R}^2$, this looks like



but this picture isn't accurate over $\mathbb{C}$ in $\mathbb{P}^2$. Instead, topologically the picture looks like "kissing spheres":

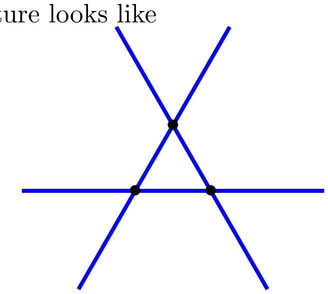


Thus, the topological version of the original equation, $x^2 - y^2 = \lambda z^2$, should be found by perturbing the kissing spheres a little to account for $\lambda \neq 0$:

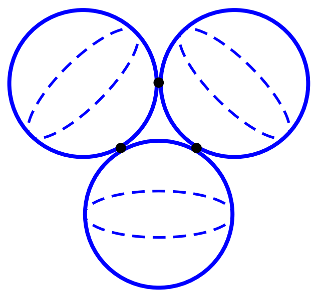


Therefore, by mildly perturbing the specialized, non-smooth conic, we find that topologically a smooth conic (those in this exercise for which $\lambda \neq 0$) is a sphere with no holes, which agrees with our work in Section 1.7.

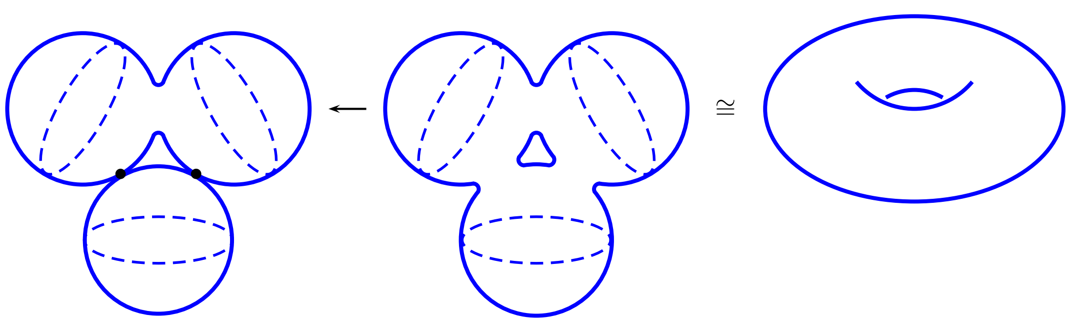
Following this same reasoning, we find another proof that a smooth cubic must be a torus when realized as a surface over $\mathbb{R}$. We begin with the highly degenerate cubic, $f(x, y, z) = (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z)(a_3x + b_3y + c_3z)$. In the real affine chart $z = 1$, the picture looks like



Again, our picture isn't valid over $\mathbb{C}$ in $\mathbb{P}^2$. Instead, the correct topological picture is that of three spheres meeting at three points, as shown.



Perturbing the top two spheres slightly, we find they join into the topological equivalent of a single sphere, but that this new figure is joined to the third sphere at two points of contact. Perturbing each of these points of intersection independently of one another, we obtain a single surface with a hole through the middle as depicted in the sequence of figures below.



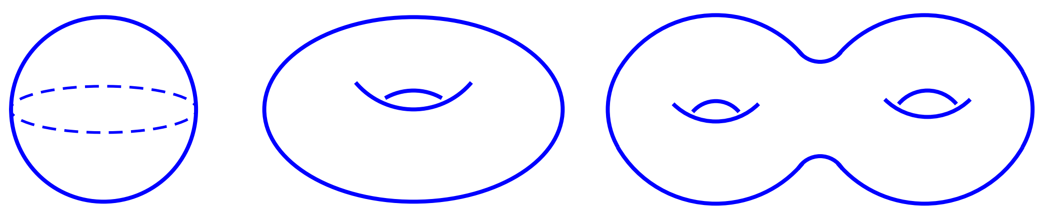
Thus a smooth cubic over $\mathbb{C}$ is topologically equivalent to a torus (a sphere with a hole through it) as a surface over $\mathbb{R}$. Note that this agrees with our results in Section 2.6.

EXERCISE 3.2.2. Mimic the arguments illustrated above to describe the real surface corresponding to a smooth quartic (fourth degree) curve over $\mathbb{C}$ in $\mathbb{P}^2$. Start with a highly degenerate quartic (the product of four pairwise non-parallel lines), draw the corresponding four spheres, and deform this surface by merging touching spheres two at a time. How many holes will the resulting figure possess?

Now do the same for a smooth quintic (fifth degree) curve. How many holes must it have?

3.2.2. Genus of a Curve. The number of holes in the real surfaces corresponding to smooth conics, cubics, quartics and quintics is a topological invariant of these curves. That is, every smooth conic is topologically equivalent to a real sphere with no holes. Every smooth cubic is topologically equivalent to a real torus (a sphere with exactly one hole through it), every smooth quartic is equivalent to a sphere with three holes and every smooth quintic to a sphere with six holes. Therefore, all smooth conics are topologically equivalent to one another, all smooth cubics are topologically equivalent, and so on, and each equivalence class is completely determined by the number of holes in the associated real surface.

DEFINITION 3.2.1. Let $\mathrm{V}(P)$ be a smooth, irreducible curve in $\mathbb{P}^2(\mathbb{C})$. The number of holes in the corresponding real surface is called the *topological genus* of the curve $\mathrm{V}(P)$.



topological genus $=0$ — topological genus $=1$ — topological genus $=2$

Presently, this notion of genus only makes sense when we are working over the reals or an extension of them. However, by the discussion above, we see that there is a connection between the genus, g, and the degree, d, of a curve. That is, all smooth curves of degree d have the same genus, so we now wish to find a formula expressing the genus as a function of the degree.

EXERCISE 3.2.3. Find a quadratic function in d, the degree of a smooth curve, that agrees with the topological genus of curves of degrees $d = 2, 3, 4$ found earlier. Now use this formula to compute the genus of a smooth quintic (fifth degree) curve. Does it match your answer to the last exercise?

DEFINITION 3.2.2. Let $\mathrm{V}(P)$ be a smooth curve of degree d. The number $\frac{(d-1)(d-2)}{2}$ is the *arithmetic genus* of the curve, which is an algebraic invariant of $\mathrm{V}(P)$.

EXERCISE 3.2.4. Argue by induction on d, the degree, that the topological genus agrees with the arithmetic genus for smooth curves, or in other words that

$$g = \frac{(d-1)(d-2)}{2}.$$

It is a theorem that the topological genus and the arithmetic genus do agree with one another whenever both are defined and make sense. However, the arithmetic version is independent of base field and enables us to exploit the genus of curves even over finite fields in positive characteristic.

3.3. Bézout's Theorem

The goal of this section is to develop the needed sharp definitions to allow a statement and a proof of Bézout's Theorem, which states that in $\mathbb{P}^2$ a curve of degree n will intersect a curve of degree m in exactly nm points, provided the points of intersection are "counted correctly".

3.3.1. Intuition behind Bézout's Theorem.

We look at how many points a straight line will intersect a conic in $\mathbb{P}^2$. Both the need to work in the complex projective plane $\mathbb{P}^2$ and the need to define intersection numbers correctly will become apparent.

EXERCISE 3.3.1. Show that the line $\mathrm{V}(x-y)$ will intersect the circle $\mathrm{V}(x^2 + y^2 - 1)$ in two points in the real plane, $\mathbb{R}^2$.

EXERCISE 3.3.2. Show that the line $\mathrm{V}(x-y+10)$ will not intersect $\mathrm{V}(x^2+y^2-1)$ in $\mathbb{R}^2$ but will intersect $\mathrm{V}(x^2+y^2-1)$ in two points in $\mathbb{C}^2$.

The last exercise demonstrates our need to work over the complex numbers. Now to see the need for projective space.

EXERCISE 3.3.3. Show that the two lines $\mathrm{V}(x-y+2)$ and $\mathrm{V}(x-y+3)$ do not intersect in $\mathbb{C}^2$. Homogenize both polynomials and show that they now intersect at a point at infinity in $\mathbb{P}^2$.

EXERCISE 3.3.4. Show that $\mathrm{V}(y-\lambda)$ will intersect $\mathrm{V}(x^2+y^2-1)$ in two points in $\mathbb{C}^2$, unless $\lambda = \pm 1$. Show that $\mathrm{V}(y-1)$ and $\mathrm{V}(y+1)$ are tangent lines to the circle $\mathrm{V}(x^2+y^2-1)$ at their respective points of intersection. Explain why we say that $\mathrm{V}(y-1)$ intersects the circle $\mathrm{V}(x^2+y^2-1)$ in one point with multiplicity two.

EXERCISE 3.3.5. Show that the line $V(y-\lambda x)$ will intersect the curve $V(y-x^3)$ in three points in $\mathbb{C}^2$, unless $\lambda = 0$. Letting $\lambda = 0$, show that $V(y)$ will intersect the curve $V(y - x^3)$ in only one point in $\mathbb{C}^2$. Explain why we that $V(y)$ intersects $V(y - x^3)$ in one point with multiplicity three.

EXERCISE 3.3.6. Show that there are no points in $\mathbb{C}^2$ in the intersection of $V(xy - 1)$ with $V(y)$. Homogenize both equations $xy = 1$ and $y = 0$. Show that there is a point of intersection at infinity. Explain why we say that $V(xy - 1)$ will intersect $V(y)$ in one point at infinity with multiplicity two.

3.3.2. Fundamental Theorem of Algebra. The goal of this section is to review the Fundamental Theorem of Algebra and consider how it might be generalized to a statement about intersections of plane curves.

Polynomials have roots. Much of the point behind high school algebra is the exploration of this fact. The need for complex numbers stems from our desire to have all possible roots for polynomials.

In this section we briefly review the Fundamental Theorem of Algebra. The exercises in this section will lead us to the realizations that such a generalization requires a precise definition of the multiplicity of a point of intersection and that the curves must lie in projective space.

Consider a polynomial $f(x)$ with real coefficients. Of course, the number of real roots of f is less than or equal to the degree of f, with equality in the case that f can be written as a product of distinct linear factors over $\mathbb{R}$.

EXERCISE 3.3.7. Give examples of second degree polynomials in $\mathbb{R}[x]$ that have zero, one, and two distinct real roots, respectively.

EXERCISE 3.3.8. Find the complex roots of your first example.

EXERCISE 3.3.9. Define the multiplicity of a root of a polynomial so that, in your second example, the single real root has multiplicity two.

The moral of the preceding exercises is that by considering complex roots, and defining multiplicity appropriately, we can make a uniform statement about the number of roots of a polynomial. Compare the following definition with the definition you produced in the exercise above.

DEFINITION 3.3.1. Let $f(x)$ be a polynomial in $\mathbb{C}[x]$. If $f(x) = (x - a)^m g(x)$, $m > 0$, such that $(x - a)$ does not divide $g(x)$, then we say that the *multiplicity of the root a* of $f(x)$ is m.

THEOREM 3.3.10 (Fundamental Theorem of Algebra). If $f(x)$ is a polynomial of degree d in $\mathbb{C}[x]$, then

$$f(x) = (x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_r)^{m_r},$$

where each a_i is a complex root of multiplicity m_i and $\sum_{i=1}^{r} m_i = d$.

Another way of stating this theorem is that the graph of $y = f(x)$ in $\mathbb{C}^2$ intersects the complex line $x = 0$ in d points, counted with multiplicity. A natural generalization of this would be to consider the intersection of a curve defined by $f(x, y) = 0$, where f is a degree d polynomial in $\mathbb{C}[x, y]$, and a line defined by $ax + by + c = 0$.

EXERCISE 3.3.11. Let $f(x, y) = x^2 - y^2 - 1$ and $g(x, y) = x$. Sketch $\mathrm{V}(f)$ and $\mathrm{V}(g)$ in $\mathbb{R}^2$. Do they intersect? Find $\mathrm{V}(f) \cap \mathrm{V}(g)$ in $\mathbb{C}^2$.

EXERCISE 3.3.12. Let $g(x, y) = ax + by + c$, $b \neq 0$, in $\mathbb{C}[x, y]$. Let $f(x, y) = \sum_i a_i x^{r_i} y^{s_i}$ be any polynomial of degree d in $\mathbb{C}[x, y]$. Show that the number of points in $\mathrm{V}(f) \cap \mathrm{V}(g)$ is d, if the points are counted with an appropriate notion of multiplicity. (Substitute $y = \dfrac{-ax - c}{b}$ into $f = 0$, so that $f = 0$ becomes a polynomial equation of degree d in the single variable x. Apply the Fundamental Theorem of Algebra.)

What about the intersection of two curves, one defined by a polynomial of degree d and the other defined by a polynomial of degree e? To answer this question we will need a more general definition of multiplicity—one that is inspired by the previous exercise, and for the most uniform statement we will need to consider curves in the complex projective plane.

3.3.3. Intersection Multiplicity. The goal of this section is to understand Bézout's Theorem on the number of points in the intersection of two plane curves. The statement of this theorem requires the definition of the intersection multiplicity of a point p in the intersection of two plane curves defined by polynomials f and g, respectively. We would like to define this notion in such a way that we can often, through elimination of variables, reduce its calculation to an application of the Fundamental Theorem of Algebra. The first step in this direction is to generalize the idea of multiplicity of a root.

We want a rigorous definition for the multiplicity of a point on a curve $\mathrm{V}(P)$, which will require us to first review multivariable Taylor series expansions.

EXERCISE 3.3.13. Show that $P(x, y) = 5 - 8x + 5x^2 - x^3 - 2y + y^2$ is equal to $(y - 1)^2 - (x - 2)^2 - (x - 2)^3$, by directly expanding the second polynomial. Now, starting with $P(x, y) = 5 - 8x + 5x^2 - x^3 - 2y + y^2$, calculate its Taylor series expansion at the point $(2, 1)$:

$$\text{Taylor expansion of } P \text{ at } (2,1) = \sum_{n,m=0}^{\infty} \frac{1}{n!m!} \frac{\partial^{n+m} P}{\partial x^n \partial y^m}(2,1)(x-2)^n (y-1)^m$$

$$= P(2,1) + \frac{\partial P}{\partial x}(2,1)(x-2) + \frac{\partial P}{\partial y}(2,1)(y-1) + \frac{1}{2}\frac{\partial^2 P}{\partial x^2}(2,1)(x-2)^2 + \dots$$

DEFINITION 3.3.2. Let f be a non-homogeneous polynomial (in any number of variables) and let p be a point in the set $\mathrm{V}(f)$. The *multiplicity of f at p*, denoted $m_p f$, is the degree of the lowest degree non-zero term of the Taylor series expansion of f at p.

Notice that if $p \notin V(f)$, then $f(p) \neq 0$, so the lowest degree non-zero term of the Taylor expansion of f at p is $f(p)$, which has degree zero. If $p \in V(f)$, then $f(p) = 0$, so $m_p f$ must be at least one.

EXERCISE 3.3.14. Let f be a non-homogeneous polynomial (in any number of variables) of degree n.

(1) Show that $m_p f = 1$ if and only if p is a nonsingular point. Hence, $m_p(f) = 1$ for every point $p \in V(f)$ if and only if $V(f)$ is nonsingular.
(2) Show that $m_p f \leq n$ for all $p \in V(f)$. Hence, $1 \leq m_p f \leq n$ for all $p \in V(f)$.

EXERCISE 3.3.15. Let $f(x, y) = xy$. What is the multiplicity of f at the origin? Let $p = (0, 1)$, and calculate $m_p f$.

EXERCISE 3.3.16. Let $f(x, y) = x^2 + xy - 1$. Calculate the multiplicity of f at $p = (1, 0)$.

We are interested in curves in the complex projective plane, $\mathbb{P}^2$, and hence in zero sets of homogeneous polynomials. Luckily this does not matter.

EXERCISE 3.3.17. Consider the homogeneous polynomial

$$P(x, y, z) = zy^2 - (x - z)^3.$$

We want to show that the point $(1 : 0 : 1) \in \mathrm{V}(P)$ has multiplicity two, no matter how P is dehomgenized. Show when we dehomogenize by setting $z = 1$, that the point $x = 1, y = 0$ has multiplicity two for $P(x, y, 1)$. Now show when we dehomogenize by setting $x = 1$, that the point $y = 0, z = 1$ has multiplicity two for $P(1, y, z)$.

EXERCISE 3.3.18. Let $(a : b : c) \in \mathrm{V}(f)$. Show no matter how we dehomogenize that the multiplicity of f at the point $(a : b : c)$ remains the same. (This is quite a long problem to work out in full detail).

The following theorem establishes the existence of a nicely behaved intersection multiplicity. We will not prove this theorem now, but we will revisit it in a later chapter after we have more fully developed the dictionary between algebra and geometry. The statement of this theorem and our treatment of it closely follows that of Fulton [**Ful69**].

THEOREM 3.3.19 (Intersection Multiplicity). Given polynomials f and g in $\mathbb{C}[x, y]$ and a point p in $\mathbb{C}^2$, there is a uniquely defined number $I(p, \mathrm{V}(f) \cap \mathrm{V}(g))$ such that the following axioms are satisfied.

(1) $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) \in \mathbb{Z}_{\geq 0}$.
(2) $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = 0$ iff $p \notin \mathrm{V}(f) \cap \mathrm{V}(g)$.
(3) For an affine change of coordinates T, $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = I(T(p), \mathrm{V}(T^{-1}f) \cap \mathrm{V}(T^{-1}g))$.
(4) $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = I(p, \mathrm{V}(g) \cap \mathrm{V}(f))$.
(5) $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) \geq m_p f \cdot m_p g$ with equality iff $\mathrm{V}(f)$ and $\mathrm{V}(g)$ have no common tangent at p.
(6) $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = \sum r_i s_i I(p, \mathrm{V}(f_i) \cap \mathrm{V}(g_i))$ when $f = \prod f_i^{r_i}$ and $g = \prod g_i^{s_i}$.
(7) $I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = I(p, \mathrm{V}(f) \cap \mathrm{V}(g + af))$ for all $a \in \mathbb{C}[x, y]$.

Note that Axioms Five and Seven suggest a way to compute intersection multiplicity by reducing it to the calculation of $m_p F$, for an appropriate polynomial F. We can easily extend this definition to curves in $\mathbb{P}^2(\mathbb{C})$ by dehomogening the curves making them into curves in $\mathbb{C}^2$ containing the point in question.

EXERCISE 3.3.20. Use the above axioms to show that for $p = (0, 0)$, $I(p, \mathrm{V}(x^2) \cap \mathrm{V}(y)) = 2$. Sketch $\mathrm{V}(x^2)$ and $\mathrm{V}(y)$.

EXERCISE 3.3.21. Show for $p = (0, 0)$, $I(p, \mathrm{V}(x^2 - y) \cap \mathrm{V}(y)) = 2$. Sketch $\mathrm{V}(x^2 - y)$ and $\mathrm{V}(y)$.

EXERCISE 3.3.22. Show for $p = (0, 0)$, $I(p, \mathrm{V}(y^2 - x^2 - x^3) \cap \mathrm{V}(x)) = 2$. Sketch $\mathrm{V}(y^2 - x^2 - x^3)$ and $\mathrm{V}(x)$.

EXERCISE 3.3.23. Let $f(x, y) = x^2 + y^2 - 1$. Give examples of a real polynomial $g(x, y) = ax + by + c$ such that $\mathrm{V}(x^2 + y^2 - 1) \cap \mathrm{V}(ax + by + c)$ in $\mathbb{R}^2$ has zero, one or two points, respectively. Now consider the intersections $\mathrm{V}(f) \cap \mathrm{V}(g)$ in $\mathbb{C}^2$. In each of your three examples, find these points of intersection, calculate their multiplicities, and verify that $\sum_p I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = (\deg f)(\deg g)$.

3.3.4. Statement of Bézout's Theorem.

EXERCISE 3.3.24. Let $f = x^2 + y^2 - 1$ and $g = x^2 - y^2 - 1$. Find all points of intersection of the curves $\mathrm{V}(f)$ and $\mathrm{V}(g)$. For each point of intersection p, send p to $(0, 0)$ via a change of coordinates T. Find $I(p, f \cap g)$ by calculating $I((0, 0), T(\mathrm{V}(f)) \cap T(\mathrm{V}(g)))$. Verify that $\sum_p I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = (\deg f)(\deg g)$.

EXERCISE 3.3.25. Let $f = y - x(x - 2)(x + 2)$ and $g = y - x$. Find all points of intersection of the curves $\mathrm{V}(f)$ and $\mathrm{V}(g)$. For each point of intersection p, send p to $(0, 0)$ via a change of coordinates T. Find $I(p, f \cap g)$ by calculating $I((0, 0), T(\mathrm{V}(f)) \cap T(\mathrm{V}(g)))$. Verify that $\sum_p I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = (\deg f)(\deg g)$.

The previous exercises may have led you to conjecture that if f and g are any polynomials, then $\sum_p I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = (\deg f)(\deg g)$. This is not true for all curves $\mathrm{V}(f)$ and $\mathrm{V}(g)$ in $\mathbb{C}^2$, though, as the next exercise illustrates.

EXERCISE 3.3.26. Let $f = y - x^2$ and $g = x$. Verify that the origin is the only point of $\mathrm{V}(f) \cap \mathrm{V}(g)$ in $\mathbb{C}^2$ and that $I((0, 0), \mathrm{V}(f) \cap \mathrm{V}(g)) = 1$.

The way to unify the previous exercises is to consider the polynomials as restrictions to an affine plane of homogeneous polynomials, well-defined on the projective plane. The corresponding curves in the projective plane will always intersect in the "correct" number of points, counted with multiplicity. This is Bézout's Theorem.

THEOREM 3.3.27 (Bézout's Theorem). *Let f and g be homogeneous polynomials in $\mathbb{C}[x, y, z]$ with no common component, and let $\mathrm{V}(f)$ and $\mathrm{V}(g)$ be the corresponding curves in $\mathbb{P}^2(\mathbb{C})$. Then*

$$\sum_{p \in \mathrm{V}(f) \cap \mathrm{V}(g)} I(p, \mathrm{V}(f) \cap \mathrm{V}(g)) = (\deg f)(\deg g).$$

EXERCISE 3.3.28. Homogenize the polynomials in Exercise 3.3.26, and find the two points of $\mathrm{V}(f) \cap \mathrm{V}(g)$ in $\mathbb{P}^2(\mathbb{C})$.

EXERCISE 3.3.29. Let $f = x^2 - y^2 - 1$ and $g = x - y$. Sketch $\mathrm{V}(f)$ and $\mathrm{V}(g)$ in $\mathbb{R}^2$. Homogenize f and g and verify Bézout's Theorem in this case. Describe the relationship between the points of intersection in $\mathbb{P}^2(\mathbb{C})$ and the sketch in $\mathbb{R}^2$. Repeat this exercise with $g = y + x$.

EXERCISE 3.3.30. Confirm that the curves defined by $x^2+y^2=1$ and $x^2+y^2=4$ do not intersect in $\mathbb{C}^2$. Homogenize these equations and confirm Bézout's Theorem in this case. Would a sketch of the circles in $\mathbb{R}^2$ give you any insight into the intersections in $\mathbb{P}^2(\mathbb{C})$?

3.3.5. Resultants.

The goal of this section is to use the resultant of two polynomials to find their common roots. The resultant will be the main tool in our proof of Bézout's Theorem.

While the Fundamental Theorem of Algebra tells us that a one-variable polynomial of degree d has exactly d roots, counting multiplicities, it gives us no means for actually finding these roots. Similarly, what if we want to know if two one-variable polynomials have a common root? The most naive method would be to find the roots for each of the polynomials and see if any of the roots are the same. In practice, though, this method is quite difficult to implement, since we have no easy way for finding these roots. The resultant is a totally different approach for determining if the polynomials share a root. The resultant is the determinant of a matrix; this determinant will be zero precisely when the two polynomials have a common root.

DEFINITION 3.3.3. The *resultant* $\mathrm{Res}(f,g;x)$ of two polynomials $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ and $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$ is defined to be the determinant of the $(m+n)\times(m+n)$ matrix

$$\mathrm{Res}(f,g;x)=\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \cdots & \ldots & \ldots & 0 \\ 0 & 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \cdots & \ldots & \ldots & 0 \\ 0 & 0 & \cdots & b_{m-1} & \cdots & \cdots & \cdots & b_0 \end{pmatrix}.$$

An important property of resultants is that $f(x)$ and $g(x)$ have a common root if and only if $\mathrm{Res}(f,g)=0$. The following three exercises will illustrate this property.

EXERCISE 3.3.31. Let $f(x)=x^2-1$ and $g(x)=x^2+x-2$.

(1) Find the roots of f and g and show that they share a root.
(2) Show that $\mathrm{Res}(f,g)=0$.

EXERCISE 3.3.32. Let $f(x) = x^2 - 1$ and $g(x) = x^2 - 4$.

(1) Find the roots of f and g and show that they have no roots in common.
(2) Show that $\mathrm{Res}(f, g) \neq 0$.

EXERCISE 3.3.33. (1) Let $f(x) = x - r$ and $g(x) = x - s$. Find $\mathrm{Res}(f, g)$. Verify that $\mathrm{Res}(f, g) = 0$ if and only if $r = s$.
(2) Let $f(x) = x - r$ and $g(x) = (x - s_1)(x - s_2)$. Find $\mathrm{Res}(f, g)$. Verify that $\mathrm{Res}(f, g) = 0$ if and only if $r = s_1$ or $r = s_2$.

EXERCISE 3.3.34. For a degree two polynomial $f(x) = a_2x^2 + a_1x + a_0 = a_2(x - r_1)(x - r_2)$, we have

$$\begin{aligned} \frac{a_1}{a_2} &= -(r_1 + r_2) \\ \frac{a_0}{a_2} &= r_1r_2. \end{aligned}$$

Use these relations between the coefficients and roots to show that if

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 = a_2(x - r_1)(x - r_2) \\ g(x) &= b_2x^2 + b_1x + b_0 = b_2(x - s_1)(x - s_2) \end{aligned}$$

then $\mathrm{Res}(f, g) = a_2^2b_2^2(r_1 - s_1)(r_1 - s_2)(r_2 - s_1)(r_2 - s_2)$.

EXERCISE 3.3.35. Let $f(x, y) = x^2 + y^2 - 2$ and $g(x, y) = x^2 - xy + y^2 + y - 2$.

(1) Treating f and g as polynomials in x, compute

$$R(y) = \mathrm{Res}(f, g; x) = \det \begin{pmatrix} 1 & 0 & y^2 - 2 & 0 \\ 0 & 1 & 0 & y^2 - 2 \\ 1 & -y & y^2 + y - 2 & 0 \\ 0 & 1 & -y & y^2 + y - 2 \end{pmatrix}$$

(2) Set $R(y) = 0$ and solve for y to find the projections on the y-axis of the points of intersection of $\mathrm{V}(f)$ and $\mathrm{V}(g)$.

EXERCISE 3.3.36. The two lines $\mathrm{V}(x-y)$ and $\mathrm{V}(x-y+2)$ are parallel in the affine plane, but intersect at $(1 : 1 : 0)$ in $\mathbb{P}^2$. Treating $f(x, y, z) = x - y$ and $g(x, y, z) = x - y + 2z$ as one-variable polynomials in x, show that $\mathrm{Res}(x - y, x - y + 2z; x) = 0$ when $z = 0$.

EXERCISE 3.3.37. Let $f(x, y) = 4x - 3y$ and $g(x, y) = x^2 + y^2 - 25$. Use the resultant $\mathrm{Res}(f, g; x)$ to find the points of intersection of $\mathrm{V}(f)$ and $\mathrm{V}(g)$.

EXERCISE 3.3.38. Let $f(x) = ax^2 + bx + c$.

(1) Find $\mathrm{Res}(f, f')$.
(2) Under what conditions will $\mathrm{Res}(f, f') = 0$?

In these last two exercises of this section, you will prove our previous assertion that the polynomials f and g have a common root if and only if $\mathrm{Res}(f, g) = 0$.

EXERCISE 3.3.39. Show that if r is a common root of f and g, then the vector $\mathbf{x} = \begin{pmatrix} r^{m+n-1} \\ r^{m+n-2} \\ \vdots \\ r \\ 1 \end{pmatrix}$ is in the null space of the resultant matrix of f and g, and thus $\mathrm{Res}(f, g) = 0$.

EXERCISE 3.3.40 (from Kirwan, *Complex Algebraic Curves* [**Kir92**], Lemma 3.3, p. 67). Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$.

(1) Prove that f and g have a common root $x = r$ if and only if there exists a polynomial $p(x)$ of degree $m - 1$ and a polynomial $q(x)$ of degree $n - 1$ such that $p(x)f(x) = q(x)g(x)$.

(2) Write $p(x) = \alpha_{m-1}x^{m-1} + \cdots + \alpha_1 x + \alpha_0$ and $q(x) = \beta_{n-1}x^{n-1} + \cdots + \beta_1 x + \beta_0$. By comparing coefficients, show that the polynomial equation $p(x)f(x) = q(x)g(x)$ corresponds to the system

$$\begin{array}{ccc} \alpha_{m-1}a_n & = & \beta_{n-1}b_m \\ \alpha_{m-1}a_{n-1} + \alpha_{m-2}a_n & = & \beta_{n-1}b_{m-1} + \beta_{n-2}b_m \\ & \vdots & \\ \alpha_0 a_0 & = & \beta_0 b_0 \end{array}$$

(3) Prove that this system of equations has a non-zero solution

$$(\alpha_{m-1}, \alpha_{m-2}, \ldots, \alpha_0, \beta_{n-1}, \beta_{n-2}, \ldots, \beta_0)$$

if and only if $\mathrm{Res}(f, g) = 0$.

3.3.6. Proof of Bézout's Theorem. Now we are ready to outline a proof of Bézout's Theorem. Full details can be found in Cox, Little, O'Shea, *Ideals Varieties and Algorithms* [**CLO07**], Chapter 8, Section 7.

EXERCISE 3.3.41. Let $f(x, y, z) = 3x + y + 2z$ and $g(x, y, z) = x + 5z$. Show that $\mathrm{Res}(f, g; z)$ is a homogeneous polynomial in x and y of degree 1.

EXERCISE 3.3.42. Let $f(x, y, z) = x^2 + y^2 + z^2$ and $g(x, y, z) = 2x + 3y - z$. Show that $\mathrm{Res}(f, g; z)$ is a homogeneous polynomial of degree 2.

EXERCISE 3.3.43. Let $f(x, y, z) = x^2 + xy + xz$ and $g(x, y, z) = x^2 + y^2 + z^2$. Show that $\mathrm{Res}(f, g; z)$ is a homogeneous polynomial of degree 4.

The next exercise is a generalization of these exercises.

EXERCISE 3.3.44 (Cox, Little, O'Shea [**CLO07**], Lemma 5, p. 425). Let $f, g \in \mathbb{C}[x, y, z]$ be homogeneous polynomials of degrees m and n, respectively. If $f(0,0,1)$ and $g(0,0,1)$ are nonzero, then $\mathrm{Res}(f, g; z)$ is homogeneous of degree mn in x and y.

EXERCISE 3.3.45. Let $f(x, y) = x^2-8xy+15y^2$. Show that $V(f) = \{(3,1),(5,1)\}$ and that $f(x, y) = (x-3y)(x-5y)$.

EXERCISE 3.3.46. Let $f(x, y) = x^2+y^2$. Show that $V(f) = \{(i,1),(-i,1)\}$ and that $f(x, y) = (x+iy)(x-iy)$.

EXERCISE 3.3.47. Let $f(x, y) = 2x^2 + 3xy + 4y^2$. Show that

$$V(f) = \{(-3+\sqrt{7}i, 2), (-3-\sqrt{7}i, 2)\}$$

and that

$$f(x, y) = \frac{1}{2}[2x - (-3+\sqrt{7}i)y][2x - (-3-\sqrt{7}i)y].$$

EXERCISE 3.3.48. Let $f(x, y) = x^3 - 5x^2y - 14xy^2$. Show that $V(f) = \{(0,1),(7,1),(-2,1)\}$ and that $f(x, y) = x(x+2y)(x-7y)$.

The previous exercises are special cases of the general result presented next.

EXERCISE 3.3.49. ([**CLO07**], Lemma 6, p. 427) Let $f \in \mathbb{C}[x, y]$ be homogeneous, and let $\mathrm{V}(f) = \{(r_1, s_1), \ldots, (r_t, s_t)\}$. Show that

$$f = c(s_1x - r_1y)^{m_1} \cdots (s_tx - r_ty)^{m_t},$$

where c is a nonzero constant.

EXERCISE 3.3.50. Let $\mathrm{V}(f)$ and $\mathrm{V}(g)$ be curves in $\mathbb{P}^2(\mathbb{C})$ with no common components. Choose homogeneous coordinates for $\mathbb{P}^2(\mathbb{C})$ so that the point $(0:0:1)$ is not in $\mathrm{V}(f)$ or $\mathrm{V}(g)$ and is not collinear with any two points of $\mathrm{V}(f)\cap\mathrm{V}(g)$. (What follows will be independent of this choice of coordinates, though it is not obvious.) Show that if $p = (u:v:w)$ is in $\mathrm{V}(f)\cap\mathrm{V}(g)$, then $I(p, \mathrm{V}(f)\cap\mathrm{V}(g))$ is the exponent of $(vx-uy)$ in the factorization of $Res(f, g; z)$, i.e. check the axioms that define intersection multiplicity.

EXERCISE 3.3.51. Deduce Bézout's Theorem from Exercises 3.3.44, 3.3.49, and 3.3.50.

EXERCISE 3.3.52. Let $f = yz - x^2$ and $g = yz - 2x^2$, and let $\mathcal{C} = \mathrm{V}(f)$ and $\mathcal{D} = \mathrm{V}(g)$.

(1) Find $\mathcal{C}\cap\mathcal{D}$ by solving $\mathrm{Res}(f, g; z) = 0$.

(2) One of the points of intersection is $(0:0:1)$. Check that $(1:0:0)$ is not in $\mathcal{C}$ or $\mathcal{D}$ and is not collinear with any two points of $\mathcal{C} \cap \mathcal{D}$.
(3) Find an invertible 3×3 matrix A such that $A(1:0:0) = (0:0:1)$.
(4) Compute $\mathrm{Res}(f \circ A^{-1}, g \circ A^{-1}; z)$. This will be a homogeneous polynomial in x, y; factor it completely and read the intersection multiplicities for the points in $A(\mathcal{C}) \cap A(\mathcal{D})$. These are the multiplicities for the corresponding points in $\mathcal{C} \cap \mathcal{D}$.

3.4. Regular Functions and Function Fields

3.4.1. The Affine Case. We want to understand the functions defined on a curve.

Exercise 3.4.1. Let $P(x,y) = x^2 + xy + 1$. Consider the two polynomials

$$f_1(x,y) = x^2 \quad \text{and} \quad f_2(x,y) = 2x^2 + xy + 1$$

Find a point $(a,b) \in \mathbb{C}^2$ such that

$$f_1(a,b) \neq f_2(a,b).$$

Now show that if $(a,b) \in \mathbb{C}^2$ with the extra condition that the corresponding point $(a,b) \in \mathrm{V}(P)$, then

$$f_1(a,b) = f_2(a,b).$$

To some extent, we would like to say that the polynomials f_1 and f_2 are the same as far as points on the curve $\mathrm{V}(P)$ are concerned.

Why is it in the above exercise that $f_1(a,b) = f_2(a,b)$ for any point $(a,b) \in \mathrm{V}(P)$? The key is to look at $f_2(x,y) - f_1(x,y)$.

Definition 3.4.1. Let $\mathrm{V}(P)$ be an irreducible curve. Let $f(x,y)$ and $g(x,y)$ be two polynomials. We say that

$$f(x,y) \sim g(x,y)$$

if $P(x,y)$ divides $f(x,y) - g(x,y)$.

Exercise 3.4.2. Show that $\sim$ defines an equivalence relation on polynomials. (Recall that an *equivalence relation* $\sim$ on a set X satisfies the conditions (i.) $a \sim a$ for all $a \in X$, (ii.) $a \sim b$ implies $b \sim a$, and (iii.) $a \sim b$ and $b \sim c$ implies $a \sim c$.)

Definition 3.4.2. Let $\mathrm{V}(P)$ be an irreducible curve. The *ring of regular functions* on $\mathrm{V}(P)$ is the space of all polynomials $f(x,y)$ modulo the equivalence relation $\sim$. Denote this ring by $\mathcal{O}(V)$. (We will also denote this by $\mathcal{O}_V$.)

You should be worried that we are calling $\mathcal{O}(V)$ a ring without proof. We shall remedy that situation now.

EXERCISE 3.4.3. We want to show that addition and multiplication are well-defined on $\mathcal{O}(V)$. Suppose that

$$f_1(x,y) \sim f_2(x,y) \quad \text{and} \quad g_1(x,y) \sim g_2(x,y).$$

Show that

$$f_1(x,y) + g_1(x,y) \sim f_2(x,y) + g_2(x,y),$$

which means that addition is well-defined in $\mathcal{O}(V)$. Also show

$$f_1(x,y)g_1(x,y) \sim f_2(x,y)g_2(x,y),$$

which means that multiplication is well-defined in $\mathcal{O}(V)$.

Hence for any curve $\mathrm{V}(P)$, we have the regular ring $\mathcal{O}(V)$ of functions defined on $\mathrm{V}(P)$. (Once we know the operations are well-defined, checking the ring axioms is straightforward and left as an exercise for the interested reader.)

EXERCISE 3.4.4. Suppose $\mathrm{V}(P)$ is an irreducible curve. Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be two polynomials. Show that if $fg \sim 0$, then either $f \sim 0$ or $g \sim 0$. Conclude that the ring of functions on an irreducible curve is an integral domain.

There is also a field of functions associated to $\mathrm{V}(P)$. Morally this field will simply be all of the fractions formed by the polynomials in $\mathcal{O}(V)$.

DEFINITION 3.4.3. Let the function field, $\mathcal{K}(V)$, for the curve $\mathrm{V}(P)$ be all rational functions

$$\frac{f(x,y)}{g(x,y)}$$

where

(1) P does not divide g (which is a way of guaranteeing that g, the denominator, is not identically zero on the curve $\mathrm{V}(P)$), and
(2) $\dfrac{f_1(x,y)}{g_1(x,y)}$ is identified with $\dfrac{f_2(x,y)}{g_2(x,y)}$ if P divides $f_1g_2 - f_2g_1$.

We want $\mathcal{K}(V)$ to mimic the rational numbers. Recall that the rational numbers $\mathbb{Q}$ are all the fractions

$$\frac{a}{b}$$

such that $a, b \in \mathbb{Z}$, $b \neq 0$ and $\frac{a}{b}$ is identified with $\frac{c}{d}$ if $ad - bc = 0$.

Now, you should be concerned with us calling $\mathcal{K}(V)$ a field. We need to define addition and multiplication on $\mathcal{K}(V)$, using the rational numbers, $\mathbb{Q}$, as a guide.

DEFINITION 3.4.4. On $\mathcal{K}(V)$, define addition and multiplication by

$$\frac{f(x,y)}{g(x,y)} + \frac{h(x,y)}{k(x,y)} = \frac{f(x,y)k(x,y) + g(x,y)h(x,y)}{g(x,y)k(x,y)}$$

and

$$\frac{f(x,y)}{g(x,y)} \cdot \frac{h(x,y)}{k(x,y)} = \frac{f(x,y)h(x,y)}{g(x,y)k(x,y)}.$$

EXERCISE 3.4.5. Suppose

$$f_1 \sim f_2, \quad g_1 \sim g_2, \quad h_1 \sim h_2, \quad \text{and} \quad k_1 \sim k_2.$$

Show that $\frac{f_1}{g_1} + \frac{h_1}{k_1}$ can be identified in $\mathcal{K}(V)$ to $\frac{f_2}{g_2} + \frac{h_2}{k_2}$. Similarly, show that $\frac{f_1}{g_1} \cdot \frac{h_1}{k_1}$ can be identified in $\mathcal{K}(V)$ to $\frac{f_2}{g_2} \cdot \frac{h_2}{k_2}$.

EXERCISE 3.4.6. Show that $\mathcal{K}(V)$ is a field. (This is an exercise in abstract algebra; its goal is not only to show that $\mathcal{K}(V)$ is a field but also to provide the reader with an incentive to review what a field is.)

3.4.2. The Projective Case. We have seen that the natural space for the study of curves is not $\mathbb{C}^2$ but the projective plane $\mathbb{P}^2$. The corresponding functions will have to be homogeneous polynomials. This section will be to a large extent a copying of the previous section, with the addition of the needed words about homogeneity.

EXERCISE 3.4.7. Let $P(x,y,z) = x^2 + xy + z^2$. Consider the two polynomials

$$f_1(x,y,z) = x^2 \quad \text{and} \quad f_2(x,y,z) = 2x^2 + xy + z^2$$

Find a point $(a:b:c) \in \mathbb{P}^2$ such that

$$f_1(a,b,c) \neq f_2(a,b,c).$$

Now show that if $(a:b:c) \in \mathbb{P}^2$ with the extra condition that the corresponding point $(a:b:c) \in \mathrm{V}(P)$, then

$$f_1(a,b,c) = f_2(a,b,c).$$

Why is it in the above exercise that $f_1(a,b,c) = f_2(a:b:c)$ for any point $(a:b:c) \in \mathrm{V}(P)$? The key is to look at $f_2(x,y,z) - f_1(x,y,z)$.

DEFINITION 3.4.5. Let $\mathrm{V}(P)$ be an irreducible curve. Let $f(x,y,z)$ and $g(x,y,z)$ be two homogeneous polynomials of the same degree. We say that

$$f(x,y,z) \sim g(x,y,z)$$

if $P(x,y,z)$ divides $f(x,y,z) - g(x,y,z)$.

EXERCISE 3.4.8. Show that $\sim$ defines an equivalence relation on polynomials. (Recall that an *equivalence relation* $\sim$ on a set X satisfies the conditions (i.) $a \sim a$ for all $a \in X$, (ii.) $a \sim b$ implies $b \sim a$, and (iii.) $a \sim b$ and $b \sim c$ implies $a \sim c$.)

In the affine case, we used the analogous equivalence relation to define the ring of polynomials on the curve $\mathrm{V}(P)$. That is a bit more difficult in this case, as we do not want to allow the adding of two homogeneous polynomials of different degrees. This is handled via defining the notion of a graded ring, which we will do in chapter five. Building to that definition, we consider:

EXERCISE 3.4.9. Suppose that

$$f_1(x, y, z) \sim f_2(x, y, z) \quad \text{and} \quad g_1(x, y, z) \sim g_2(x, y, z),$$

with the additional assumption that all four polynomials are homogeneous of the same degree. Show that

$$f_1(x, y, z) + g_1(x, y, z) \sim f_2(x, y, z) + g_2(x, y, z),$$

and

$$f_1(x, y, z)g_1(x, y, z) \sim f_2(x, y, z)g_2(x, y, z).$$

Luckily we have a projective analog to the functions field.

DEFINITION 3.4.6. Let the function field, $\mathcal{K}(V)$, for the curve $\mathrm{V}(P)$, where $P(x, y, z)$ is a homogeneous polynomial, be all rational functions

$$\frac{f(x, y, z)}{g(x, y, z)}$$

where

(1) both f and g are homogeneous of the same degree,
(2) P does not divide g (which is a way of guaranteeing that g, the denominator, is not identically zero on the curve $\mathrm{V}(P)$), and
(3) $\dfrac{f_1(x, y, z)}{g_1(x, y, z)}$ is identified with $\dfrac{f_2(x, y, z)}{g_2(x, y, z)}$ if P divides $f_1g_2 - f_2g_1$. We denote this identification by setting
$$\frac{f_1(x, y, z)}{g_1(x, y, z)} \sim \frac{f_2(x, y, z)}{g_2(x, y, z)}.$$

As before, we want $\mathcal{K}(V)$ to mimic the rational numbers.

DEFINITION 3.4.7. On $\mathcal{K}(V)$, define addition and multiplication by

$$\frac{f(x, y, z)}{g(x, y, z)} + \frac{h(x, y, z)}{k(x, y, z)} = \frac{f(x, y, z)k(x, y, z) + g(x, y, z)h(x, y, z)}{g(x, y, z)k(x, y, z)}$$

and

$$\frac{f(x, y, z)}{g(x, y, z)} \cdot \frac{h(x, y, z)}{k(x, y, z)} = \frac{f(x, y, z)h(x, y, z)}{g(x, y, z)k(x, y, z)},$$

when f, g, h and k are all homogeneous and f and g have the same degree and h and k have the same degree.

We now want to link the equivalence relation for the projective case with the equivalence relation for the affine case.

In fact, we will show that this $\mathcal{K}(V)$ is isomorphic, in some sense, to the function field of the previous section (which is why we are using the same notation for both). For now, we will specify the $\mathcal{K}(V)$ of this section as $\mathcal{K}_{\mathbb{P}}(V)$ and the $\mathcal{K}(V)$ of the previous section as $\mathcal{K}_{\mathbb{A}}(V)$

Define

$$T : \mathcal{K}_{\mathbb{P}}(V) \to \mathcal{K}_{\mathbb{A}}(V)$$

by setting

$$T\left(\frac{f(x,y,z)}{g(x,y,z)}\right) = \frac{f(x,y,1)}{g(x,y,1)}$$

We first show that T is well-defined.

EXERCISE 3.4.10. Let $f(x,y,z)$ and $g(x,y,z)$ be two homogeneous polynomials of the same degree such that $f(x,y,z) \sim g(x,y,z)$ with respect to the homogeneous polynomial $P(x,y,z)$. Show that $f(x,y,1) \sim g(x,y,1)$ with respect to the non-homogeneous polynomial $P(x,y,1)$.

EXERCISE 3.4.11. Let $f_1(x,y,z), f_2(x,y,z), g_1(x,y,z)$ and $g_2(x,y,z)$ be homogeneous polynomials of the same degree such that $f_1(x,y,z) \sim f_2(x,y,z)$ and $g_1(x,y,z) \sim g_2(x,y,z)$ with respect to the homogeneous polynomial $P(x,y,z)$. Show that in $\mathcal{K}_{\mathbb{A}}(V)$ we have

$$T\left(\frac{f_1(x,y,z)}{g_1(x,y,z)}\right) \sim T\left(\frac{f_1(x,y,z)}{g_1(x,y,z)}\right).$$

Hence T indeed maps the field $\mathcal{K}_{\mathbb{P}}(V)$ to the field $\mathcal{K}_{\mathbb{A}}(V)$. Next we want to show that T is a field homomorphism, which is the point of the next two exercises.

EXERCISE 3.4.12. Let $f(x,y,z)$ and $g(x,y,z)$ be two homogeneous polynomials of the same degree and let $h(x,y,z)$ and $k(x,y,z)$ be two other homogeneous polynomials of the same degree. Show that

$$T\left(\frac{f(x,y,z)}{g(x,y,z)} + \frac{h(x,y,z)}{k(x,y,z)}\right) = T\left(\frac{f(x,y,z)}{g(x,y,z)}\right) + T\left(\frac{h(x,y,z)}{k(x,y,z)}\right).$$

EXERCISE 3.4.13. Let $f(x,y,z)$ and $g(x,y,z)$ be two homogeneous polynomials of the same degree and let $h(x,y,z)$ and $k(x,y,z)$ be two other homogeneous polynomials of the same degree. Show that

$$T\left(\frac{f(x,y,z)}{g(x,y,z)} \cdot \frac{h(x,y,z)}{k(x,y,z)}\right) = T\left(\frac{f(x,y,z)}{g(x,y,z)}\right) \cdot T\left(\frac{h(x,y,z)}{k(x,y,z)}\right).$$

To show that T is one-to-one, we use that one-to-oneness is equivalent to the only element mapping to zero is zero itself.

EXERCISE 3.4.14. Suppose $f(x, y, z)$ and $g(x, y, z)$ are two homogeneous polynomials of the same degree such that

$$T\left(\frac{f(x,y,z)}{g(x,y,z)}\right) = 0$$

in $\mathcal{K}_{\mathbb{A}}(V)$. Show that

$$\frac{f(x,y,z)}{g(x,y,z)} = 0$$

in $\mathcal{K}_{\mathbb{P}}(V)$.

To finish the proof that T is an isomorphism, we must show that T is onto.

EXERCISE 3.4.15. Given two polynomials $f(x, y)$ and $g(x, y)$, find two homogeneous polynomials $F(x, y, z)$ and $G(x, y, z)$ of the same degree such that

$$T\left(\frac{F(x,y,z)}{G(x,y,z)}\right) = \frac{f(x,y)}{g(x,y)}.$$

3.5. The Riemann-Roch Theorem

The goal of this section is to develop the Riemann-Roch Theorem, a result that links the algebraic and topological properties of a curve.

3.5.1. Intuition behind Riemann-Roch. Here is a fairly simple question. Let $\mathcal{C} = \mathrm{V}(P)$ be a curve in $\mathbb{P}^2$. Choose some point p on the curve. Is there a rational function $F(x, y, z) \in \mathcal{K}(\mathcal{C})$ with a pole (an infinity) of order one exactly at the point p, with no other poles? Recall that a rational function in $\mathcal{K}(\mathcal{C})$ has the form

$$F(x,y,z) = \frac{f(x,y,z)}{g(x,y,z)},$$

where f and g are homogeneous polynomials of the same degree with the additional property that neither f not g are zero identically on $\mathrm{V}(P)$ (which means that the polynomial P can divide neither f nor g). The poles of F on the curve $\mathrm{V}(P)$ occur when the denominator of F is zero. Thus we must look at the set of intersection points:

$$\mathrm{V}(g) \cap \mathrm{V}(P).$$

By Bézout's theorem, there should be $\deg(g) \cdot \deg(P)$ points of intersection. Unless P has degree one, there cannot be only one zero in $\mathrm{V}(g) \cap \mathrm{V}(P)$, which means that F cannot have a single isolated pole of order one on $\mathcal{C}$.

There is a subtlety that we need to consider. It could be that the number of intersection points in $\mathrm{V}(g) \cap \mathrm{V}(P)$ is greater than one but that at all of these points, besides our chosen point p, the numerator f has the same zeros, canceling those from the denominator. The heart of Riemann-Roch is showing that this does not happen. The Riemann-Roch Theorem will give us information about what type of elements in $\mathcal{K}(\mathcal{C})$ can exist with prescribed poles on $\mathcal{C} = \mathrm{V}(P)$.

We now want to see that the straight line $\mathbb{P}^1$ has a particularly well-behaved function field.

Exercise 3.5.1. If x and y are the homogeneous coordinates for $\mathbb{P}^1$, show that the rational function

$$F(x, y) = \frac{x}{y}$$

has a single zero at $(0 : 1)$ and a single pole at $(1 : 0)$.

Exercise 3.5.2. For $\mathbb{P}^1$, find a rational function with a single zero at $(1 : -1)$ and a single pole at $(1 : 0)$.

Exercise 3.5.3. For $\mathbb{P}^1$, find a rational function with zeros at $(1 : -1)$ and at $(0 : 1)$ and a double pole at $(1 : 0)$.

Exercise 3.5.4. For $\mathbb{P}^1$, find a rational function with zeros at $(1 : -1)$ and $(0 : 1)$ and poles at $(1 : 0)$ and $(1 : 1)$.

Exercise 3.5.5. For $\mathbb{P}^1$, show that there cannot be a rational function with zeros at $(1 : -1)$ and at $(0 : 1)$ and a single pole at $(1 : 0)$ with no other poles.

3.5.2. Divisors. The goal of this section is to define divisors on a curve $\mathrm{V}(P)$.

In the last section, we asked several questions concerning zeros and poles on curves with prescribed multiplicities. We will now introduce divisors as a tool to keep track of this information.

Definition 3.5.1. A *divisor* on a curve $\mathcal{C} = \mathrm{V}(P)$ is a formal finite linear combination of points on $\mathcal{C}$ with integer coefficients, $D = n_1p_1 + n_2p_2 + \cdots + n_kp_k$. The sum $\sum_{i=1}^k n_i$ of the coefficients is called the *degree* of D. When each $n_i \geq 0$ we say that D is *effective*.

Given two divisors D_1 and D_2 on $\mathrm{V}(P)$, we say

$$D_1 \leq D_2$$

if and only if $D_2 - D_1$ is effective. This defines a partial ordering on the set of all divisors on $\mathrm{V}(P)$.

Part of the reason that divisors are natural tools to study a curve is their link with rational functions.

Consider a non-zero function F in the function field, $\mathcal{K}(\mathcal{C})$, of the curve $\mathcal{C} = \mathrm{V}(P)$. Associate to F the divisor $\mathrm{div}(F) = \sum n_ip_i$, where the sum is taken over all zeros and poles of F on $\mathrm{V}(P)$ and n_i is the multiplicity of the zero at p_i and $-n_j$ is the order of the pole at p_j.

Definition 3.5.2. Any divisor that can be written as $\operatorname{div}(w)$ for a function $w \in \mathcal{K}(\mathcal{C})$ is called a *principal divisor* on $\mathcal{C} = \mathrm{V}(P)$.

Note that for the plane curve $\mathcal{C} = \mathrm{V}(P)$ defined by $P(x,y,z) = 0$, any $w \in \mathcal{K}(\mathcal{C})$ can be written as $w = \frac{f(x,y,z)}{g(x,y,z)}$, where f and g are homogeneous polynomials of the same degree in $\mathbb{C}[x,y,z]/\langle P(x,y,z)\rangle$.

Exercise 3.5.6. Let x and y be homogeneous coordinates on $\mathbb{P}^1$ and let $w = \frac{x}{y}$. Write the divisor $\operatorname{div}(w)$ as a formal sum of points.

Exercise 3.5.7. Let x, y, z be homogeneous coordinates on $\mathbb{P}^2$. For the cubic curve $\mathrm{V}(y^2z - x^3 - xz^2)$, write the divisor $\operatorname{div}(\frac{y}{z})$ as a formal sum of points.

Exercise 3.5.8. Let x, y, z be homogeneous coordinates on $\mathbb{P}^2$. For the cubic curve $\mathrm{V}(y^2z - x^3 - xz^2)$, show that the divisor $D = 2(0:0:1) - 2(0:1:0)$ is principal.

Exercise 3.5.9. Show that a principal divisor has degree zero.

Exercise 3.5.10. Prove that the set of all divisors on a curve $\mathrm{V}(P)$ form an abelian group under addition and that the subset of principal divisors is a subgroup.

3.5.3. Vector space $L(D)$ associated to a divisor. The goal of this section is to associate to any divisor on a curve $\mathcal{C}$ a vector space that is a subspace of the function field $\mathcal{K}(\mathcal{C})$. The dimension of this vector space will be critical for the Riemann-Roch Theorem.

Definition 3.5.3. For a divisor D on a curve $\mathcal{C}$, define $L(D)$ to be

$$L(D) = \{F \in \mathcal{K}(\mathcal{C}) : F = 0 \text{ or } \operatorname{div}(F) + D \geq 0\}.$$

Thus for $D = \sum n_p p$, we have $F \in L(D)$ when F has a pole of order at most n_p for points p with $n_p > 0$ and F has a zero of multiplicity at least $-n_p$ at points p with $n_p < 0$.

Exercise 3.5.11. Consider the curve $\mathbb{P}^1$. Let $D = (1:0) + (0:1)$. Show that

$$\frac{(x-y)(x+y)}{xy} \in L(D).$$

Exercise 3.5.12. Consider the curve $\mathbb{P}^1$. Let $D = (1:0) + (0:1)$. Show that

$$\frac{(x-y)(x+y)}{xy} \in L(kD),$$

for any positive integer $k > 0$.

EXERCISE 3.5.13. Continuing with the previous problem. Show that

$$\frac{xy}{(x-y)(x+y)} \notin L(D).$$

EXERCISE 3.5.14. Let $D = (1:0:1)+(-1:0:1)$ be a divisor on $\mathrm{V}(x^2+y^2-z^2)$. Show that

$$\frac{x}{y} \in L(D)$$

but that $\frac{y}{x} \notin L(D)$.

EXERCISE 3.5.15. Let D be a divisor on $\mathrm{V}(P)$. Show that $L(D)$ is a complex vector space.

EXERCISE 3.5.16. For a smooth curve $\mathrm{V}(P)$, find $L(0)$.

EXERCISE 3.5.17. Find $L(D)$ for the divisor $D = (0:1)$ on $\mathbb{P}^1$.

EXERCISE 3.5.18. Prove if $\deg(D) < 0$, then $L(D) = \{0\}$, the trivial space.

EXERCISE 3.5.19. Prove if $D_1 \leq D_2$, then $L(D_1) \subseteq L(D_2)$.

In the next section, we will see that the dimension of $L(D)$ is finite.

3.5.4. $L(D+p)$ **versus** $L(D)$**.** The goal of this section is to begin the proof of the Riemann-Roch Theorem.

We write $l(D)$ for the dimension of $L(D)$ as a vector space over $\mathbb{C}$. At the end of this chapter we will be discussing the Riemann-Roch Theorem, which gives sharp statements linking the dimension, $l(D)$, of the vector space $L(D)$ with the degree of D and the genus of the curve $\mathcal{C}$. We will start the proof here, by proving:

THEOREM 3.5.20. Let D be a divisor on a curve $\mathcal{C}$ and let $p \in \mathcal{C}$ be any point on the curve. Then

$$l(D+p) \leq l(D) + 1.$$

By Exercise 3.5.19, we know that $l(D) \leq l(D+p)$. Thus the above theorem is stating that by adding a single point to a divisor, we can increase the dimension of the corresponding vector space by at most one.

EXERCISE 3.5.21. Let $D = \sum n_p p$ be a divisor on the curve $\mathrm{V}(P)$. Use this theorem together with the result of Exercise 3.5.18 to prove that $l(D)$, the dimension of the vector space $L(D)$, is finite.

The proof of Theorem 3.5.20 uses some basic linear algebra.

EXERCISE 3.5.22. Let V be a complex vector space. Let

$$T : V \to \mathbb{C}$$

be a linear transformation. Recall that the kernel of T is

$$\ker(T) = \{v \in V : T(v) = 0\}.$$

Show that $\ker(T)$ is a subspace of V.

EXERCISE 3.5.23. Using the above notation, show that

$$\dim(\ker(T)) \leq \dim(V) \leq \dim(\ker(T)) + 1.$$

(This problem will require you to look up various facts about linear transformations and dimensions.)

For the next few exercises, assume that D is a divisor on a curve $\mathcal{C}$ and $p \in \mathcal{C}$ is a point on the curve.

EXERCISE 3.5.24. Suppose there is a linear transformation

$$T : L(D + p) \to \mathbb{C}$$

such that

$$\ker(T) = L(D).$$

Show then that

$$l(D + p) \leq l(D) + 1.$$

Thus to prove the theorem it suffices to construct such a linear transformation. Let $D = \sum n_q q$, where each $n_q \in \mathbb{Z}$, the q are points on $\mathcal{C}$ and all but a finite number of the coefficients, n_q, are zero. We call the integer n_q the *multiplicity* of the point q for the divisor D.

EXERCISE 3.5.25. Show that the multiplicity of the point p for the divisor $D+p$ is exactly one more than the multiplicity of p for the divisor D.

EXERCISE 3.5.26. Let $p = (0 : 1 : 1) \in \mathrm{V}(x^2 + y^2 - z^2)$. Set $D = 2p + (1 : 0 : 1)$. Let $F \in L(D)$. Even though $F(x, y, z)$ can have a pole (a singularity) at the point p, show that the function $x^2 F(x, y, z)$ cannot have a pole at p. Show if p is a zero of the function $x^2 F(x, y, z)$, then $F \in L(D - p)$.

EXERCISE 3.5.27. Use the same notation as in the previous exercise. Define a map

$$T : L(D) \to \mathbb{C}$$

as follows. Dehomogenize by setting $z = 1$. Set $T(F)$ to be the number obtained by plugging in $(0, 1)$ to the function $x^2 F(x, y, 1)$. Show that

$$T\left(\frac{(2y - z)(2y + z)}{x^2}\right) = 3.$$

Exercise 3.5.28. Use the notation from the previous exercise. Show that

$$T : L(D) \to \mathbb{C}$$

is a linear transformation with kernel $L(D - p)$.

We need to make a few choices about our curve $\mathcal{C}$ and our point p. By choosing coordinates correctly, we can assume that $p = (0 : y : 1)$. We choose a line that goes through the point p and is not tangent to the curve $\mathcal{C}$. By rotating our coordinates, if needed, we can assume that the line is given by $\mathcal{L} = \mathrm{V}(x)$.

Exercise 3.5.29. Let n be the multiplicity of the point p for the divisor $D + p$. For any $F \in L(D + p)$, show that the function $x^n F(x, y, 1)$ does not have a pole at p.

Exercise 3.5.30. Using the notation from the previous problem, show that if $x^n F(x, y, 1)$ has a zero at p means that $F \in L(D)$.

Exercise 3.5.31. Let n be the multiplicity of the point p for the divisor $D + p$. Define

$$T : L(D + p) \to \mathbb{C}$$

by setting $T(F)$ to be the number obtained by plugging in $(0, y)$ to the function $x^n F(x, y, 1)$. Show that T is a linear transformation with kernel $L(D)$.

Thus we have shown that

$$l(D) \leq l(D + p) \leq l(D) + 1.$$

3.5.5. Linear equivalence of divisors. The goal of this section is to introduce a relation on divisors, called linear equivalence.

Recall that a divisor D on a curve $\mathcal{C}$ is called principal if it is of the form $\mathrm{div}(w)$ for some $w \in \mathcal{K}(\mathcal{C})$.

Definition 3.5.4. Two divisors D_1 and D_2 are *linearly equivalent*, written as $D_1 \equiv D_2$, if $D_1 - D_2$ is principal.

Exercise 3.5.32. Prove that linear equivalence is an equivalence relation on the set of all divisors on $\mathrm{V}(P)$.

Exercise 3.5.33. Prove for any two points p and q in $\mathbb{P}^1$, $p \equiv q$.

EXERCISE 3.5.34. For any fixed point p, prove that any divisor on $\mathbb{P}^1$ is linearly equivalent to mp for some integer m.

EXERCISE 3.5.35. Prove if $D_1 \equiv D_2$, then $L(D_1) \cong L(D_2)$ as vector spaces over $\mathbb{C}$.

3.5.6. Hyperplane divisors. The goal for this section is to explicitly calculate the dimensions, $l(D)$, for a special class of divisors.

We have defined divisors on a curve $\mathcal{C}$ as finite formal sums of points on $\mathcal{C}$. In section 3.5.2 we extended this definition by considering the divisor of a homogeneous polynomial $f(x, y, z)$, where $V(f)$ and $\mathcal{C}$ share no common component. We now look at an important case where $f(x, y, z)$ is linear.

EXERCISE 3.5.36. Consider the curve $\mathrm{V}(x^2 + y^2 - z^2)$. Determine the divisor

$$D_1 = \mathrm{V}(x - y) \cap \mathrm{V}(x^2 + y^2 - z^2)$$

and the divisor

$$D_2 = \mathrm{V}(x) \cap \mathrm{V}(x^2 + y^2 - z^2).$$

Show that $D_1 \equiv D_2$.

EXERCISE 3.5.37. Keeping with the notation from the previous problem, let D_3 be the divisor on

$$\mathrm{V}(x^4 + 2y^4 - x^3 z + z^4) \cap \mathrm{V}(x^2 + y^2 - z^2).$$

Show that $D_3 \equiv 4D_1$. (Hint: do not explicitly calculate the divisor D_3).

EXERCISE 3.5.38. Keeping with the notation from the previous problems, let $f(x, y, z)$ be a homogeneous polynomial of degree 3. Show that

$$\frac{f(x, y, z)}{(x - y)^3} \in L(3D_1).$$

EXERCISE 3.5.39. Keeping with the notation from the previous problems, let $f(x, y, z)$ be a homogeneous polynomial of degree k. Show that

$$\frac{f(x, y, z)}{(x - y)^k} \in L(kD_1).$$

DEFINITION 3.5.5. Let $\mathcal{C} = \mathrm{V}(P)$ be a plane curve defined by a homogeneous polynomial $P(x, y, z)$ of degree d. Define a *hyperplane divisor* H on $\mathcal{C}$ to be the divisor of zeros of a linear function in $\mathbb{C}[x, y, z]$, meaning that for some linear function $\ell(x, y, z)$, set

$$H = \mathrm{V}(\ell) \cap \mathrm{V}(P).$$

We now consider the more general case.

EXERCISE 3.5.40. Suppose that H and H' are hyperplane divisors on a curve $\mathcal{C}$. Prove that $H \equiv H'$.

EXERCISE 3.5.41. With the same notation as the previous problem, show for any homogeneous polynomial $f(x,y,z)$ of degree m in $\mathbb{C}[x,y,z]$ that

$$\frac{f(x,y,z)}{\ell^m} \in L(mH).$$

Now we start calculating $l(mH) = \dim L(mH)$, for any hyperplane divisor H.

We know from the above exercise that $L(mH)$ contains elements of the form $\frac{f(x,y,z)}{\ell^m}$. In fact, every element in $L(mH)$ can be written in this form. To prove this we use

THEOREM 3.5.42 (Noether's AF+BG Theorem). [**?**]

Let $F(x,y,z)$ and $G(x,y,z)$ be homogeneous polynomials defining plane curves that have no common component. Let $U(x,y,z)$ be a homogeneous polynomial that satisfies the following condition: suppose for every point P in the intersection $V(F) \cap V(G)$, $I_P(F,U) \geq I_P(F,G)$. Then there are homogeneous polynomials A and B such that $U = AF + BG$.

EXERCISE 3.5.43. In the case of the Theorem, what are the degrees of the polynomials A and B?

EXERCISE 3.5.44. Let $F(x,y,z) = x$ and $G(x,y,z) = y$. Show that any polynomial U vanishing at $(0:0:1)$ satisfies the condition of the Theorem, thus there are A and B such that $U = AF + BG$.

EXERCISE 3.5.45. Let $F(x,y,z) = x^2 + y^2 + z^2$ and $G(x,y,z) = x^3 - y^2 z$. Show that the polynomial $U = x^4 + y^2 z^2$ satisfies the condition of the Theorem, and find A and B such that $U = AF + BG$.

We now use this Theorem to determine the form of the general element in $L(mH)$ in the following steps.

EXERCISE 3.5.46. Let $U \in L(mH)$. Show that U can be written as $U = \frac{u}{v}$ where u and v are homogeneous polynomials of the same degree in $\mathbb{C}[x,y,z]$ and $\operatorname{div}(v) \leq \operatorname{div}(u) + \operatorname{div}(\ell^m)$.

EXERCISE 3.5.47. Let $\mathcal{C} = V(F)$ and let $U = \frac{u}{v} \in L(mH)$, where u and v are homogeneous polynomials of the same degree in $\mathbb{C}[x,y,z]$. Show for all $P \in V(F) \cap V(v)$, $I_P(F, u\ell^m) \geq I_P(F,v)$.

EXERCISE 3.5.48. Under the assumptions of the previous exercise, use Noether's Theorem to conclude there exist A and B with $u\ell^m = AF + Bv$. Show that this implies $U = \frac{B}{\ell^m}$ in $K(C)$.

Thus the vector space $L(mH)$ consists of all functions in $K(C)$ of the form $\frac{f}{\ell^m}$ for homogeneous polynomials f of degree m. To find the dimension of $L(mH)$, we need to find the dimension of the vector space of possible numerators, f. The key will be that P cannot divide f.

EXERCISE 3.5.49. Let $\mathbb{C}_m[x, y, z]$ denote the set of all homogeneous polynomials of degree m together with the zero polynomial. Show that if $f, g \in \mathbb{C}_m[x, y, z]$ and if $\lambda, \mu \in \mathbb{C}$, then

$$\lambda f + \mu g \in \mathbb{C}_m[x, y, z].$$

Conclude that $\mathbb{C}_m[x, y, z]$ is a vector space over $\mathbb{C}$.

EXERCISE 3.5.50. Show that $\dim \mathbb{C}_1[x, y, z] = 3$. Show that a basis is $\{x, y, z\}$.

EXERCISE 3.5.51. Show that $\dim \mathbb{C}_2[x, y, z] = 6$. Show that a basis is $\{x^2, xy, xz, y^2, yz, z^2\}$.

EXERCISE 3.5.52. Show that

$$\dim \mathbb{C}_m[x, y, z] = \binom{m+2}{m}.$$

(By definition

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

This number, pronounced "n choose k", is the number of ways of choosing k items from n, where order does not matter.)

EXERCISE 3.5.53. Let $P(x, y, z)$ be a homogeneous polynomial of degree d. In the vector space $\mathbb{C}_m[x, y, z]$, let

$$W = \{f(x, y, z) \in \mathbb{C}_m[x, y, z] : P|f\}.$$

If $f, g \in W$ and if $\lambda, \mu \in \mathbb{C}$, then show

$$\lambda f + \mu g \in W.$$

Show that W is a vector subspace of $\mathbb{C}_m[x, y, z]$.

EXERCISE 3.5.54. With the notation of the previous problem, show that the vector space W is isomorphic to the vector space $\mathbb{C}_{m-d}[x, y, z]$. (Recall that this means you must find a linear map $T : \mathbb{C}_{m-d}[x, y, z] \to W$ that is one-to-one and onto.) Conclude that

$$\dim(W) = \dim \mathbb{C}_{m-d}[x, y, z].$$

EXERCISE 3.5.55. Show that

$$l(mH) = \dim \mathbb{C}_m[x, y, z] - \dim \mathbb{C}_{m-d}[x, y, z],$$

where $\mathbb{C}_n[x, y, z]$ is the space of homogeneous polynomials of degree n. Thus

$$l(mH) = \frac{(m+1)(m+2)}{2} - \frac{(m-d+1)(m-d+2)}{2}.$$

Exercise 3.5.56. Let ℓ be a linear function and let H be the corresponding hyperplane divisor on $\mathrm{V}(P)$, where $P(x, y, z)$ is homogeneous of degree d. Show that $\deg(H) = d$ and in general, that $\deg(mH) = md$. (Hint: Think Bézout.)

Exercise 3.5.57. Use the degree-genus formula $g = \dfrac{(d-1)(d-2)}{2}$ to show that

$$l(mH) = md - g + 1.$$

3.5.7. Riemann's Theorem.

Our goal is to prove Riemann's Theorem.

Throughout this section, let $\mathcal{C} = \mathrm{V}(P)$ be a plane curve of degree d and genus g.

Theorem 3.5.58 (Riemann's Theorem). If D is a divisor on a plane curve $\mathcal{C}$ of genus g, then

$$l(D) \geq \deg D - g + 1.$$

Our real goal is eventually to prove the Riemann-Roch Theorem, which finds the explicit term that is needed to change the above inequality into an equality.

Exercise 3.5.59. Show that for any hyperplane divisor H and any positive integer m, we have

$$l(mH) = \deg(mH) - g + 1.$$

Following notation used in Fulton's *Algebraic Curves* [**Ful69**], set

$$S(D) = \deg D + 1 - l(D).$$

Exercise 3.5.60. Suppose that for all divisors D we have

$$S(D) \leq g.$$

Show that Riemann's theorem is then true.

Thus we want to show that $S(D) \leq g$, for any divisor D.

Exercise 3.5.61. Show, for any hyperplane divisor H, that $S(mH) = g$ for all positive integers m.

Exercise 3.5.62. Let $D_1 \leq D_2$. Show that $l(D_1) \leq l(D_2)$.

Exercise 3.5.63. Recall for any divisor D and point p on the curve $\mathcal{C}$ that $l(D) \leq l(D + p) \leq l(D) + 1$. Show that

$$S(D + p) \geq S(D).$$

EXERCISE 3.5.64. Suppose that $D_1 \equiv D_2$ for two divisors on the curve $\mathcal{C}$. Show that

$$S(D_1) = S(D_2).$$

EXERCISE 3.5.65. Let $f(x, y, z) \in \mathcal{O}(V)$ be a homogeneous polynomial of degree m. Let D be the divisor on

$$\mathrm{V}(f) \cap \mathrm{V}(P)$$

and let H be a hyperplane divisor on $\mathcal{C}$. Show that $D \equiv mH$ and that $\deg(D) = md$.

EXERCISE 3.5.66. Let $p = (a : b : c) \in \mathrm{V}(P)$ for some curve $\mathrm{V}(P)$ of degree d. Suppose that not both a and b are zero. (This is not a big restriction on the point.) Let

$$f(x, y, z) = ay - bx.$$

Let

$$D = \mathrm{V}(f) \cap \mathrm{V}(P)$$

be a divisor on $\mathrm{V}(P)$. Show that $p \leq D$.

EXERCISE 3.5.67. Let $p_1 = (a_1 : b_1 : c_1) \in \mathrm{V}(P)$ and $p_2 = (a_2 : b_2 : c_2) \in \mathrm{V}(P)$ for some curve $\mathrm{V}(P)$ of degree d. Suppose that not both a_1 and b_1 are zero and similarly for a_2 and b_2. Let

$$f(x, y, z) = (a_1 y - b_1 x)(a_2 y - b_2 x).$$

Let

$$D = \mathrm{V}(f) \cap \mathrm{V}(P)$$

be a divisor on $\mathrm{V}(P)$. Show that $p_1 + p_2 \leq D$.

EXERCISE 3.5.68. Let $p_1, p_2, \ldots, p_k \in \mathrm{V}(P)$ for some curve $\mathrm{V}(P)$ of degree d. Find a polynomial f such that if

$$D = \mathrm{V}(f) \cap \mathrm{V}(P)$$

then $p_1 + \cdots + p_k \leq D$.

EXERCISE 3.5.69. Let H be a hyperplane divisor on $\mathcal{C}$. Using the divisor D from the previous problem, show that there is a positive integer m such that $D \equiv mH$.

EXERCISE 3.5.70. Let $D = \sum n_k p_k$ be an effective divisor on $\mathcal{C} = \mathrm{V}(P)$. Let n be any positive integer. Prove that there is an $m \geq n$ and points $q_1, \ldots, q_k$ on $\mathcal{C}$ such that $D + \sum q_i \equiv mH$.

EXERCISE 3.5.71. Let $D = \sum n_k p_k$ be a divisor on a curve $\mathrm{V}(P)$. Show that there are points $q_1, \ldots, q_n$ on $\mathrm{V}(P)$, which need not be distinct, such that $D + q_1 + \cdots + q_n$ is an effective divisor.

EXERCISE 3.5.72. Let $D = \sum n_k p_k$ be a divisor on a curve $\mathrm{V}(P)$. Let n be a positive integer. Prove that there exists an integer m, $m \geq n$, and points $q_1, \ldots, q_k$ on $\mathcal{C}$ such that $D + \sum q_i \equiv mH$.

EXERCISE 3.5.73. Let D be a divisor on a curve $\mathcal{C}$ and let H be any hyperplane. Show that there is a positive integer m so that

$$S(D) \leq S(mH).$$

EXERCISE 3.5.74. Prove Riemann's Theorem.

3.5.8. Differentials. In calculus we learn that the slope of the graph $y = f(x)$ is given by the derivative $\frac{dy}{dx}$ at each point where it is defined. For a curve defined implicitly, say by an equation $P(x, y) = 0$, using implicit differentiation we compute $\frac{dy}{dx} = \frac{\frac{\partial P}{\partial x}}{\frac{\partial P}{\partial y}}$. Similarly we define the differential of the function $P(x, y)$ to be $dP = \frac{\partial P}{\partial x}dx + \frac{\partial P}{\partial y}dy$.

More generally, a differential form on $\mathbb{C}^2$ is a sum of terms $g\ df$, for functions $f, g \in \mathcal{K}(\mathbb{C}^2)$ (recall that this means f and g are ratios of polynomials in two variables). Of course we have the usual rules from calculus,

$$\begin{aligned} d(f+g) &= df + dg \\ d(cf) &= cdf \\ d(fg) &= gdf + fdg \end{aligned}$$

for $c \in \mathbb{C}, f, g \in \mathcal{K}(\mathbb{C}^2)$.

EXERCISE 3.5.75. (1) Find the differential of $f(x, y) = x^2 + y^2 - 1$.
(2) Use your answer for part (1) to find the slope of the circle $f(x, y) = 0$ at a point (x, y).
(3) For which points on the circle is this slope undefined?

EXERCISE 3.5.76. (1) Find the differential of $f(x, y) = x^3 + x - y^2$.
(2) Use your answer for part (1) to find the slope of the curve $f(x, y) = 0$ at a point (x, y).
(3) For which points on the curve is this slope undefined?

EXERCISE 3.5.77. Prove that the set of all differential forms on $\mathbb{C}^2$ is a vector space over $\mathcal{K}(\mathbb{C}^2)$ with basis $\{dx, dy\}$.

To define differentials on an affine curve $P(x, y) = 0$ in $\mathbb{C}^2$, we use the relation $dP = \frac{\partial P}{\partial x}dx + \frac{\partial P}{\partial y}dy = 0$. As in calculus this gives the slope $-\frac{\partial P/\partial x}{\partial P/\partial y}$ of the curve when $\frac{\partial P}{\partial y} \neq 0$. We can also use this expression to express dy in the form $g(x, y)dx$ for a function $g \in \mathcal{K}(\mathbb{C}^2)$ (namely, $g = -\frac{\partial P/\partial x}{\partial P/\partial y}$, the slope of our curve).

Suppose that $f \in \mathcal{K}(\mathcal{C})$ is determined by some $F(x, y) \in \mathcal{K}(\mathbb{C}^2)$ restricted to $\mathcal{C}$. We wish to define the differential df to be dF restricted to $\mathcal{C}$. This appears to depend on the choice of $F(x,y)$, which is only well-defined up to the addition of terms of the form $G(x,y)P(x,y)$ for $G(x,y) \in \mathcal{K}(\mathbb{C}^2)$. Yet $d(GP) = G(x,y)\ dP + P(x,y)\ dG$, and we know that $P(x,y) = dP = 0$ on $\mathcal{C}$. Thus any $F + GP \in \mathcal{K}(\mathbb{C}^2)$ that represents $f \in \mathcal{K}(\mathcal{C})$ has $d(F+GP) = dF$ when restricted to $\mathcal{C}$, so taking df to be the restriction of dF is well-defined. With this established, we may define differentials on an affine curve $\mathcal{C} = \mathrm{V}(P)$ to be sums of terms of the form $g\ df$ for $g, f \in \mathcal{K}(\mathcal{C})$.

Exercise 3.5.78. Prove that the set of all differential forms on a non-singular curve $\mathcal{C} = \mathrm{V}(P)$ in $\mathbb{C}^2$ is a vector space over $\mathcal{K}(\mathcal{C})$.

Exercise 3.5.79. Prove that the vector space of differentials on a non-singular curve $\mathcal{C} = \mathrm{V}(P)$ in $\mathbb{C}^2$ has dimension one over $\mathcal{K}(\mathcal{C})$.

3.5.9. Local Coordinates. To extend our definition of differential forms to projective curves $\mathcal{C} = \mathrm{V}(P)$ in $\mathbb{P}^2$, we will consider the affine pieces of $\mathcal{C}$ obtained by dehomogenizing the defining polynomial $P(x,y,z)$. We can cover $\mathbb{P}^2$ by three *affine coordinate charts*, that is three copies of $\mathbb{C}^2$, as follows. The bijective map

$$\varphi : \mathbb{P}^2 \backslash \mathrm{V}(z) \to \mathbb{C}^2$$

defined by $\varphi(x:y:z) = \left(\frac{x}{z}, \frac{y}{z}\right)$ assigns coordinates $r = \frac{x}{z}, s = \frac{y}{z}$ for all points $(x:y:z)$ with $z \neq 0$. Similarly we can set $t = \frac{x}{y}, u = \frac{z}{y}$ for all $(x:y:z)$ with $y \neq 0$, and $v = \frac{y}{x}, w = \frac{z}{x}$ when $x \neq 0$. (These three coordinate systems give a more careful way to "dehomogenize" polynomials in $\mathbb{P}^2$, compared to simply setting one coordinate equal to 1 as in the first chapter.)

Exercise 3.5.80. Verify that the map $\varphi : \mathbb{P}^2 \backslash \mathrm{V}(z) \to \mathbb{C}^2$ is a bijection.

Exercise 3.5.81. Use the above coordinates for three affine charts on $\mathbb{P}^2$.

(1) Find coordinates for the point $(-1:2:3)$ in each of the three coordinate charts.
(2) Find all points in $\mathbb{P}^2$ that cannot be represented in (r,s) affine space.
(3) Find the points in $\mathbb{P}^2$ that are not in either (r,s) or (t,u) affine space.

Exercise 3.5.82. In this exercise you will find the change of coordinates functions between coordinate charts.

(1) Write the local coordinates r and s as functions of t and u.
(2) Write the local coordinates r and s as functions of v and w.
(3) Write the local coordinates v and w as functions of t and u.

Now let $\mathcal{C}$ be the curve defined by the vanishing of a homogeneous polynomial $P(x,y,z)$. We will work locally by considering an affine part of the curve in one of the affine charts. Let $p = (a:b:c) \in \mathcal{C}$. At least one of a, b, c must be non-zero; let's assume $c \neq 0$, so we can look at the affine part of our curve $P(\frac{x}{z}, \frac{y}{z}, 1) = P(r, s) = 0$ in $\mathbb{C}^2$. We assume that $\mathcal{C}$ is smooth, thus $\frac{\partial P}{\partial r} \neq 0$ or $\frac{\partial P}{\partial s} \neq 0$ at $(r, s) = (\frac{a}{c}, \frac{b}{c})$.

We will use the following version of the Implicit Function Theorem for curves in the plane. This Theorem tells us that when p is a smooth point of a curve, near p the curve looks like the graph of a function. For example, the circle $x^2 + y^2 = 1$ is smooth at the point $p = (0, 1)$, and we know that near p we can write the circle as the graph $y = \sqrt{1 - x^2}$. Although this formula will not work for all points of the circle, near p we may use x as a local coordinate for our curve.

Theorem 3.5.83. Implicit Function Theorem (Kirwan, Appendix B)

Let $F(v, w)$ be a polynomial over $\mathbb{C}$ and let (v_0, w_0) be a point on the curve $F = 0$. Assume $\frac{\partial F}{\partial w}(v_0, w_0) \neq 0$. Then there are open neighborhoods V and W of v_0 and w_0, respectively, and a holomorphic function $f : V \to W$ such that $f(v_0) = w_0$ and for $v \in V$, if $f(v) = w$ then $F(v, w) = 0$.

In our example $P(x, y) = x^2 + y^2 - 1 = 0$ at the point $p = (0, 1)$, $\frac{\partial P}{\partial y} \neq 0$, thus by the Implicit Function Theorem x is a local coordinate.

Exercise 3.5.84. We extend our circle example to the projective curve $\mathcal{C} = \mathrm{V}(x^2 + y^2 - z^2)$.

(1) Let's consider the point $p = (1 : 0 : 1)$, so we can dehomogenize to (r, s) affine coordinates. Find a function $f(s)$ that expresses $\mathcal{C}$ as the graph $r = f(s)$ near p. At this point $\frac{\partial f}{\partial s} = 0$; explain why r is not a local coordinate at p.
(2) Alternately write the affine part of $\mathcal{C}$ in (v, w) coordinates and give an alternate expression for $\mathcal{C}$ as the graph of a function near p.

Exercise 3.5.85. Let $\mathcal{C} = \mathrm{V}(x^2 - yz)$.

(1) Show that this curve is covered by the two charts (r, s) and (t, u), that is every point $p \in \mathcal{C}$ can be written in at least one of these coordinate systems.
(2) Show that r is a local coordinate at all points $p = (a : b : c) \in \mathcal{C}$ with $c \neq 0$.
(3) Show that t is a local coordinate at the point $(0 : 1 : 0)$.

Exercise 3.5.86. Let $\mathcal{C} = \mathrm{V}(x^3 - y^2 z - xz^2)$.

(1) Show that every point $p \in \mathcal{C}$ can be written in either (r, s) or (t, u) coordinates.
(2) Show that r is a local coordinate at all points $p = (a : b : c) \in \mathcal{C}$ with $b, c \neq 0$.
(3) Find all points on $\mathcal{C}$ with $b = 0$ or $c = 0$ and determine a local coordinate at each point.

We will use local coordinates to write differential forms on curves. As the derivative provides local (that is, in a small neighborhood of a point) information about a curve, it makes sense to use this approach for differentials.

Let ω be a differential form on a non-singular curve $\mathrm{V}(P) \subset \mathbb{C}^2$. In a previous exercise, we showed that any differential form on an affine curve in $\mathbb{C}^2$ can be written as $f(x,y)dx$. At any point $p=(a,b)$ on the curve at least one of $\frac{\partial P}{\partial x}, \frac{\partial P}{\partial y}$ must be non-zero (by the definition of non-singular). Assume $\frac{\partial P}{\partial y}(a,b) \neq 0$; by the Implicit Function Theorem there exists a holomorphic function g defined on neighborhoods of a and b with $y = g(x)$. This means that we can consider x as a coordinate for the curve near the point p and we can write $\omega = h(x)dx$ near p for some rational function $h(x)$.

EXERCISE 3.5.87. Consider the curve $\mathrm{V}(x^2 - y)$ in $\mathbb{C}^2$.

(1) Show that x is a coordinate at all points on this curve.
(2) Write the differential dy in the form $f(x)dx$.
(3) Show that any differential form can be written as $h(x)dx$ for some rational function $h(x)$.

EXERCISE 3.5.88. Consider the curve $\mathrm{V}(x^2 + y^2 - 1)$ in $\mathbb{C}^2$.

(1) Show that x is a coordinate at all points (a,b) with $b \neq 0$.
(2) At each point on $\mathrm{V}(x^2+y^2-1) \cap \mathrm{V}(y)$ find $g(y)$ with $x = g(y)$.
(3) Write the differential dx in the form $f(y)dy$.

Using local coordinates we can now describe differential forms on a curve $\mathcal{C} = V(P(x,y,z))$ in $\mathbb{P}^2$. Using the previous notation we have three affine pieces of our curve, corresponding to the $(r,s) = (\frac{x}{z}, \frac{y}{z})$, $(t,u) = (\frac{x}{y}, \frac{z}{y})$, and $(v,w) = (\frac{y}{x}, \frac{z}{x})$ coordinate charts. For an affine piece of our curve, say in the (r,s) coordinate system, we can write a differential form as $h(r)dr$ (or $h(s)ds$) for a rational function h. Using the changes of coordinates between the three affine charts we can translate this form to each set of coordinates. Thus a differential form on $\mathcal{C}$ is a collection of differential forms on each affine piece of our curve, such that these pieces "match" under our changes of coordinates.

EXERCISE 3.5.89. Let $\mathcal{C}$ be the curve $\mathrm{V}(x^2 - yz)$ in $\mathbb{P}^2$, which dehomogenizes to $r^2 - s = 0$ in the (r,s) affine chart.

(1) Show that the differential form ds can be written as $2rdr$.
(2) Use the appropriate change of coordinates to write ds in the form $f(u)du$.
(3) Use the appropriate change of coordinates to write ds in the form $g(w)dw$.

EXERCISE 3.5.90. Let $\mathcal{C}$ be the curve $\mathrm{V}(x^2+y^2-z^2)$ in $\mathbb{P}^2$. Use the appropriate changes of coordinates to write the differential form dr in each coordinate chart.

3.5.10. The Canonical Divisor. We now define the divisor associated to a differential form on a smooth projective curve $\mathcal{C} \subset \mathbb{P}^2$. For any differential form ω, we want to determine a divisor $div(\omega) = \sum n_p p$, a finite sum of points $p \in \mathcal{C}$ with integer coefficients n_p.

Throughout this section we will use the notation:

$$r = \frac{x}{z},\ s = \frac{y}{z},$$

$$t = \frac{x}{y},\ u = \frac{z}{y},$$

$$v = \frac{y}{x},\ w = \frac{z}{x}.$$

To define the canonical divisor, let $p = (a : b : c)$ be any point on $\mathcal{C}$ and assume $c \neq 0$. By de-homogenizing we can consider p as a point on the affine piece of $\mathcal{C}$ given by $P(\frac{x}{z}, \frac{y}{z}, 1) = 0$ in $\mathbb{C}^2$. As $\mathcal{C}$ is non-singular, at least one of

$$\frac{\partial P}{\partial x}, \frac{\partial P}{\partial y}, \frac{\partial P}{\partial z}$$

is non-zero at $(a : b : c)$. Moreover, as $c \neq 0$, by Euler's formula either $\frac{\partial P(r,s,1)}{\partial r} \neq 0$ or $\frac{\partial P(r,s,1)}{\partial s} \neq 0$ at $(r, s) = (\frac{a}{c}, \frac{b}{c})$. Assume $\frac{\partial P(r,s,1)}{\partial s} \neq 0$; then we have r as local coordinate at p. Thus we can write

$$\omega = h(r)dr$$

near p. We define the order n_p of $\mathrm{div}(\omega)$ at p to be the order of the divisor of the rational function $h(r)$ at p.

As a first example, let $\mathcal{C}$ be the curve $\mathrm{V}(x^2 - yz)$, and let $\omega = ds$. In a previous exercise we determined how to transform ω among the different affine charts. We now use these expressions to compute the divisor of ω.

Exercise 3.5.91. (1) Show that r is a local coordinate for all points $p = (a : b : c)$ on $\mathcal{C}$ with $c \neq 0$.
(2) Show that we can write ω in the form $2rdr$ for all points with $c \neq 0$.
(3) Show that at all points with $c \neq 0$, the divisor of $2r$ is $(0 : 0 : 1)$, since $2r$ has a simple zero at this point.
(4) Show that when $c = 0$, then $p \in \mathcal{C}$ implies that $p = (0 : 1 : 0)$. Verify that t is a local coordinate for $\mathcal{C}$ at $(0 : 1 : 0)$.
(5) Show that $\omega = -\frac{2}{t^3}dt$ at $(0 : 1 : 0)$, and at this point $-\frac{2}{t^3}$ has a pole of order 3 at $(0 : 1 : 0)$: thus the divisor is $-3(0 : 1 : 0)$.
(6) Conclude that the divisor of ω is $(0 : 0 : 1) - 3(0 : 1 : 0)$.

The above computation for the divisor $\omega = ds$ depended on our choice of local coordinate r. We now want to show that the calculation of ω is actually independent of which local coordinate we choose. Suppose we have a curve $\mathrm{V}(P)$. Let r_1 and r_2 be two different local coordinates.

picutre

Thinking of r_2 as the actual local coordinate, we can write r_1 as a function of r_2, meaning that there is a function g such that

$$r_1 = g(r_2).$$

But thinking of r_1 as the actual local coordinate, we can in turn find a function h such that

$$r_2 = h(r_1).$$

Then we have

$$r_1 = g(h(r_1)),$$

which means, from calculus, that

$$\frac{dg}{dr_2} = \frac{dr_1}{dr_2} \neq 0.$$

EXERCISE 3.5.92. Show that this definition of divisor $\omega = ds$ does not depend on our choice of local coordinates at p. (Key will be the use of the chain rule.)

Since the order of the divisor of a differential form is well-defined, we can make the following definition.

DEFINITION 3.5.6. The canonical divisor class $K_{\mathcal{C}}$ on a curve $\mathcal{C}$ is the divisor associated to any differential form ω on $\mathcal{C}$.

Of course we also need to check that the linear equivalence class of the divisor $K_{\mathcal{C}}$ does not depend on our choice of differential form.

EXERCISE 3.5.93. Assume $\mathcal{C}$ is a non-singular curve.

(1) Let $f, g \in \mathcal{K}(\mathcal{C})$. Show that $\mathrm{div}(f dg) \equiv \mathrm{div}(dg)$.
(2) Let ω_1, ω_2 be two differential forms on $\mathcal{C}$. Show that

$$\mathrm{div}(\omega_1) \equiv \mathrm{div}(\omega_2).$$

(In an earlier section we showed that the vector space of differential forms, over the field of rational functions, is one-dimensional.)

EXERCISE 3.5.94. To compute the canonical divisor of the projective line $\mathbb{P}^1$, write $(x : y)$ for coordinates of $\mathbb{P}^1$, with affine charts $u = \frac{x}{y}$ and $v = \frac{y}{x}$.

(1) Show that the divisor of du is equal to $-2(1:0)$.
(2) Show that the divisor of dv is equal to $-2(0:1)$.
(3) Prove that the divisors of the two differential forms du and dv are linearly equivalent.

EXERCISE 3.5.95. Let $\mathcal{C} = \mathrm{V}(x^2 - yz)$. We have already seen that

$$(ds) = (0:0:1) - 3(0:1:0).$$

The goal of this exercise is to show that

$$(dr) \equiv (ds).$$

(1) Compute the divisor of the differential form dr.
(2) Prove that the divisors of the two differential forms dr and ds are linearly equivalent and of degree -2.

EXERCISE 3.5.96. Let $\mathcal{C}$ be the curve defined by $P(x, y, z) = x^2 + y^2 - z^2 = 0$. We will compute the divisor of the differential form dr.

(1) For points $p = (a : b : c) \in \mathcal{C}$ with $c = 0$, show that $w = \frac{z}{x}$ is a local coordinate. Use that $r = \frac{1}{w}$ to write dr as $h(w)dw$. Show that there are two points on $\mathcal{C}$ with $w = 0$ and that $h(w)$ has a pole of order two at each.
(2) For points $p = (a : b : c) \in \mathcal{C}$ with $c \neq 0$ and $\frac{\partial P}{\partial y} \neq 0$, show that r is a local coordinate. Conclude that the divisor of dr has no zeros or poles when $z \neq 0, \frac{\partial P}{\partial y} \neq 0$.
(3) For points $p = (a : b : c) \in \mathcal{C}$ with $c \neq 0$ and $\frac{\partial P}{\partial y} = 0$, show that $\frac{\partial P}{\partial x} \neq 0$ and therefore $a \neq 0$. By the Implicit Function Theorem $s = \frac{y}{z}$ is a local coordinate at these points. Use $r^2 + s^2 = 1$ to write $dr = h(s)ds$ and show that $h(s)$ has zeros of multiplicity one at each of these points.
(4) Conclude that $div(\omega)$ is a divisor of degree -2.

In the previous exercises we found that the divisor of a differential form on a curve of genus 0 has degree -2. For a general smooth curve we have the following relation between genus and degree of $K_{\mathcal{C}}$.

THEOREM 3.5.97. *The degree of a canonical divisor on a non-singular curve $\mathcal{C}$ of genus g is $2g - 2$.*

We outline a proof of this theorem in the following exercises.

EXERCISE 3.5.98. Let $\mathcal{C}$ be a non-singular curve defined by a homogeneous polynomial $P(x, y, z)$ of degree n.

(1) Show that by changing coordinates if necessary we may assume $(1 : 0 : 0) \notin \mathcal{C}$.
(2) Show that the curve $\mathcal{C}$ is covered by two copies of $\mathbb{C}^2$, $\{(a : b : c) : c \neq 0\}$ and $\{(a : b : c) : b \neq 0\}$. Conclude that at every point of C we may use either the coordinates (r, s), where $r = \frac{x}{z}, s = \frac{y}{z}$, or (t, u), where $t = \frac{x}{y}, u = \frac{z}{y}$.

(3) Let $P_1(r,s) = P(r,s,1)$ and $P_2(t,u) = P(t,1,u)$ be the de-homogenized polynomials defining C in the two coordinate systems. Prove that

$$\begin{aligned} \frac{\partial P_1}{\partial r} &= \frac{\partial P}{\partial x}(r,s,1) \\ \frac{\partial P_1}{\partial s} &= \frac{\partial P}{\partial y}(r,s,1) \\ \frac{\partial P_2}{\partial t} &= \frac{\partial P}{\partial x}(t,1,u) \\ \frac{\partial P_2}{\partial u} &= \frac{\partial P}{\partial z}(t,1,u). \end{aligned}$$

(4) Explain why $(1:0:0) \notin \mathcal{C}$ implies that $\frac{\partial P_1}{\partial r}$ has degree $n-1$.

(5) Show that by changing coordinates if necessary we may assume if $p = (a : b : c) \in \mathcal{C}$ with $\frac{\partial P}{\partial x}(a,b,c) = 0$, then $c \neq 0$.

We will find the degree of $K_{\mathcal{C}}$ by computing the divisor of the differential one-form $\omega = ds$, where $s = \frac{y}{z}$. By the previous exercise we may assume $(1:0:0) \notin \mathcal{C}$ and if $p = (a:b:c) \in \mathcal{C}$ with $\frac{\partial P}{\partial x}(a,b,c) = 0$, then $c \neq 0$.

Exercise 3.5.99. First consider points $(a:b:c)$ on the curve with $c \neq 0$ and $\frac{\partial P}{\partial x} \neq 0$. Show that s is a local coordinate and ω has no zeros or poles at these points.

Exercise 3.5.100. Next we determine $\text{div}(\omega)$ at points $(a:b:c)$ with $c \neq 0$ and $\frac{\partial P}{\partial x} = 0$.

(1) Show that we must have $\frac{\partial P}{\partial y} \neq 0$ at these points, and that r is a local coordinate.

(2) Use $P(r,s,1) = 0$ to write $\omega = ds$ in the form $f(r)dr$.

(3) Compute the degree of $\text{div}(\omega)$ at these points by determining the order of the zeros or poles of $f(r)$.

Exercise 3.5.101. Now we determine $\text{div}(\omega)$ at points $(a:b:c)$ with $c = 0$. By our choice of coordinates, we are assuming that $(a:b:c) \in \text{V}(P)$ with $c = 0$ can only happen if $\frac{\partial P}{\partial x} \neq 0$.

(1) Show that u is a local coordinate.

(2) Write $\omega = ds$ in the form $g(u)du$.

(3) Compute the degree of $\text{div}(\omega)$ at these points by determining the order of the zeros or poles of $g(u)$.

(4) Conclude that $\text{div}(\omega)$ has degree $n(n-1) - 2n = n(n-3)$. Use exercise 3.3.4 to show that this is equal to $2g-2$, where g is the genus of $\mathcal{C}$.

Exercise 3.5.102. Let $\mathcal{C} = V(xy + xz + yz)$.

(1) Find a change of coordinates to transform $\mathcal{C}$ to an equivalent curve $\mathcal{C}'$ such that $(1:0:0) \notin \mathcal{C}'$ and such that if $p = (a:b:c) \in \mathcal{C}$ with $c = 0$, then $\frac{\partial P}{\partial x}(a, b, c) \neq 0$.
(2) Compute the canonical divisor class of $\mathcal{C}'$ by computing the divisor of $\omega = ds$.

3.5.11. The space $L(K - D)$. We will now see the important role that the canonical divisor plays in the Riemann-Roch Theorem. We proved previously Riemann's Theorem,

$$l(D) \geq \deg D - g + 1$$

for any divisor D on a smooth curve $\mathcal{C}$ of genus g. We now improve this result by determining the value of $l(D) - (\deg D - g + 1)$. We will show that for all D on $\mathcal{C}$, this difference is equal to the dimension of the space $L(K_{\mathcal{C}} - D)$.

We have seen for any point $p \in \mathcal{C}$, $l(D) \leq l(D+p) \leq l(D) + 1$, that is $L(D)$ is either equal to $L(D+p)$ or a subspace of codimension one. Applying this to the divisor $K-D$, we have either $l(K-D) = l(K-D-p)$ or $L(K-D) = l(K-D-p)+1$.

For our next result we need an important consequence of the Residue Theorem: there is no differential form on $\mathcal{C}$ with a simple (order one) pole at one point and no other poles.

Exercise 3.5.103. We will show if $L(D) \subsetneq L(D+p)$ then $L(K-D-p) = L(K-D)$.

(1) Assume $L(D) \subsetneq L(D+p)$ and $L(K-D-p) \subsetneq L(K-D)$. Show that this implies the existence of functions $f, g \in \mathcal{K}(\mathcal{C})$ with $\mathrm{div}(f) + D + p \geq 0$ and $\mathrm{div}(g) + K - D \geq 0$, such that these relations are equalities at p.
(2) Let ω be a differential form on $\mathcal{C}$ so that $\mathrm{div}(\omega) \equiv K_{\mathcal{C}}$. Show that $\mathrm{div}(fg\omega) + p \geq 0$ and thus the form $fg\omega$ has a simple pole at p.
(3) Explain why this contradicts the Residue Theorem (see appendix).
(4) Show that this result is equivalent to the inequality $l(D+p) - l(D) + l(K-D) - l(K-D-p) \leq 1$.

Exercise 3.5.104. Let $q_1, \ldots, q_k$ be points on the curve $\mathcal{C}$. Use the previous exercise and induction to show

$$l(D + \sum_1^k q_i) - l(D) + l(K-D) - l(K - D - \sum_1^k q_i) \leq k.$$

The next problem has nothing to do with the previous one, but does use critically that $l(D) = 0$ if D has negative degree. It will be the last step that we need before proving Riemann-Roch in the next section.

Exercise 3.5.105. Prove there exists a positive integer n such that $l(K_{\mathcal{C}} - nH) = 0$, where H is a hyperplane divisor.

3.5.12. Riemann-Roch Theorem. We have previously shown Riemann's Theorem: for a divisor D on a smooth plane curve $\mathcal{C}$ of genus g, $l(D) \geq \deg D - g + 1$. This result provides a bound for the dimension of the space of functions on $\mathcal{C}$ with poles bounded by the divisor D. A remarkable fact is that we can explicitly calculate the error term in this inequality; that is, we can improve this result in the Riemann Roch Theorem:

THEOREM 3.5.106. If D is a divisor on a smooth plane curve $\mathcal{C}$ of genus g and $K_{\mathcal{C}}$ is the canonical divisor of $\mathcal{C}$, then

$$l(D) - l(K_{\mathcal{C}} - D) = \deg D - g + 1.$$

This theorem allows us to explictly calculate the dimensions of spaces of functions on our curve $\mathcal{C}$ in terms of the genus of $\mathcal{C}$ and the degree of the bounding divisor D. As before we will prove this for smooth curves in the plane, but in fact the result also holds for singular curves. The Riemann-Roch Theorem can also be generalized to higher dimensional varieties. In the next several exercises we complete the proof.

EXERCISE 3.5.107. Let n be a positive integer with $l(K_{\mathcal{C}} - nH) = 0$; use Exercise 3.5.63 to show there exists $m > n$ and $q_1, \ldots, q_k \in \mathcal{C}$ with $D + \sum_1^k q_i \equiv mH$. Show that the degree of D is $m \deg \mathcal{C} - k$.

EXERCISE 3.5.108. Using the notation of the previous Exercise and Exercise 3.5.97, show that

$$l(mH) - l(D) + l(K_{\mathcal{C}} - D) \leq k.$$

EXERCISE 3.5.109. Using the notation of the previous Exercise and that

$$\deg(mH) = m \deg(\mathcal{C}) - g + 1$$

(Exercise 3.5.50), show that

$$l(D) - l(K_{\mathcal{C}} - D) \geq \deg D - g + 1.$$

EXERCISE 3.5.110. Show that

$$\deg(D) - g + 1 \geq l(D) - l(K_{\mathcal{C}} - D).$$

(Hint: think of $K_{\mathcal{C}} - D$ as a divisor.)

EXERCISE 3.5.111. Prove the Riemann-Roch Theorem: show that

$$l(D) - l(K_{\mathcal{C}} - D) = \deg D - g + 1.$$

EXERCISE 3.5.112. Use the Riemann Roch Theorem to prove for a divisor D with $\deg D > 0$ on an elliptic curve, $l(D) = \deg D$.

EXERCISE 3.5.113. For a smooth curve $\mathcal{C}$ prove that the genus g is equal to the dimension of the vector space $L(K_{\mathcal{C}})$.

EXERCISE 3.5.114. Suppose D is a divisor of degree $2g-2$ with $l(D) = g$. Prove that D is linearly equivalent to the canonical divisor.

3.5.13. Associativity of the Group Law for a Cubic. As an application of Riemann-Roch, we will finally provide a proof of associativity for the group law on a cubic curve. Starting with a smooth cubic curve $\mathcal{C}$, we must show, given any three points $P, Q, R \in \mathcal{C}$, that

$$(P+Q)+R = P+(Q+R).$$

Most of the following exercises will depend on the material in chapter two. We start, though, with how we will use the Riemann-Roch theorem.

EXERCISE 3.5.115. Let T be a point on the smooth cubic curve $\mathcal{C}$. Show that $L(T)$ is one-dimensional and conclude that the only rational functions in $L(T)$ are constant functions.

EXERCISE 3.5.116. Let S and T be two points on the smooth cubic curve $\mathcal{C}$. Suppose there is a rational function f such that

$$(f)+T = S.$$

Show that $S = T$.

Let

$$S = (P+Q)+R, \quad T = P+(Q+R).$$

Here the ' + " refers to the cubic addition, not the divisor addition. Our goal is to show that $S = T$.

Let

$$A = P+Q, \quad B = Q+R.$$

Again, the addition is the cubic law addition. Let $\mathcal{O}$ denote the identity element of the smooth cubic curve $\mathcal{C}$.

EXERCISE 3.5.117. Find a linear function $l_1(x,y,z)$ such that

$$(l_1 = 0) \cap \mathcal{C} = \{P, Q, -A\}.$$

Here $-A$ refers to the inverse of A with respect to the group law of the cubic.

EXERCISE 3.5.118. Find a linear function $l_2(x,y,z)$ such that

$$(l_2 = 0) \cap \mathcal{C} = \{A, \mathcal{O}, -A\}.$$

Exercise 3.5.119. Find a rational function ϕ such that

$$(\phi) = P + Q - A - \mathcal{O}.$$

Here the addition is the addition for divisors.

Exercise 3.5.120. Find a linear function $l_3(x, y, z)$ such that

$$(l_3 = 0) \cap \mathcal{C} = \{A, R, -S\}.$$

Here $-S$ refers to the inverse of S with respect to the group law of the cubic.

Exercise 3.5.121. Find a linear function $l_4(x, y, z)$ such that

$$(l_4 = 0) \cap \mathcal{C} = \{S, \mathcal{O}, -S\}.$$

Exercise 3.5.122. Find a rational function ψ such that

$$(\psi) = A + R - S - \mathcal{O}.$$

Here the addition is the addition for divisors.

Exercise 3.5.123. Show that

$$(\psi\phi) = P + Q + R - S - 2\mathcal{O}.$$

Here the addition is the addition for divisors.

Exercise 3.5.124. Following the outline of the last six exercise, find a rational function μ so that

$$(\mu) = P + Q + R - T - 2\mathcal{O}.$$

Here the addition is the addition for divisors.

Exercise 3.5.125. Show that $\frac{\mu}{\psi\phi}$ is a rational function such that

$$\left(\frac{\mu}{\psi\phi}\right) + T = S.$$

Exercise 3.5.126. Put these exercises together to prove that the group law for cubics is associative.

Exercise 3.5.127. Show that $(0, 0)$ is a singular point of $\mathrm{V}(x^2 - y^2)$ in $\mathbb{C}^2$. Sketch the curve $\mathrm{V}(x^2 - y^2)$ in $\mathbb{R}^2$, to see that at the origin there is no well-defined tangent.

Exercise 3.5.128. Show that $(0 : 0 : 1)$ is a singular point on $\mathrm{V}(zy^2 - x^3)$ in $\mathbb{P}^2$. (This curve is called the *cuspidal cubic*. See also Exercise **??**.)

Exercise 3.5.129. Show that $\mathrm{V}(y^2z - x^3 + x^2z)$ in $\mathbb{P}^2$ is singular at $(0 : 0 : 1)$. (This curve is called the *nodal cubic*. See also Exercise **??**.)

EXERCISE 3.5.130. Let V be $\mathrm{V}(x^4 + y^4 - 1)$ in $\mathbb{C}^2$.

(1) Is V singular?
(2) Homogenize V. Is the corresponding curve in $\mathbb{P}^2$ singular?

EXERCISE 3.5.131. Let V be $\mathrm{V}(y - x^3)$ in $\mathbb{C}^2$.

(1) Is V singular?
(2) Homogenize V. Is the corresponding curve in $\mathbb{P}^2$ singular? If so, find an affine chart of $\mathbb{P}^2$ containing one of its singularities, and dehomogenize the curve in that chart.

EXERCISE 3.5.132. Show that $V((x + 3y)(x - 3y + z))$ has a singularity.

EXERCISE 3.5.133. Let V be $\mathrm{V}(y^2 z - x^3 + 3xz^2)$ in $\mathbb{P}^2$. Is V singular?

3.6. Blowing up

We begin this section by describing the blow-up of the plane $\mathbb{C}^2$ at the origin. Let

$$\pi : \mathbb{C}^2 \times \mathbb{P}^1 \longrightarrow \mathbb{C}^2$$

be the projection

$$((x, y), (u : v)) \mapsto (x, y).$$

Let

$$\tilde{Y} = \{((x, y), (x : y)) \ : \text{ at least one of } x \text{ or } y \text{ is nonzero}\} \subset \mathbb{C}^2 \times \mathbb{P}^1.$$

Set

$$Y = \tilde{Y} \cup \pi^{-1}((0, 0)).$$

EXERCISE 3.6.1. Verify that $\pi^{-1}((0, 0))$ can be identified with $\mathbb{P}^1$. Show that the restriction of π to $\tilde{Y}$ is a bijection between $\tilde{Y}$ and $\mathbb{C}^2 - (0, 0)$. (Neither of these are deep.)

The set Y, along with the projection $\pi : Y \longrightarrow \mathbb{C}^2$, is called the *blow-up* of $\mathbb{C}^2$ at the point $(0, 0)$. (For the rest of this section, the map π will refer to the restriction projection $\pi : Y \longrightarrow \mathbb{C}^2$.)

We look at the blow up a bit more carefully. We can describe $\tilde{Y}$ as

$$\begin{aligned} \tilde{Y} &= \{((x, y), (x : y)) \ : \text{ at least one of } x \text{ or } y \text{ is nonzero}\} \subset \mathbb{C}^2 \times \mathbb{P}^1 \\ &= \{(x, y) \times (u : v) \in \mathbb{C}^2 \times \mathbb{P}^1 : xv = yu, (x, y) \neq (0, 0)\} \end{aligned}$$

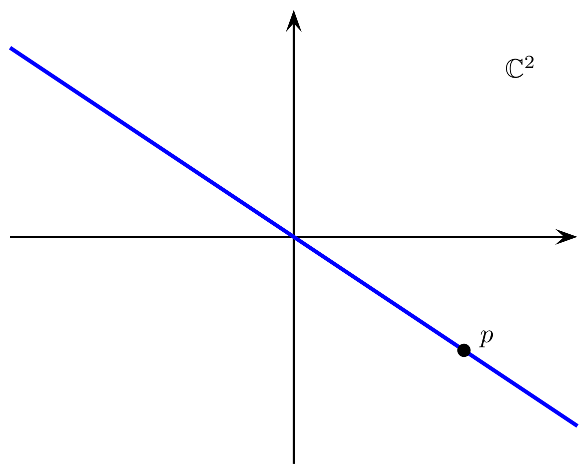
Then Y is simply

$$Y = \{(x, y) \times (u : v) \in \mathbb{C}^2 \times \mathbb{P}^1 : xv = yu\}.$$

Recall that the projective line $\mathbb{P}^1$ can be thought of as all lines in $\mathbb{C}^2$ containing the origin. Thus Y is the following set:

$$\{(\text{points } p \text{ in } \mathbb{C}^2) \times (\text{lines } l \text{ through } (0,0)) : p \in l\}.$$

The above exercise is simply a restatement that through every point p in $\mathbb{C}^2 - (0,0)$ there is a unique line through that point and the origin.

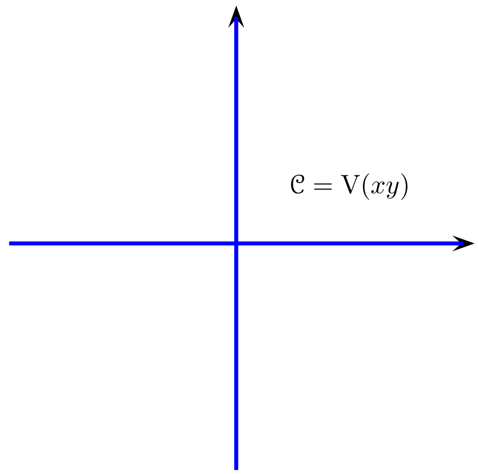


More generally, if $\mathcal{C}$ is a curve in $\mathbb{C}^2$ that passes through the origin, then the there is a bijection between $\mathcal{C} - (0,0)$ and the set $\pi^{-1}(\mathcal{C} - (0,0))$ in Y. The blow-up of $\mathcal{C}$ at the origin, denoted $Bl_{(0,0)}\mathcal{C}$, is the closure of $\pi^{-1}(\mathcal{C}\ (0,0))$ in Y, in a sense that will be made precise in Chapter 4, along with the restricted projection map:

$$Bl_{(0,0)}\mathcal{C} = \text{Closure of } \pi^{-1}(\mathcal{C}\ (0,0)).$$

Intuitively, $\pi^{-1}(\mathcal{C}\ (0,0))$ resembles a punctured copy of $\mathcal{C}$ in $\mathbb{C}^2 \times \mathbb{P}^1$, and there is an obvious way to complete this punctured curve. If the origin is a smooth point of $\mathcal{C}$, then the blow-up at the origin is simply a copy of $\mathcal{C}$. If the origin is a singular point, then the blow-up contains information about how the tangents to $\mathcal{C}$ behave near the origin.

We want to look carefully at an example. Consider $\mathcal{C} = \mathrm{V}(xy)$ in $\mathbb{C}^2$. Here we are interested in the zero locus of $xy = 0$,



or, in other words, the x-axis (when $y = 0$) union the y-axis (when $y = 0$). We will show in two ways that the blow up of $\mathcal{C}$ has two points over the origin $(0,0)$: $(0,0) \times (0:1)$ and $(0,0) \times (1:0)$, which correspond to the x-axis and the y-axis.

Let $P(x,y) = xy$. We know that π is a bijection away from the origin. We have that

$$\pi^{-1}(\mathcal{C} - (0,0)) = \{(x,y) \times (x:y) : xy = 0, (x,y) \neq (0,0)\}.$$

We know that

$$\mathcal{C} = \mathrm{V}(xy) = \mathrm{V}(x) \cup \mathrm{V}(y).$$

We will show that there is one point over the origin of the blow-up of $\mathrm{V}(x)$ and one point (a different point) over the origin of the blow-up of $\mathrm{V}(xy)$.

We have

$$\begin{aligned} \pi^{-1}(\mathrm{V}(x) - (0,0)) &= \{(x,y) \times (0:y) : 0 = x, (x,y) \neq (0,0)\} \\ &= \{(0,y) \times (0:y) : y \neq 0\} \\ &= \{(0,y) \times (0:1) : y \neq 0\} \end{aligned}$$

Then as $y \to 0$, we have

$$(0,y) \times (0:1) \to (0,0) \times (0:1),$$

a single point as desired, corresponding to the y-axis.

Similarly, we have

$$\begin{aligned} \pi^{-1}(\mathrm{V}(y) - (0,0)) &= \{(x,y) \times (x:0) : y = 0, (x,y) \neq (0,0)\} \\ &= \{(x,0) \times (x:0) : x \neq 0\} \\ &= \{(x,0) \times (1:0) : x \neq 0\} \end{aligned}$$

Then as $x \to 0$, we have

$$(x, 0) \times (1 : 0) \to (0, 0) \times (1 : 0),$$

a single, different point, again as desired, corresponding to the x- axis.

Now for a slightly different way of thinking of the blow-up. The projective line can be covered by two copies of C, namely by $(u : 1)$ and $(1 : v)$. For any point $(u : v) \in \mathbb{P}^1$, at least one of u or v cannot be zero. If $u \neq 0$, then we have

$$(u : v) = (1 : v/u)$$

while if $v \neq 0$, we have

$$(u : v) = (u/v : 1).$$

In either case, we can assume that $u = 1$ or that $v = 1$.

Start with $u = 1$. We can identify $(x, y) \times (1 : v)$ with $\mathbb{C}^3$, having coordinates x, y, v. Then the blow-up of $\mathrm{V}(xy)$ will be the closure of

$$\begin{aligned} xy &= 0 \\ y &= xv \\ (x, y) &= (0, 0). \end{aligned}$$

Plugging xv for y into the top equation, we have

$$x^2 v = 0.$$

Since $x \neq 0$, we can divide through by x to get

$$v = 0.$$

Then we have as our curve $(x, xv) \times (1 : 0) = (x, 0) \times (1 : 0)$. Then as $x \to 0$, we have

$$(x, 0) \times (1 : 0) \to (0, 0) \times (1 : 0),$$

Now let $v = 1$. We can identify $(x, y) \times (u : 1)$ with $\mathbb{C}^3$, having coordinates x, y, u. Then the blow-up of $\mathrm{V}(xy)$ will be the closure of

$$\begin{aligned} xy &= 0 \\ yu &= x \\ (x, y) &= (0, 0). \end{aligned}$$

Plugging yu for x into the top equation, we have

$$y^2 u = 0.$$

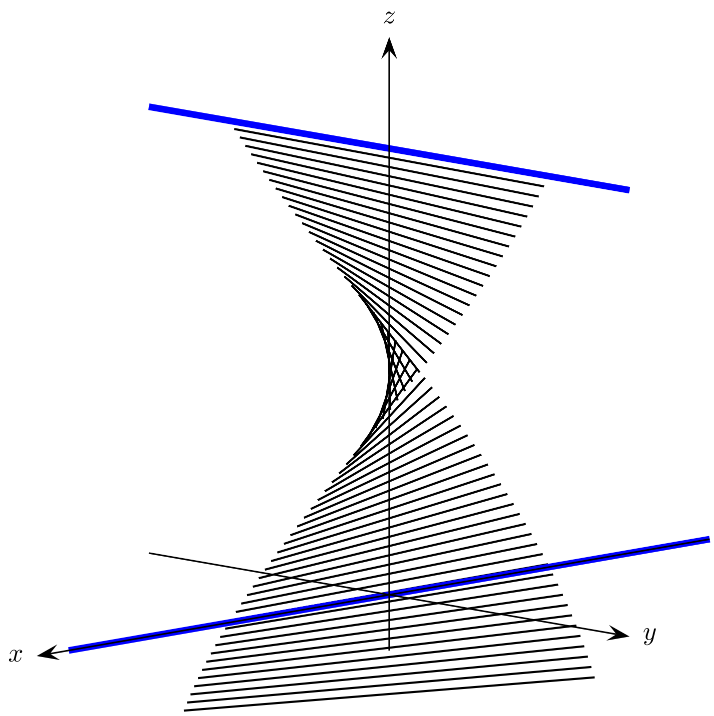
Since $y \neq 0$, we can divide through by y to get

$$u = 0.$$

Then we have as our curve $(yu, y) \times (0:1) = (0, y) \times (0:1)$. Then as $y \to 0$, we have

$$(0, y) \times (0:1) \to (0,0) \times (0:1),$$

In either case, the blow-up looks like



Each of these techniques will be needed for various of the following problems.

Exercise 3.6.2. Let $\mathcal{C} = \mathrm{V}(y - x^2)$ in $\mathbb{C}^2$. Show that this curve is smooth. Sketch this curve in $\mathbb{C}^2$. Sketch a picture of $Bl_{(0,0)}\mathcal{C}$. Show that the blow-up projects bijectively to $\mathcal{C}$.

Exercise 3.6.3. Let $\mathcal{C} = \mathrm{V}(x^2 - y^2)$ in $\mathbb{C}^2$. Show that this curve has a singular point at the origin. Sketch this curve in $\mathbb{C}^2$. Blow up $\mathcal{C}$ at the origin, showing that there are two points over the origin, and then sketch a picture of the blow up.

Exercise 3.6.4. Let $\mathcal{C} = \mathrm{V}(y^2 - x^3 + x^2)$. Show that this curve has a singular point at the origin. Sketch this curve in $\mathbb{C}^2$. Blow up $\mathcal{C}$ at the origin, and sketch a picture of the blow up. Show that there are two points over the origin.

Exercise 3.6.5. Let $\mathcal{C} = \mathrm{V}(y^2 - x^3)$. Show that this curve has a singular point at the origin. Sketch this curve in $\mathbb{C}^2$. Blow up $\mathcal{C}$ at the origin, and sketch a picture of the blow up. Show that there is only one point over the origin.

EXERCISE 3.6.6. Let $\mathcal{C} = \mathrm{V}((x-y)(x+y)(x+2y))$ be a curve in $\mathbb{C}^2$. Show that this curve has a singular point at the origin. Sketch this curve in $\mathbb{C}^2$. Blow up $\mathcal{C}$ at the origin, and sketch a picture of the blow up. Show that there are three points over the origin.

The previous exercises should convey the idea that if the original curve is singular at the origin, then the blow-up seems to be less singular at its point over the origin. We currently can't express precisely what this means, since our definition of singularity applies only to curves in the plane, and the blow-up does not lie in a plane. Algebraic ideas developed in Chapter 4 will allow us to make this idea precise.

Of course, there is nothing special about the origin in affine space, and we could just as easily blow up curves at any other point. Also, the definition of blowing up can easily be extended to curves in projective spaces. Blowing up will be discussed in full generality in Chapter 4, once we have the necessary algebraic tools.

CHAPTER 4

Affine Varieties

The goal of this chapter is to start using more algebraic concepts to describe the geometry of curves and surfaces in a fairly concrete setting. We will translate the geometric features into the language of ring theory, which can then be extended to encompass curves and surfaces defined over objects besides the real numbers or the complex numbers. You will need to know some basic facts about rings, including ideals, prime ideals, maximal ideals, sub-rings, quotient rings, ring homomorphisms, ring isomorphisms, integral domains, fields, and local rings. Most undergraduate abstract algebra texts include this material, and can be used as a reference. In addition, some concepts from topology and multivariable calculus are needed. We have tried to include just enough of these topics to be able to work the problems.

By considering the set of points where a polynomial vanishes, we can see there is a correspondence between the algebraic concept of a polynomial and the geometric concept of points in the space. This chapter is devoted to understanding that connection. Here tools from abstract algebra, especially commutative ring theory, will be become key.

Definition 4.0.1. For a field k, the *affine n-space over k* is the set

$$\mathbb{A}^n(k) = \{(a_1, a_2, \dots, a_n) : a_i \in k \quad \text{for} \quad i = 1, \dots, n\}.$$

We write simply $\mathbb{A}^n$ when the field k is understood.

For example, $\mathbb{A}^2(\mathbb{R})$ is the familiar Euclidean space $\mathbb{R}^2$ from calculus, and $\mathbb{A}^1(\mathbb{C})$ is the complex line. We are interested in subsets of $\mathbb{A}^n$ that are the zero sets of a collection of polynomials over k.

4.1. Zero Sets of Polynomials

Recall that $k[x_1, x_2, \dots, x_n]$ is the commutative ring of all polynomials in the variables $x_1, x_2, \dots, x_n$ with coefficients in the field k. Frequently for us, our field will be the complex numbers $\mathbb{C}$, with the field of the real numbers $\mathbb{R}$ being our second most common field.

4.1.1. Over $\mathbb{C}$.

EXERCISE 4.1.1. Describe or sketch the zero set of each polynomial over $\mathbb{C}$.

(1) $\{x^2 + 1\}$
(2) $\{y - x^2\}$

EXERCISE 4.1.2. (1) Show that the zero set of $x^2 + y^2 - 1$ in $\mathbb{C}^2$ is unbounded. Contrast with the zero set of $x^2 + y^2 - 1$ in $\mathbb{R}^2$.
(2) Show that the zero set of any nonconstant polynomial in two variables over $\mathbb{C}$ is unbounded.

EXERCISE 4.1.3. Find a set of polynomials $\{P_1, \dots, P_n\}$, all of whose coefficients are real numbers, whose common zero set is the given set.

(1) $\{(3, y) : y \in \mathbb{R}\}$ in $\mathbb{R}^2$
(2) $\{(1, 2)\}$ in $\mathbb{R}^2$
(3) $\{(1, 2), (0, 5)\}$ in $\mathbb{R}^2$
(4) Generalize the method from part iii. to any finite set of points $\{a_1, \dots, a_n\}$ in $\mathbb{R}^2$.

EXERCISE 4.1.4. Find a set of polynomials $\{P_1, \dots, P_n\}$, all of whose coefficients are complex numbers, whose common zero set is the given set.

(1) $\{(3 + 2i, -i)\}$ in $\mathbb{C}^2$
(2) $\{(3 + 2i, -i), (0, 1 - 4i)\}$ in $\mathbb{C}^2$
(3) Generalize the method from part ii. to any finite set of points $\{b_1, \dots, b_n\}$ in $\mathbb{C}^2$.

EXERCISE 4.1.5. (1) Is any finite subset of $\mathbb{C}^2$ the zero set of a polynomial $\mathbb{C}[x, y]$? Prove or find a counterexample.
(2) Is there an infinite subset of $\mathbb{C}^2$ that is the common zero set of a finite collection of polynomials in $\mathbb{C}[x, y]$?
(3) Find an infinite set of points in $\mathbb{C}$ that is not the common zero set of a finite collection of polynomials in $\mathbb{C}[x]$?
(4) Is there any infinite set of points in $\mathbb{C}$, besides $\mathbb{C}$ itself, that is the common zero set of a finite collection of polynomials in $\mathbb{C}[x]$?

4.1.2. Over $\mathbb{Z}_5$. One of the great advantages of algebraic geometry is that we may consider polynomials over any field. Our fields do not even need to be infinite! We can define $\mathbb{Z}_5$ using an equivalence relation; $a \equiv b$ if and only if $a - b$ is a multiple of 5. There are 5 elements in this field, we can call them 0, 1, 2, 3, and 4. Addition and multiplication is defined by the usual operation followed by equating the result with its representative from this set.

EXERCISE 4.1.6. Find the zero set of each polynomial in $\mathbb{Z}_5$.

(1) $x^2 + 1$
(2) $x^2 - 2$

EXERCISE 4.1.7. Sketch the zero set of each polynomial in $\mathbb{A}^2(\mathbb{Z}_5)$.

(1) $y - x^2$
(2) $y^2 - 2xy + x^2$
(3) $xy - 3y - x^2 + 3x$

4.1.3. Over Any Field k. Much of the reason that modern algebraic geometry heavily influences not just geometry but also number theory is that we can allow our coefficients to be in any field, even those for which no geometry is immediately apparent.

EXERCISE 4.1.8. (1) Show that if k is an infinite field, and $P \in k[x_1, \ldots, x_n]$ is a polynomial whose zero set is $\mathbb{A}^n(k)$, then $P = 0$. Hint: Use induction on n.
(2) Is there any finite field for which this result holds?

4.2. Algebraic Sets

The zero sets of polynomials in affine space are called algebraic sets.

DEFINITION 4.2.1. Let $S \subseteq k[x_1, \ldots, x_n]$ be a set of polynomials over k. The *algebraic set* defined by S is

$$V(S) = \{(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n(k) : P(a_1, a_2, \ldots, a_n) = 0 \quad \text{for} \quad \text{all} \quad P \in S\}.$$

EXERCISE 4.2.1. Sketch the algebraic sets.

(1) $V(x^3 + 1)$ in $\mathbb{A}^1(\mathbb{C})$
(2) $V((y - x^2)(y^2 - x))$ in $\mathbb{A}^2(\mathbb{R})$
(3) $V(y - x^2, y^2 - x)$ in $\mathbb{A}^2(\mathbb{R})$
(4) $V(y^2 - x^3 + x)$ in $\mathbb{A}^2(\mathbb{R})$
(5) $V(x - 2y + 3z)$ in $\mathbb{A}^3(\mathbb{R})$
(6) $V(z - 3, z - x^2 - y^2)$ in $\mathbb{A}^3(\mathbb{R})$
(7) $V(xy - z^2y) = V(y(x - z^2))$ in $\mathbb{A}^3(\mathbb{R})$
(8) $V(y - x + x^2)$ in $\mathbb{A}^2(\mathbb{Z}_3)$

EXERCISE 4.2.2. Algebraic Sets in $\mathbb{R}^n$ and $\mathbb{C}^n$:

(1) Show that for any $a \in \mathbb{R}$, the singleton $\{a\}$ is an algebraic set.
(2) Show that any finite collection of numbers $\{a_1, a_2, \ldots, a_k\}$ in $\mathbb{R}$ is an algebraic set.
(3) Show that a circle in $\mathbb{R}^2$ is an algebraic set.
(4) Show that the set $\{(-1/\sqrt{2}, 1/\sqrt{2}), (1/\sqrt{2}, -1/\sqrt{2})\} \subset \mathbb{R}^2$ is an algebraic set.

(5) Show that any line in $\mathbb{R}^3$ is an algebraic set.

(6) Give an example of a subset of $\mathbb{C}^2$ that is not an algebraic set.

(7) Give an example of a nonconstant polynomial P in $\mathbb{R}[x, y]$ such that the algebraic set $X = \{(x, y) \in \mathbb{R}^2 | P(x, y) = 0\}$ is the empty set.

(8) Is there a nonconstant polynomial P in $\mathbb{C}[x, y]$ such that the algebraic set $X = \{(x, y) \in \mathbb{C}^2 | P(x, y) = 0\}$ is the empty set? Explain why or why not.

(9) Suppose $X_1 = \{(x, y) \in \mathbb{C}^2 | x + y = 0\}$ and $X_1 = \{(x, y) \in \mathbb{C}^2 | x - y = 0\}$. Find a polynomial $Q \in \mathbb{C}[x, y]$ such that $X_1 \cup X_2 = \{(x, y) \in \mathbb{C}^2 | Q(x, y) = 0\}$.

(10) Suppose $X_1 = \{(x_1, x_2, \ldots, x_n) \in \mathbb{C}^n | P_1(x_1, x_2, \ldots, x_n) = 0\}$ and $X_2 = \{(x_1, x_2, \ldots, x_n) \in \mathbb{C}^n | P_2(x_1, x_2, \ldots, x_n) = 0\}$. Give a single polynomial Q such that $X_1 \cup X_2 = \{(x_1, x_2, \ldots, x_n) \in \mathbb{C}^n | Q(x_1, x_2, \ldots, x_n) = 0\}$.

Exercise 4.2.3. (1) Is any finite subset of $\mathbb{A}^2(\mathbb{R})$ an algebraic set?

(2) Is any finite subset of $\mathbb{A}^2(\mathbb{C})$ an algebraic set?

Exercise 4.2.4. Show that the set $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) :: 0 \leq x \leq 1, y = 0\}$ is **not** an algebraic set. (Hint: any one-variable polynomial, that is not the zero polynomial, can only have a finite number of roots.)

Exercise 4.2.5. Show that the empty set and $\mathbb{A}^n(k)$ are algebraic sets in $\mathbb{A}^n(k)$.

Exercise 4.2.6. Show that if $X = V(f_1, \ldots, f_s)$ and $W = V(g_1, \ldots, g_t)$ are algebraic sets in $\mathbb{A}^n(k)$, then $X \cup W$ and $X \cap W$ are algebraic sets in $\mathbb{A}^n(k)$.

4.3. Zero Sets via $V(I)$

The goal of this section is to start to see how ideals in rings give us algebraic sets.

Exercise 4.3.1. Let $f(x, y), g(x, y) \in \mathbb{C}[x, y]$. Show that

$$V(f, g) = V(f - g, f + g).$$

Exercise 4.3.2. Show that $V(x+y, x-y, 2x+y^2, x+xy+y^3, y+x^2y) = V(x, y)$.

Thus the polynomials that define a zero set are far from being unique. But there is an algebraic object that comes close to be uniquely linked to a zero set.

The following exercise is key to algebraic geometry.

Exercise 4.3.3. Let I be the ideal in $k[x_1, \ldots, x_n]$ generated by a set $S \subset k[x_1, \ldots, x_n]$. Show that $V(S) = V(I)$. Thus every algebraic set is defined by an ideal.

While it is not quite true that the set $V(I)$ uniquely determines the ideal I, we will soon see how to restrict our class of ideas so that the associated ideal will be unique.

Exercise 4.3.4. For $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$, let I be the ideal generated by f and g and let J be the ideal generated by f alone.

(1) Show that $J \subset I$.
(2) Show that
$$V(I) \subset V(J).$$

Exercise 4.3.5. Show that if I and J are ideals in $k[x_1, \ldots, x_n]$ with $I \subset J$, then $V(I) \supset V(J)$.

Exercise 4.3.6. You may find exercise 4.2.6 useful here.

(1) Show that an arbitrary intersection of algebraic sets is an algebraic set.
(2) Show that a finite union of algebraic sets is an algebraic set.
(3) Use your answers to parts a. and b. and exercise 4.2.5 to conclude that the collection of complements of algebraic sets forms a topology on $\mathbb{A}^n(k)$.

4.3.1. Ideals Associated to Zero Sets. We have seen that the set of polynomials that define a zero set is not unique. We need to find a structure derived from these polynomials that is unique. At first glance, it looks like an ideal of the polynomial ring would do the job. As we will see, not all ideals will work, but a particular type of ideal is what we need.

Definition 4.3.1. Let V be a an algebraic set in $\mathbb{A}^n(k)$. The *ideal of* V is given by

$$I(V) = \{P \in k[x_1, \ldots, x_n] : P(a_1, \ldots, a_n) = 0 \quad \text{for} \quad \text{all} \quad (a_1, \ldots, a_n) \in V\}.$$

Similarly, for any set of points X in $\mathbb{A}^n(k)$, we define

$$I(X) = \{P \in k[x_1, \ldots, x_n] : P(a_1, \ldots, a_n) = 0 \quad \text{for} \quad \text{all} \quad (a_1, \ldots, a_n) \in X\}.$$

Exercise 4.3.7. Show that $I(V)$ is an ideal in the ring $k[x_1, \ldots, x_n]$.

Exercise 4.3.8. Let X be a set of points in $\mathbb{A}^n(k)$.

(1) Show that $X \subseteq V(I(X))$.
(2) Find a set X with $X \neq V(I(X))$.
(3) In part b., can you find a set X such that $I(X) \neq \langle 0 \rangle$?
(4) Show that if X is a non-empty algebraic set, then $X = V(I(X))$.

Exercise 4.3.9. Let I be an ideal in $k[x_1, \ldots, x_n]$.

(1) Show that $I \subseteq I(V(I))$.
(2) Find an ideal I with $I \neq I(V(I))$.
(3) In part ii., can you find an ideal I such that $V(I) \neq \emptyset$?
(4) Show that if I is the ideal given by an algebraic set, then $I = I(V(I))$.

It looks like there is a correspondence between algebraic sets and some ideals. Let's examine the properities of a good ideal a little more closely.

DEFINITION 4.3.2. Let I be an ideal in $k[x_1, \ldots, x_n]$. The *radical of I* is defined as

$$\mathrm{Rad}(I) = \{P \in k[x_1, \ldots, x_n] : P^m \in I \text{ for some } m > 0\}.$$

An ideal I is called a *radical ideal* if $I = \mathrm{Rad}(I)$.

EXERCISE 4.3.10. Let $f(x, y) = (x^2 - y + 3)^2 \in \mathbb{C}[x, y]$. Show that the ideal I generated by f is not radical. Find $\mathrm{Rad}(I)$.

EXERCISE 4.3.11. Let I be an ideal in $k[x_1, \ldots, x_n]$. Show that $\mathrm{Rad}(I)$ is an ideal.

Thus for any algebraic set X, there is the uniquely defined associated radical ideal.

EXERCISE 4.3.12. Let X be a set of points in $\mathbb{A}^n(k)$. Show that $I(X)$ is a radical ideal.

EXERCISE 4.3.13. Show that $\mathrm{Rad}(I) \subset I(V(I))$ for any ideal I in $k[x_1, \ldots, x_n]$.

EXERCISE 4.3.14. Let X and W be algebraic sets in $\mathbb{A}^n(k)$. Show that $X \subset W$ if and only if $I(X) \supset I(W)$. Conclude that $X = W$ if and only if $I(X) = I(W)$.

4.4. Functions on Zero Sets and the Coordinate Ring

One of the themes in 20th century mathematics is that it is not clear what is more important in geometry: the actual geometric point set or the space of functions defined on the geometric point set. So far in this chapter, we have been concentrating on the point set. We now turn to the functions on the point sets.

Let $V \subseteq \mathbb{A}^n(k)$ be an algebraic set. Then it is very natural to consider the set

$$\mathcal{O}(V) := \{f : V \to k \mid f \text{ is a polynomial function}\}.$$

EXERCISE 4.4.1. Show that if we equip $k[V]$ with pointwise addition and multiplication of functions, then $k[V]$ is a ring. We will call $k[V]$ the *coordinate ring* associated to V.

Given an algebraic set V, recall that by $I(V)$ we mean the vanishing ideal of V, i.e. the ideal in $k[x_1, \ldots, x_n]$ consisting of polynomial functions f that satisfy $f(V) = 0$ for all $\bar{x} \in V$.

EXERCISE 4.4.2. Let $f(x, y) = x^2 + y^2 - 1 \in \mathbb{C}[x, y]$. Consider the two polynomials $g(x, y) = y, h(x, y) = x^2 + y^2 + y - 1$.

(1) Find a point $(a, b) \in \mathbb{A}^2(\mathbb{C})$ such that
$$g(a, b) \neq h(a, b).$$
(2) Show for any point $(a, b) \in V(f)$ that
$$g(a, b) = h(a, b).$$

Thus g and h are different as functions on $\mathbb{A}^2(\mathbb{C})$ but should be viewed as equal on algebraic set $V(I)$.

Exercise 4.4.3. Let $f(x, y) = x^2 + y^2 - 1 \in \mathbb{C}[x, y]$. Suppose that $g, h \in \mathbb{C}[x, y]$ such that for all $(a, b) \in V(f)$ we have $g(a, b) = h(a, b)$. Show that the polynomial $g(x, y) - h(x, y) \in < x^2 + y^2 - 1 >$.

Exercise 4.4.4. Let V be an algebraic set in $\mathbb{A}^n(k)$. Prove that $\mathcal{O}(V)$ is ring-isomorphic to $k[x_1, \ldots, x_n]/I(V)$. (Here we are using that two functions should be viewed as equal if they agree on all points of the domain.)

Exercise 4.4.5. Let $V \subseteq k^n$ be an algebraic set. Prove that there is one-to-one correspondence from the set of all ideals of $k[x_1, \ldots, x_n]/I(V)$ onto the set of all ideals of $k[x_1, \ldots, x_n]$ containing $I(V)$.

Exercise 4.4.6. Let $V \subseteq k^n$ and $W \subseteq k^m$ be algebraic sets.

(1) Let $f : V \to W$ be a polynomial map, and define $\phi : k[W] \to k[V]$ by $\phi(g) = g \circ f$. Show that ϕ is a k-algebra homomorphism.
(2) Show that for each k-algebra homomorphism $\phi : k[W] \to k[V]$ there exists a polynomial map $f : V \to W$ such that $\phi(g) = g \circ f$, for all $g \in k[W]$.

4.5. Hilbert Basis Theorem

The goal of this section is prove the Hilbert Basis Theorem, which has as a consequence that every ideal in $\mathbb{C}[x_1, \ldots, x_n]$ is finitely generated.

How many polynomials are needed to define an algebraic set $V \subset \mathbb{C}^n$? Is there a finite number of polynomials $f_1, f_2, \ldots, f_m$ such that
$$V = \{a \in \mathbb{C}^n : f_i(a) = 0, \forall\, 1 \leq i \leq m\},$$
or are there times that we would need an infinite number of defining polynomials?

Exercise 4.5.1. Let $V = (x^2 + y^2 - 1 = 0)$. Show that $I(V)$ contains an infinite number of elements.

We know that there are an infinite number of possible defining polynomials, but do we need all of them to define V. In the above exercise, all we need is the single $x^2 + y^2 - 1$ to define the entire algebraic set. If there are times when we need an infinite number of defining polynomials, then algebraic geometry would be extremely hard. Luckily, the Hilbert Basis Theorem has as its core that we only need a finite set of polynomials to generate any ideal. The rest of this section will be pure algebra.

Recall that a (commutative) ring R is said to be *Noetherian* if every ideal I in R is finitely generated. (Recall that all rings considered in this book are commutative.)

We will define a ring R to be *noetherian* if every ideal of R is finitely generated.

EXERCISE 4.5.2. Show that every field and every principal ideal domain are Noetherian.

EXERCISE 4.5.3. Let R be a ring. Prove that the following three conditions are equivalent:

(1) R is Noetherian.
(2) Every ascending chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ of ideals in R is stationary, i.e., there exists N such that for all $n \geq N$, $I_n = I_N$.
(3) Every nonempty set of ideals in R has a maximal element (with inclusion being the ordering between ideals).

In what follows, we guide the reader through a proof of the Hilbert Basis Theorem.

EXERCISE 4.5.4. Consider the polynomial ring $R[x]$, where R is a Noetherian ring. If $I \subseteq R[x]$ is an ideal and $n \in \mathbb{N}$, let I_n be the set of leading coefficients of elements of I of degree n. Prove that I_n is an ideal in R.

EXERCISE 4.5.5. Consider the polynomial ring $R[X]$, where R is a Noetherian ring. Show that any ideal $I \subseteq R[X]$ is finitely generated.

The previous exercise establishes the following

THEOREM 4.5.6 (Hilbert Basis Theorem). *If R is a Noetherian ring then $R[x]$ is also a Noetherian ring.*

Sketch of proof. Let $I \subset R[x]$ be an ideal of $R[x]$. We show I is finitely generated.
Step 1. Let f_1 be a nonzero element of least degree in I.
Step 2. For $i > 1$, let f_i be an element of least degree in $I \setminus \{f_1, \ldots, f_{i-1}\}$, if possible.
Step 3. For each i, write $f_i = a_i x^{d_i} +$ lower order terms. That is, let a_i be the leading coefficient of f_i. Set $J = (a_1, a_2, \ldots)$.
Step 4. Since R is Noetherian, $J = (a_1, \ldots, a_m)$ for some m.
Step 5. Claim that $I = (f_1, \ldots, f_m)$. If not, there is an f_{m+1}, and we can subtract off its leading term using elements of $(f_1, \ldots, f_m)$ to get a contradiction.

EXERCISE 4.5.7. Justify **Step 4** in the above proof sketch.

EXERCISE 4.5.8. Fill in the details of **Step 5**.

EXERCISE 4.5.9. Show that if R is Noetherian then $R[x_1, \ldots, x_n]$ is Noetherian.

DEFINITION 4.5.1. Loosely speaking, a *formal power series is a power series in which questions of convergence are ignored.*

DEFINITION 4.5.2. The set of all formal power series in variable x with coefficients in a commutative ring R form another ring that is written $R[[X]]$, and called the *ring of formal power series in the variable x over R.*

EXERCISE 4.5.10. Let R be a Noetherian ring. Prove that the formal power series ring $R[[x]]$ is also Noetherian.

EXERCISE 4.5.11. Let R be a ring all of whose prime ideals are finitely generated. Prove that R is Noetherian.

4.6. Hilbert Nullstellensatz

The goal of this section is to guide the reader through a proof of Hilbert's Nullstellensatz. Hilbert's Nullstellensatz show there is a one-to correspondence between algebraic sets in $\mathbb{C}^n$ and radical ideals.

(This section is based on Arrondo's "Another Elementary Proof of the Nullstellensatz," which appeared in the American Mathematical Monthly on February of 2006.)

We know, given any ideal $I \subset \mathbb{C}[x_1, x_2, \ldots, x_n]$, that

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

But can there be some other ideal $J \subset \mathbb{C}[x_1, x_2, \ldots, x_n]$, with $V(J) = V(I)$ but $\sqrt{I} \neq \sqrt{J}$? The punch line for this section is that this is impossible.

EXERCISE 4.6.1. Prove that there exist $\lambda_1, \ldots, \lambda_4 \in \mathbb{C}$ such that the coefficient of x_4^2 in $f(x_1 + \lambda_1 x_4, x_2 + \lambda_2 x_4 x_3 + \lambda_3 x_4, x_4)$ is nonzero, where $f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4$.

EXERCISE 4.6.2. Let F be an infinite field and f be a nonconstant polynomial in $F[x_1, \ldots, x_n]$ (with $n \geq 2$). Prove that there exist $\lambda_1, \ldots, \lambda_n$ in F such that the coefficient of x_n^d in $f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$ is nonzero, whenever d is the total degree of $f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$.

EXERCISE 4.6.3. Let $I \subset \mathbb{C}[x_1, \ldots, x_4]$ be an ideal containing the polynomial $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$. Prove that, up to a change of coordinates and scaling, I contains a polynomial g monic in the variable x_4. (By *monic*, we mean that the coefficient of the highest power for x_n is one.)

EXERCISE 4.6.4. Let I be a proper ideal of $F[x_1, \ldots, x_n]$. Prove that, up to a change of coordinates and scaling, I contains a polynomial g monic in the variable x_n.

EXERCISE 4.6.5. Let I be a proper ideal of $F[x_1, \ldots, x_n]$ and let I' be the set of all polynomials in I that do not contain the indeterminate x_n. Prove that I' is an ideal of $F[x_1, \ldots, x_{n-1}]$ and that, modulo a change of coordinates and scaling (as in the previous exercise), the ideal I' is a proper ideal.

EXERCISE 4.6.6. Let I be an ideal of $F[x_1, \ldots, x_n]$ and let $g \in I$ be a polynomial monic in the variable x_n. Suppose there exists $f \in I$ such that $f(a_1, \ldots, a_{n-1}, x_n) = 1$. Consider $\operatorname{Res}(f, g; x_n)$ be the *resultant* of f and g with respect to the variable x_n, (refer to Definition 3.3.3) where $f = f_0 + f_1x_n + \cdots + f_dx_n^d$ with all the f_i in $F[x_1, \ldots, x_{n-1}]$ so that $f_0(a_1, \ldots, a_{n-1}) = 1$ and $f_i(a_1, \ldots, a_{n-1}) = 0$ for $1 \le i \le n$, and $g = g_0 + g_1x_n + \cdots g_{e-1}x_n^{e-1} + 1 \cdot x_n^e$ with all the g_j in $F[x_1, \ldots, x_{n-1}]$. Show that (under the current faulty hypotheses)

(1) $R \in I$;
(2) $R \in I'$;
(3) $R(a_1, \ldots, a_{n-1}) = 1$.

EXERCISE 4.6.7. Let I be a proper ideal of $F[x_1, \ldots, x_n]$. Prove that, modulo a change of coordinates and scaling, the set

$$J := \{f(a_1, \ldots, a_{n-1}, x_n) \mid f \in I\}$$

is a proper ideal of $F[x_n]$.

EXERCISE 4.6.8. Let I be a proper ideal of $F[x_1, \ldots, x_n]$. Prove that if F is algebraically closed, then there exists $(a_1, \ldots, a_n)$ in F^n such that $f(a_1, \ldots, a_n) = 0$ for all $f \in I$.

EXERCISE 4.6.9 (Weak Nullstellensatz). Let F be an algebraically closed field. Then an ideal I in $F[x_1, \ldots, x_n]$ is maximal if and only if there are elements $a_i \in F$ such that I is the ideal generated by the elements $x_i - a_i$; that is $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

Recall that an ideal I of a ring R is said to be a *radical ideal* if $x^n \in I$ for some $n \ge 1$ implies that $x \in I$. Given an arbitrary ideal I of a ring R, the *radical* $\sqrt{I}$ of I is the set of all elements $x \in R$ such that some positive power of x is in I.

EXERCISE 4.6.10. Given a ring R and an ideal I of R, prove that the radical $\sqrt{I}$ of I is an ideal.

EXERCISE 4.6.11. Let F be a field, and let V be an algebraic set in F^n for some $n \geq 1$. Prove that $I(V)$ is a radical ideal in the polynomial ring $F[x_1, \ldots, x_n]$. Moreover, prove that $V(I(V)) = A$ for any algebraic set A. (By $V(I)$ we mean the vanishing set of I.)

EXERCISE 4.6.12. Give an example where $\sqrt{I} \subsetneq I(V(\sqrt{I}))$, where $V(J)$ denotes the vanishing set of J.

EXERCISE 4.6.13 (Strong Nullstellensatz). Let F be an algebraically closed field and let I be an ideal of the polynomial ring $F[x_1, \ldots, x_n]$. Then $I(V(I)) = \sqrt{I}$.

4.7. Variety as Irreducible Algebraic Set: Prime Ideals

The goal of this section is to define affine varieties and to explore their topology and coordinate rings.

4.7.1. Irreducible components.

DEFINITION 4.7.1. An algebraic set V is *reducible* if $V = V_1 \cup V_2$, where V_1 and V_2 are algebraic sets with $V_1 \subsetneq V$ and $V_2 \subsetneq V$. An algebraic set that is not reducible is said to be *irreducible*.

DEFINITION 4.7.2. An *affine variety* is an irreducible algebraic set.

EXERCISE 4.7.1. Show that $\mathbb{A}^1$ is irreducible, so $\mathbb{A}^1$ is an affine variety.

EXERCISE 4.7.2. Decide if the following algebraic sets in $\mathbb{A}^2$ are reducible or irreducible.

(1) $V(x)$
(2) $V(x+y)$
(3) $V(xy)$

EXERCISE 4.7.3. Let $f \in k[x,y]$ and set $V = V(f)$. Show that if f factors as a product $f = gh$ of nonconstant polynomials $g, h \in k[x,y]$, then V is reducible.

4.7.2. Prime and non-prime ideals.

DEFINITION 4.7.3. A proper ideal $I \subset R$ is a *prime ideal* in R if, whenever $ab \in I$ for $a, b \in R$, either $a \in I$ or $b \in I$ (or both).

DEFINITION 4.7.4. A proper ideal $I \subset R$ is a *maximal ideal* in R if $I \subsetneq J \subset R$ for some ideal J implies that $J = R$.

Exercise 4.7.4. Every ideal I in $\mathbb{Z}$ is of the form $I = \langle m \rangle$ for some $m \in \mathbb{Z}$.

(1) For what values of m is the ideal $I = \langle m \rangle$ a prime ideal in $\mathbb{Z}$.
(2) For what values of m is the ideal $I = \langle m \rangle$ a maximal ideal in $\mathbb{Z}$.

Exercise 4.7.5. Let $f(x, y) = xy \in k[x, y]$. Show that the ideal $\langle f \rangle$ is not a prime ideal.

Exercise 4.7.6. Let $f \in k[x]$ be a nonconstant polynomial. Prove that f is an irreducible polynomial if and only if $\langle f \rangle$ is a prime ideal.

Exercise 4.7.7. Let I be an ideal in a ring R.

(1) Show that $I \subset R$ is a prime ideal if and only if R/I is an integral domain.
(2) Show that $I \subset R$ is a maximal ideal if and only if R/I is a field.
(3) Explain why every maximal ideal in R is prime.

Exercise 4.7.8. Let I be an ideal in a ring R. Show that

$$\sqrt{I} = \bigcap_{\text{prime } \mathfrak{p} \supseteq I} \mathfrak{p},$$

where $\mathrm{Rad}(I) = \{a \in R : a^n \in I \text{ for some } n > 0\}$.

Exercise 4.7.9. Let $\varphi : R \to S$ be a ring homomorphism.

(1) Let $J \subset S$ be a prime ideal in S. Show that $\varphi^{-1}(J)$ is a prime ideal in R.
(2) Let $J \subset S$ be a maximal ideal in S. Is $\varphi^{-1}(J)$ a maximal ideal in R? Prove or find a counterexample.

4.7.3. Varieties and Prime Ideals. We now reach the key results of this section.

Exercise 4.7.10. Let $V \subset \mathbb{A}^n$ be an algebraic set.

(1) Suppose that V is reducible, say $V = V_1 \cup V_2$ where V_1 and V_2 are algebraic sets with $V_1 \subsetneq V$ and $V_2 \subsetneq V$. Show that there are polynomials $P_1 \in I(V_1)$ and $P_2 \in I(V_2)$ such that $P_1 P_2 \in I(V)$ but $P_1, P_2 \notin I(V)$. Conclude that $I(V)$ is not a prime ideal.
(2) Prove that if $I(V)$ is not a prime ideal in $k[x_1, \ldots, x_n]$, then V is a reducible algebraic set.

is a prime ideal.

Exercise 4.7.11. Let V be an algebraic set in $\mathbb{A}^n$. Prove that the following are equivalent:

(1) V is an affine variety.
(2) $I(V)$ is a prime ideal in $k[x_1, \ldots, x_n]$.
(3) The coordinate ring, $\mathcal{O}(V)$, of V is an integral domain.

EXERCISE 4.7.12. Let $\mathcal{C}$ be the collection of nonempty algebraic sets in $\mathbb{A}^n$ that *cannot* be written as the union of finitely many irreducible algebraic sets.

(1) Suppose $\mathcal{C}$ is not empty. Show that there is an algebraic set V_0 in $\mathcal{C}$ such that V_0 does not contain any other set in $\mathcal{C}$. [Hint: If not, construct an infinite descending chain of algebraic sets $V_1 \supset V_2 \supset \cdots$ in $\mathbb{A}^n$. This implies $I(V_1) \subset I(V_2) \subset \cdots$ is an infinite ascending chain of ideals in $k[x_1, \ldots, x_n]$. Why is this a contradiction?]
(2) Show that the result of part (1) leads to a contradiction, so our assumption that $\mathcal{C}$ is not empty was false. Conclude that every algebraic set in $\mathbb{A}^n$ can be written as a union of a finite number of irreducible algebraic sets in $\mathbb{A}^n$.
(3) Let V be an algebraic set in $\mathbb{A}^n$. Show that V can be written as a union of finitely many irreducible algebraic sets in $\mathbb{A}^n$, $V = V_1 \cup \cdots \cup V_k$, such that no V_i contains any V_j.
(4) Suppose that $V_1 \cup \cdots \cup V_k = W_1 \cup \cdots \cup W_\ell$, where the V_i, W_j are irreducible algebraic sets in $\mathbb{A}^n$ such that no V_i contains any V_j and no W_i contains any W_j if $i \neq j$. Show that $k = \ell$ and, after rearranging the order, $V_1 = W_1, \ldots, V_k = W_k$.

Therefore, every algebraic set in $\mathbb{A}^n$ can be expressed uniquely as the union of finitely many affine varieties, no one containing another.

4.7.4. Examples.

EXERCISE 4.7.13. Show that $\mathbb{A}^n$ is an irreducible algebraic set for every $n \geq 1$. Thus every affine space is an affine variety.

EXERCISE 4.7.14. Let $f \in k[x, y]$ be an irreducible polynomial. Show that $V(f)$, which is a curve in $\mathbb{A}^2$, is an irreducible algebraic set.

4.8. Subvarieties

The goal of this section is to define subvarieties and see how some of their ideal theoretic properties.

DEFINITION 4.8.1. Let W be an algebraic variety that is properly contained in an algebraic variety $V \subset \mathbb{A}^n(k)$. Then W is a *subvariety* of V.

EXERCISE 4.8.1. Let $V = (x - y = 0) \subset \mathbb{A}^2(\mathbb{C})$. Show that the point $p = (1, 1)$ is a subvariety of V, while the point $q = (1, 2)$ is not a subvariety of V.

EXERCISE 4.8.2. Still using the notation from the first problem, show that $I(V)$ is contained in an infinite number of distinct prime ideals. Give a geometric interpretation for this.

EXERCISE 4.8.3. From the previous problem, find $I(V), I(p)$ and $I(q)$. Show that

$$I(V) \subset I(p)$$

and

$$I(V) \not\subset I(q).$$

EXERCISE 4.8.4. Let W be a subvariety of V. Show that

$$I(V) \subset I(W).$$

EXERCISE 4.8.5. Let V and W be two algebraic varieties in $\mathbb{A}^n(k)$. Suppose that

$$I(V) \subset I(J).$$

Show that W is a subvariety of V.

Thus we have an elegant diagram:

$$\begin{array}{ccc} W & \subset & V \\ I(W) & \supset & I(V) \end{array}$$

We now want to explore the relation between the coordinate ring $\mathcal{O}(V)$ and any coordinate ring $\mathcal{O}(W)$ for any subvariety W of a variety V.

EXERCISE 4.8.6. Continue letting $V = (x - y = 0) \subset \mathbb{A}^2(\mathbb{C})$, with subvariety $p = (1, 1)$. Find a polynomial $f \in \mathbb{C}[x, y]$ that is not identically zero on points of V but is zero at p, meaning there is a point $q \in V$ with $f(q) \neq 0$ but $f(p) = 0$. Show that

$$\sqrt{(f, I)} = J,$$

where $I = I(V)$ and $J = I(p)$. (Hint: if you choose f reasonably, then the ideal (f, I) will itself be equal to the ideal J.)

We have to worry a bit about notation. For $V \subset \mathbb{A}^n(k)$, we know that $\mathcal{O}(V) = k[x_1, \ldots, x_n]/I(V)$. Then given any $f \in k[x_1, \ldots, x_n]$, we can think of f as a function on V and hence as an element of $\mathcal{O}$, but we must keep in mind that if we write $f \in \mathcal{O}$, then f is standing for the equivalence class $f + I$, capturing that if f and $g \in k[x_1, \ldots, x_n]/I(V)$ agree on all points of V, the $f - g \in I$ and hence $f + I = g + I$, representing the same function in $\mathcal{O}$.

We have a ring theoretic exercise first.

EXERCISE 4.8.7. Let R be a commutative ring. Let $I \subset J$ be two ideals in R. Show that J/I is an ideal in the quotient ring R/I. Show that there is a natural onto map

$$R/I \to R/J$$

whose quotient is the ideal J/I.

EXERCISE 4.8.8. Continue letting $V = (x - y = 0) \subset \mathbb{A}^2(\mathbb{C})$, with subvariety $p = (1,1)$. Explicitly check the above exercise for $R = \mathbb{C}[x,y], I = (V)$ and $J = I(p)$.

For any type of subsets $W \subset V$, if $f : V \to k$, then there is the natural restriction map $f|_W : W \to k$, which just means for all $p \in W$ that we define

$$f|_W(p) = f(p).$$

EXERCISE 4.8.9. Let W be a subvariety of a variety $V \subset \mathbb{A}^n(k)$. Let $f \in \mathcal{O}(V)$. Show that the above restriction map sends f to an element of $\mathcal{O}(W)$ and that this restriction map is a ring homomorphism.

EXERCISE 4.8.10. Show that the kernel of the above restriction map is $I(W)/I(V)$ in the ring $\mathcal{O}(V)$.

EXERCISE 4.8.11. Discuss why each subvariety W of V should correspond to an onto ring homomorphism from the coordinate ring $\mathcal{O}(V)$ to a commutative ring.

Thus there are three equivalent ways for thinking of subvarieties of an algebraic variety V:

(1) W as an algebraic variety probably contained in an algebraic variety V.
(2) A prime ideal J properly containing the prime ideal $I(V)$
(3) A quotient ring of the ring $\mathcal{O}(V) = k[x_1, \ldots, x_n]/I(V)$.

4.9. Function Fields

The goal of this section is to associate not just a ring to an algebraic variety but also a field. This field plays a critical role throughout algebraic geometry.

Every algebraic variety V corresponds to a prime ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$. This allowed us to define the ring of functions on V, namely the quotient ring $\mathcal{O}_V = \mathbb{C}[x_1, \ldots, x_n]/I$. But every commutative ring sits inside of a field, much like the integers can be used to define the rational numbers. The goal of this subsection is to define the *function field* $\mathcal{K}_V$, which is the smallest field that the quotient ring $\mathcal{O}_V$ lives in.

DEFINITION 4.9.1. Given an algebraic variety V corresponding to a prime ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$, the *function field* $\mathcal{K}_V$ is:

$$\mathcal{K}_V = \left\{ \frac{f}{g} : f, g \in \mathcal{O}_V \right\} / \left(\frac{f_1}{g_1} = \frac{f_2}{g_2} \right) \}$$

where $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ means that

$$f_1 g_2 - f_2 g_1 \in I.$$

So far, $\mathcal{K}_V$ is simply a set. To make it into a field, we need to define how to add and multiply its elements. Define addition to be:

$$\frac{e}{f} + \frac{g}{h} = \frac{eh + fg}{fh}$$

and multiplication to be

$$\frac{e}{f} \cdot \frac{g}{h} = \frac{eg}{fh}.$$

EXERCISE 4.9.1. Show that addition is well-defined. This means you must show that if

$$\frac{e_1}{f_1} = \frac{e_2}{f_2}, \ \frac{g_1}{h_1} = \frac{g_2}{h_2},$$

then

$$\frac{e_1 h_1 + f_1 g_1}{f_1 h_1} = \frac{e_2 h_2 + f_2 g_2}{f_2 h_2}.$$

EXERCISE 4.9.2. Show that multiplication is well-defined. This means you must show that if

$$\frac{e_1}{f_1} = \frac{e_2}{f_2}, \ \frac{g_1}{h_1} = \frac{g_2}{h_2},$$

then

$$\frac{e_1 g_1}{f_1 h_1} = \frac{e_2 g_2}{f_2 h_2}.$$

Under these definitions, $\mathcal{K}_V$ is indeed a field.

Often a slightly different notation used. Just as $\mathbb{C}[x_1, \ldots, x_n]$ denotes the ring of all polynomials with complex coefficients and variables $x_1, \ldots x_n$, we let

$$\mathbb{C}(x_1, \ldots, x_n) = \left\{ \frac{f}{g} : f, g \in \mathbb{C}[x_1, \ldots, x_n] \right\}$$

subject to the natural relation that $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ means that $f_1 g_2 - f_2 g_1 = 0$. Then we could have defined the function field of a variety $V = V(I)$ to be

$$\mathcal{K}_V = \left\{ \frac{f}{g} : f, g \in \mathbb{C}[x_1, \ldots, x_n] \right\} / I.$$

4.10. Points as Maximal Ideals

DEFINITION 4.10.1. Let R be a ring. Recall that an ideal $I \subset R$ is *maximal* if I is proper ($I \neq R$) and any ideal J that contains I is either I or all of R.

EXERCISE 4.10.1. Show that for $a_1, a_2, \ldots, a_n \in k$, the ideal $I \subset k[x_1, \ldots, x_n]$ defined as

$$I = \langle x_1 - a_1, \ldots x_n - a_n \rangle$$

is maximal.

[Hint: Suppose J is an ideal with $I \subsetneq J$, and show that J contains 1.]

EXERCISE 4.10.2. Show that if an ideal $I \subset k[x_1, \ldots, x_n]$ is maximal, then $V(I)$ is either a point or empty.

EXERCISE 4.10.3. Show that $I(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

EXERCISE 4.10.4. Show that if k is an algebraically closed field, then every maximal ideal in $k[x_1, \ldots, x_n]$ can be defined as

$$I = \langle x_1 - a_1, \ldots x_n - a_n \rangle.$$

[Hint: Theorem 4.6.9.]

EXERCISE 4.10.5. Show that the result of the previous exercise is actually equivalent to Hilbert's Weak Nullstellensatz.

Combining Exercises 4.10.1 and 4.10.4, we obtain the following important fact.

THEOREM 4.10.6. In an algebraically closed field k, there is a one-to-one correspondence between points of $\mathbb{A}^n(k)$ and maximal ideals of $k[x_1, \ldots, x_n]$.

EXERCISE 4.10.7. Find a maximal ideal $I \subset \mathbb{R}[x_1, \ldots, x_n]$ for which $V(I) = \emptyset$.

4.11. The Zariski Topology

The goal of this section is to show that there is an algebraically defined topology for any ring.

4.11.1. Topologies. The development of topology is one of the great success stories of early 20th century mathematics. With a sharp definition for a topological space, once tricky notions such as "continuity" and "dimension" would have rigorous, meaningful definitions. As with most good abstractions, these definitions could be applied to situations far removed from what their founders intended. This is certainly the case in algebraic geometry.

The goal of this subsection is to briefly review what it means for a set to have a topology, using the standard topology on $\mathbb{R}$ and on $\mathbb{C}^n$ as motivating examples.

We start with the definition of a topology on a set X.

DEFINITION 4.11.1. A *topology* on the set X is given by specifying a collection $\mathcal{U}$ of subsets of X having the properties:

(1) Both the empty set and the entire set X are elements of the collection $\mathcal{U}$.
(2) The union of any subsets of X in $\mathcal{U}$ is also in $\mathcal{U}$. (It is critical that we allow even infinite unions.)
(3) The finite intersection of any subsets of X in $\mathcal{U}$ is also in $\mathcal{U}$. (Here is it critical that we only allow finite intersections.)

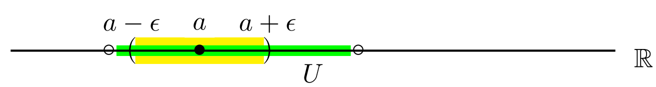
A set $U \in \mathcal{U}$ is said to be *open*. A set C is said to be *closed* if its complement $X - C$ is open.

Let us look at a few examples.

Start with the real numbers $\mathbb{R}$. We need to define what subsets will make up the collection $\mathcal{U}$.

DEFINITION 4.11.2. A set $U \subset \mathbb{R}$ is a *standard open set in* $\mathbb{R}$ if for any $a \in U$, there exists an $\epsilon > 0$ such that

$$\{x \in \mathbb{R} : |x - a| < \epsilon\} \subset U.$$



EXERCISE 4.11.1. Let $a, b \in \mathbb{R}$ with $a < b$.

(1) Show that in $\mathbb{R}$, $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ is open.
(2) Show that in $\mathbb{R}$, $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ is closed.
(3) Show that in $\mathbb{R}$, $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$ is neither open nor closed. (This type of set is often said to be half-open.)

EXERCISE 4.11.2. Show that the collection of standard open sets in $\mathbb{R}$ defines a topology on $\mathbb{R}$. This is called the *standard topology on* $\mathbb{R}$.

Let us now put a topology on $\mathbb{C}^n$.

DEFINITION 4.11.3. A set $U \subset \mathbb{C}^n$ is a *standard open set in* $\mathbb{C}^n$ if for any $a \in U$, there exists an $\epsilon > 0$ such that

$$\{x \in \mathbb{C}^n : |x - a| < \epsilon\} \subset U.$$

(Note that $|x - a| = \sqrt{|x_1 - a_1|^2 + \cdots + |x_n - a_n|^2}$ for $a = (a_1, \ldots, a_n)$ and $x = (x_1, \ldots x_n)$.)

Thus a set U is open in $\mathbb{C}^n$ if any of its points can be made the center of a little open ball that lies entirely within U.

EXERCISE 4.11.3. Show that the collection of standard open sets in $\mathbb{C}^n$ defines a topology on $\mathbb{C}^n$. This is called the *standard topology on* $\mathbb{C}^n$.

EXERCISE 4.11.4. In $\mathbb{C}^2$, show that $\mathbb{C}^2 - \mathrm{V}(x^2 + y^2 - 1)$ is open.

EXERCISE 4.11.5. In $\mathbb{C}^2$, show that $\mathbb{C}^2 - \mathrm{V}(P)$ is open for any polynomial $P(x, y)$.

EXERCISE 4.11.6. In $\mathbb{C}^3$, show that $\mathbb{C}^3 - \mathrm{V}(x^2 + y^2 + z^2 - 1)$ is open.

EXERCISE 4.11.7. In $\mathbb{C}^n$, show that $\mathbb{C}^n - \mathrm{V}(P)$ is open for any polynomial $P(x_1, x_2, \ldots, x_n)$, so $\mathrm{V}(P)$ is closed in the standard topology on $\mathbb{C}^n$.

EXERCISE 4.11.8. In $\mathbb{C}^2$, show that $\{(x, y) \in \mathbb{C}^2 : |x|^2 + |y|^2 < 1\}$ is open.

The standard topologies on $\mathbb{R}$ and $\mathbb{C}^n$ may be familiar to you. However, these are not the only topologies that can be defined on these sets. In the next exercise you will explore the finite complement topology on $\mathbb{R}$ and will see that it is different than the standard topology.

EXERCISE 4.11.9. *Finite complement topology on* $\mathbb{R}$: On $\mathbb{R}$ a set U is open if the complement of U is a finite collection of points, i.e. $U = \mathbb{R} - \{p_1, \ldots, p_k\}$. $\mathbb{R}$ and $\emptyset$ are also considered to be open sets.

(1) Verify that any arbitrary union of open sets is again open.
(2) Verify that any finite intersection of open sets is open.
(3) Conclude that the open sets defined above form a topology on $\mathbb{R}$. This is called the *finite complement topology on* $\mathbb{R}$.
(4) Show that if a set U is open in the finite complement topology, then it is open in the standard topology on $\mathbb{R}$.
(5) Give an example of an open set in the standard topology on $\mathbb{R}$ that is not open in the finite complement topology.
(6) Show that any two nonempty open sets in the finite complement topology on $\mathbb{R}$ must intersect. Is the same true in the standard topology on $\mathbb{R}$?

The final part of the previous exercise implies that the finite complement topology on $\mathbb{R}$ is not "Hausdorff" while the standard topology is. In a *Hausdorff topology* $\mathcal{U}$ on a set X, for any pair of distinct points $p, q \in X$ you can find open sets U, V such that $p \in U$, $q \in V$ and $U \cap V = \emptyset$. That is, we can "separate" p and q in X with disjoint open sets from $\mathcal{U}$. This is usually a desirable property in the study of topology, but it is not a property of the topology we use in algebraic geometry, the Zariski topology.

4.11.2. The Zariski Topology on $\mathbb{A}^n(k)$.

DEFINITION 4.11.4. Let k be a field. A set $X \subset \mathbb{A}^n(k)$ is a *Zariski-closed* set if X is an algebraic set. A set U is *Zariski-open* if $U = \mathbb{A}^n(k) - X$ where X is an algebraic set.

EXERCISE 4.11.10.

(1) Use Exercises 4.2.5 and **??** to show that the collection of Zariski-open sets in $\mathbb{A}^n(k)$ is a topology. This is called the *Zariski topology on* $\mathbb{A}^n(k)$.
(2) Show that a finite collection of points in $\mathbb{A}^n(k)$ is a Zariski-closed set.

EXERCISE 4.11.11. In this exercise, we compare the Zariski and finite complement topologies.

(1) Show that if a set U is open in the finite complement topology on $\mathbb{A}^n(k)$, then it is open in the Zariski topology on $\mathbb{A}^n(k)$.
(2) Show that the finite complement topology on $\mathbb{R}$ is the same as the Zariski topology on $\mathbb{R}$.
(3) Show that the finite complement topology on $\mathbb{C}$ is the same as the Zariski topology on $\mathbb{C}$.
(4) Show that a circle in $\mathbb{R}^2$ is a Zariski-closed set. Conclude that the Zariski topology is not the same as the finite complement topology on $\mathbb{R}^2$.

EXERCISE 4.11.12. In this exercise we describe the Zariski topology on $\mathbb{C}^2$.

(1) Show that, in $\mathbb{C}^2$, the complement of a finite number of points and algebraic curves is Zariski-open.
(2) Show that a non-empty Zariski-open set in $\mathbb{C}^2$ is the complement of a finite number of points and algebraic curves.

EXERCISE 4.11.13. Show geometrically that the Zariski topology on $\mathbb{C}^2$ is not Hausdorff.

4.11.3. Spec(R). For the standard topology on $\mathbb{C}^n$ it is critical that $\mathbb{C}^n$ has a natural notion of distance. For fields like $\mathbb{Z}_5$, there is no such distance. Luckily there is still a topology that we can associate to this or any other ring. The goal of this subsection is to define the Zariski topology for any ring R.

We first have to specify our set of points. We will see that our "points" will be the prime ideals in R. Recall that a proper ideal I in a ring R is *prime* if the following holds: whenever $f, g \in R$ with $fg \in I$, then $f \in I$ or $g \in I$. A proper ideal I of R is *maximal* if $I \subset J$ for some ideal J in R implies that either $J = I$ or $J = R$.

DEFINITION 4.11.5. The *prime spectrum* or *spectrum* of a ring R is the collection of prime ideals in R, denoted by Spec(R).

Thus for any ring R, the set on which we will define our topology is $\text{Spec}(R)$. This definition should be seen as a generalization of Theorem **??**, where we learned that points of $\mathbb{A}^n(k)$ correspond to maximal ideals in $k[x_1, \ldots, x_n]$. Since maximal ideals are prime, the set $\text{Spec}(R)$ includes all points from before and potentially more as we explore in the following exercises.

Exercise 4.11.14. Describe the following sets.

(1) $\text{Spec}(\mathbb{Z})$
(2) $\text{Spec}(\mathbb{R})$
(3) $\text{Spec}(k)$ for any field k

Exercise 4.11.15. Consider the polynomial ring $\mathbb{C}[x]$.

(1) Show that the ideal $\langle 0 \rangle$ is a prime ideal in $\mathbb{C}[x]$.
(2) Show that all prime ideals in $\mathbb{C}[x]$ are maximal ideals, except for the ideal $\langle 0 \rangle$.
(3) Show for each point $a \in \mathbb{C}$ there is a corresponding prime ideal.
(4) Explain why $\text{Spec}(\mathbb{C}[x])$ can reasonably be identified with $\mathbb{C}$.

Exercise 4.11.16. Show that there are three types of points in $\text{Spec}(\mathbb{R}[x])$:

i. The zero ideal $\langle 0 \rangle$,
ii. Ideals of the form $\langle x - a \rangle$ for a real number a,
iii. Ideals of the form $\langle x^2 + a \rangle$ for positive real numbers a.

Exercise 4.11.17. A curious property of "points" in $\text{Spec}(R)$.

(1) Show that $\langle x - y \rangle$ is a prime ideal in $\mathbb{C}[x, y]$ and hence is a point in $\text{Spec}(\mathbb{C}[x, y])$.
(2) For two fixed complex numbers a and b, show that $\langle x - a, y - b \rangle$ is a maximal ideal of $\mathbb{C}[x, y]$ and is hence also a point in $\text{Spec}(\mathbb{C}[x, y])$.
(3) Show that for every $a \in \mathbb{C}$, $\langle x - a, y - a \rangle$ contains the ideal $\langle x - y \rangle$.

Thus, in $\text{Spec}(R)$, some "points" can be contained in others. This suggests that not all points in $\text{Spec}(R)$ are created equal. Returning to our motivation in Theorem **??**, we make the following definition.

Definition 4.11.6. The *geometric points* in $\text{Spec}(R)$ are the maximal ideals.

By part (2) of Exercise 4.11.17, $\langle x - a, y - b \rangle$ is a maximal ideal in $\mathbb{C}[x, y]$, and hence a geometric point in $\text{Spec}(\mathbb{C}[x, y])$. In general, by Exercise 4.10.4, the maximal ideals in $\mathbb{C}[x_1, \ldots, x_n]$ are of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for $(a_1, \ldots, a_n) \in \mathbb{C}^n$. Thus the set of geometric points of $\text{Spec}(\mathbb{C}[x_1, \ldots, x_n])$ corresponds exactly to the set of points of $\mathbb{C}^n$. However, we should not confuse these two sets, for $\mathrm{Spec}(\mathbb{C}[x_1, \dots, x_n])$ contains many points other than its geometric ones as indicated in the previous exercises.

Now that we are better acquainted with our set of points, we are ready to define the topology.

DEFINITION 4.11.7. Let $S \subseteq R$. Define the *Zariski closed set* given by S in $\mathrm{Spec}(R)$ to be

$$Z(S) = \{P \in \mathrm{Spec}(R) : P \supseteq S\}.$$

A subset U of $\mathrm{Spec}(R)$ is *Zariski open* if there is a set $S \subseteq R$ with

$$U = \mathrm{Spec}(R) - Z(S).$$

EXERCISE 4.11.18. Let R be a ring. For a subset S of R, recall that $\langle S \rangle$ denotes the ideal in R generated by S.

(1) For a set $S \subseteq R$, show that $Z(S) = Z(\langle S \rangle)$.
(2) Show that $Z(\{0\}) = \mathrm{Spec}(R)$, and $Z(\{1\}) = \emptyset$.

EXERCISE 4.11.19. Show that a point I in $\mathrm{Spec}(R)$ is Zariski closed if and only if the ideal I is maximal in R.

Thus the geometric points of $\mathrm{Spec}(R)$ coincide with the points of $\mathrm{Spec}(R)$ that are Zariski closed. Thus we could have defined a geometric point as a point of $\mathrm{Spec}(R)$ that is Zariski closed.

As in Section **??** we want to create a dictionary for going back and forth between Zariski closed sets in $\mathrm{Spec}(R)$ and ideals in R. We have already described $Z(S)$, which assigns closed subsets of $\mathrm{Spec}(R)$ to ideals in R. Now we define the ideal associated to a subset of $\mathrm{Spec}(R)$.

DEFINITION 4.11.8. For $X \subseteq \mathrm{Spec}(R)$, define the *ideal of* X to be

$$I(X) = \bigcap_{P \in X} P.$$

By Exercise 4.7.8 part (2), $I(X)$ is a radical ideal in R.

EXERCISE 4.11.20. Let X and Y be subsets of $\mathrm{Spec}(R)$.

(1) Show that $X \subseteq Z(I(X))$.
(2) Show that if $X \subseteq Y$, then $I(Y) \subseteq I(X)$.

EXERCISE 4.11.21. Show that if X is a Zariski closed set in $\mathrm{Spec}(R)$, then $X = Z(I(X))$.

DEFINITION 4.11.9. For a subset Y of $\mathrm{Spec}(R)$, its *Zariski closure* of Y in $\mathrm{Spec}(R)$ is $\overline{Y} = Z(I(Y))$.

EXERCISE 4.11.22. Compute the Zariski closure of the following sets.

(1) $\{\langle 2\rangle, \langle 3\rangle\}$ in $\operatorname{Spec}(\mathbb{Z})$
(2) $\{\langle 0\rangle\}$ in $\operatorname{Spec}(\mathbb{Z})$
(3) $\{\langle x-y\rangle\}$ in $\operatorname{Spec}(\mathbb{C}[x,y])$

This reinforces our previous result that the geometric points of $\operatorname{Spec}(R)$ coincide with the Zariski closed points. Part (2) is especially interesting and deserves a name.

Definition 4.11.10. A point of $\operatorname{Spec}(R)$ whose closure is the whole space is called a *generic point*.

As we have already noted, the nature of points in $\operatorname{Spec}(R)$ challenges our geometric intuition. Still, we have also seen that several of the results from Section **??** for our dictionary between closed sets and ideals in R continue to hold in $\operatorname{Spec}(R)$. Here is one more of these results, which will prove important in our proof that the collection of Zariski open sets defines a topology on $\operatorname{Spec}(R)$.

Exercise 4.11.23. Show that if X and Y are Zariski closed sets in $\operatorname{Spec}(R)$, then $X \cup Y = Z(I(X) \cap I(Y))$ and $X \cap Y = Z(I(X) + I(Y))$.

Exercise 4.11.24. Show that the Zariski closed sets are closed under arbitrary intersections.

We want to show that the Zariski open sets make up a topology on $\operatorname{Spec}(R)$. We first do a few set-theoretic exercises.

Exercise 4.11.25. Let X be a set. Define for any set U in X its complement to be $U^c = X - U$. Show that

$$(U^c)^c = U.$$

Exercise 4.11.26. For subsets U_α, $\alpha \in A$, of a set X, let $C_\alpha = U_\alpha^c$.

(1) Show that

$$\bigcup_\alpha U_\alpha = X - \bigcap_\alpha C_\alpha.$$

(2) Show that

$$\bigcap_\alpha U_\alpha = X - \bigcup_\alpha C_\alpha.$$

With these results from set theory in hand, we return to the space $\operatorname{Spec}(R)$ and prove that the collection of Zariski open sets defines a topology on this set.

Exercise 4.11.27. Let U_1 and U_2 be Zariski open sets in $\operatorname{Spec}(R)$. Show that $U_1 \cap U_2$ is a Zariski open set in $\operatorname{Spec}(R)$.

Exercise 4.11.28. Let $\{U_\alpha : \alpha \in A\}$ be an arbitrary collection of Zariski open sets in $\operatorname{Spec}(R)$. Show that $\bigcup_\alpha U_\alpha$ is a Zariski open set in $\operatorname{Spec}(R)$.

Exercise 4.11.29. Show that the collection of Zariski open sets forms a topology on $\operatorname{Spec}(R)$.

4.12. Points and Local Rings

The goal of this section is to show how to link points on an algebraic variety V with local rings of $\mathcal{O}(V)$, which are subrings of the function field $\mathcal{K}_V$.

We want to study what is going on around a point p in an algebraic variety. One approach would be to understand the behavior of the functions on V near p. If we just want to know what is going on at p, then what a function is doing far from p is irrelevant. The correct ring-theoretic concept will be that of a local ring.

We start with points in affine varieties $V \subset \mathbb{A}^n(k)$ and their local rings. We then see how to put this into a much more general language.

4.12.1. Points as Maximal Ideals in Affine Varieties. In Section **??** we proved that points in $\mathbb{A}^n(k)$ correspond to maximal ideals in $k[x_1, \ldots, x_n]$ and, conversely, that maximal ideals correspond to points when the field k is algebraically closed (Theorem **??**). In the following exercises, we prove similar results for affine varieties $V \subset \mathbb{A}^n(k)$.

EXERCISE 4.12.1. Let $V = \mathrm{V}(x^2 + y^2 - 1) \subset \mathbb{A}^2(k)$. Let $p = (1, 0) \in V$. Define

$$\mathcal{M}_p = \{f \in \mathcal{O}(V) : f(p) = 0\}.$$

(1) Show that $\mathcal{M}_p$ is an ideal in $\mathcal{O}(V)$.
(2) Show that $\mathcal{M}_p$ is in fact a maximal ideal in $\mathcal{O}(V)$.

EXERCISE 4.12.2. Let $\mathcal{M}$ be a maximal ideal in $\mathcal{O}(V)$ for the variety $V = \mathrm{V}(x^2 + y^2 - 1)$ from the previous problem. Let

$$\mathrm{V}(\mathcal{M}) = \{p \in V : \text{ for all } f \in \mathcal{M},\ f(p) = 0\}.$$

Show that $\mathrm{V}(\mathcal{M})$ must be a single point on V.

EXERCISE 4.12.3. Let $V \subset \mathbb{A}^n(k)$ be an algebraic variety. Let p be a point in V. Define

$$\mathcal{M}_p = \{f \in \mathcal{O}(V) : f(p) = 0\}.$$

Show that $\mathcal{M}_p$ is a maximal ideal in $\mathcal{O}(V)$.

EXERCISE 4.12.4. Let $\mathcal{M}$ be a maximal ideal in $\mathcal{O}(V)$, for $V \subset \mathbb{A}^n(k)$. Let

$$V(\mathcal{M}) = \{p \in V : \text{ for all } f \in \mathcal{M},\ f(p) = 0\}.$$

Show that $V(\mathcal{M})$ must be a single point in V.

Thus we can either think of a point p as defining a maximal ideal in the coordinate ring $\mathcal{O}(V)$ or as a maximal ideal in $\mathcal{O}(V)$ as defining a point on V. This extends the results of Theorem **??** to affine varieties in general.

4.12.2. Local Ring at a Point. Let $V \subset \mathbb{A}^n(k)$ be an algebraic variety and let p be a point in V. We want to concentrate on the functions on V defined near p. Suppose there is a $g \in \mathcal{O}(V)$ with $g(p) \neq 0$, say $g(p) = 1$. Then close to p, whatever that means, the function g looks a lot like the constant function 1. This means that we should be allowed to look at $1/g$, which is generally not allowed in $\mathcal{O}(V)$ but is in its function field, $\mathcal{K}_V$.

Recall the construction of $\mathcal{K}_V$ from Section **??**. By definition,

$$\mathcal{K}_V = \left\{ \frac{f}{g} : f, g \in \mathcal{O}(V), g \neq 0 \right\} / \left(\frac{f_1}{g_1} \sim \frac{f_2}{g_2} \right),$$

where $f_1/g_1 \sim f_2/g_2$ if $f_1 g_2 - f_2 g_1 \in I(V)$. Addition and multiplication were defined as usual for fractions,

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \quad \text{and} \quad \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2},$$

both of which are well-defined. This set with these operations is then a field. We now define the local ring at p to be a subring of this field.

DEFINITION 4.12.1. Let p be a point on an algebraic variety V. The *local ring* associated to p is

$$\mathcal{O}_p(V) = \left\{ \frac{f}{g} \in \mathcal{K}_V : \ g(p) \neq 0 \right\}.$$

EXERCISE 4.12.5. Let p be a point in an algebraic variety V. Prove that its local ring $\mathcal{O}_p(V)$ is a subring of the function field $\mathcal{K}_V$.

EXERCISE 4.12.6. Let $V = \mathrm{V}(x^2 + y^2 - 1) \subset \mathbb{A}^2(k)$ and $p = (1, 0) \in V$.

(1) Show for $f(x, y) = x \in \mathcal{O}_p(V)$ that there is an element $g \in \mathcal{O}_p(V)$ such that $f \cdot g = 1$ in $\mathcal{O}_p(V)$.
(2) Show for $f(x, y) = y \in \mathcal{O}_p(V)$ that there can exist no element $g \in \mathcal{O}_p(V)$ such that $f \cdot g = 1$ in $\mathcal{O}_p(V)$.
(3) Show that the ring $\mathcal{O}_p(V)$ cannot be a field.

EXERCISE 4.12.7. Let p be a point in an algebraic variety $V \subseteq \mathbb{A}^n(k)$ and let

$$\mathcal{M}_p = \{ f \in \mathcal{O}_p(V) : f(p) = 0 \}.$$

(1) Suppose that $f \notin \mathcal{M}_p$. Show that there exists an element $g \in \mathcal{O}_p(V)$ such that $f \cdot g = 1$ in $\mathcal{O}_p(V)$.
(2) Show that $\mathcal{M}_p$ is the unique maximal ideal in the ring $\mathcal{O}_p(V)$.

4.12.3. Local Rings in Commutative Algebra. We now shift gears and make things quite a bit more abstract. Part of the power of algebraic geometry is that we can start with geometric insights and translate these into the language of ring theory, allowing us to think geometrically about rings for which there is little apparent geometry. This is not our emphasis in this book, but the following is included to give just a flavor of this.

In Exercise 4.12.7 we saw that the local ring at a point p in an affine variety V, $\mathcal{O}_p(V)$, has a unique maximal ideal, $\mathcal{M}_p$. Inspired by this, we make the following definition for commutative rings in general.

Definition 4.12.2. A *local ring* is a ring that has a unique maximal ideal.

Now we can talk about local rings quite generally. For example, every field is a local ring since the only proper ideal in a field is the zero ideal. However, as we have seen in Exercise 4.12.6, not every local ring is a field.

The rest of this section develops the method of localization for creating local rings from a given commutative ring R. This method is similar to the creation of $\mathcal{O}_p(V)$ above, where we create a new ring of "fractions" of elements from R with denominators from one of its subsets. In $\mathcal{O}_p(V)$, that set of denominators was $\{g \in \mathcal{O}(V) : g(p) \neq 0\}$. In this case and in all of our other experiences with fractions, both addition and multiplication require we multiply denominators and again have a valid denominator. This leads to the following definition.

Definition 4.12.3. A nonempty subset S of a ring R is said to be *multiplicatively closed* in R if, whenever $a, b \in S$, the product $ab \in S$.

Exercise 4.12.8.

(1) Show that $S = \{1, 3, 9, 27, \ldots\} = \{3^k : k \geq 0\}$ is a multiplicatively closed set in $\mathbb{Z}$.
(2) Let R be a ring and let $a \neq 0$ be an element of R. Show that the set $S = \{a^k : k \geq 0\}$ is a multiplicatively closed set in R.

Exercise 4.12.9.

(1) Let $p \in \mathbb{Z}$ be a prime number. Show that the set $\mathbb{Z} - \langle p \rangle$ is multiplicatively closed.
(2) Let R be a ring and assume that $I \subset R$ is a maximal ideal in R. Show that $S = R - I$ is multiplicatively closed.
(3) Let R be a ring and $I \subset R$ be any ideal. Under what conditions on the ideal I will the subset $S = R - I$ be a multiplicatively closed subset of R? Prove your answer.

Let S be a multiplicatively closed set in R. Define an equivalence relation $\sim$ on the set $R \times S$ as follows:

$$(r, s) \sim (r', s') \quad \Longleftrightarrow \quad \exists\, t \in S \text{ such that } t(s'r - sr') = 0.$$

Exercise 4.12.10. Show that $\sim$ is an equivalence relation on $R \times S$.

EXERCISE 4.12.11. Describe the equivalence relation $\sim$ on $R \times S$ if $0 \in S$.

Let $R_S = (R \times S)/\sim$ and let $[r,s]$ denote the equivalence class of (r,s) with respect to $\sim$. Define addition in R_S by

$$[r_1, s_1] \underset{S}{+} [r_2, s_2] = [r_1 s_2 + r_2 s_1, s_1 s_2].$$

and multiplication by

$$[r_1, s_1] \underset{S}{\cdot} [r_2, s_2] = [r_1 r_2, s_1 s_2].$$

EXERCISE 4.12.12. Show that $\underset{S}{+}$ and $\underset{S}{\cdot}$ are well-defined operations on R_S.

With a little work checking the axioms, one can show that R_S is a ring under the addition and multiplication defined above. This ring is called the *localization* of R at S.

EXERCISE 4.12.13. Let $S = \mathbb{Z} - \{0\}$. What is $\mathbb{Z}_S$? Is $\mathbb{Z}_S$ a local ring?

EXERCISE 4.12.14. Let $R = \mathbb{Z}$ and $S = \{2^k : k \geq 0\} = \{1, 2, 4, 8, \ldots\}$.

(1) Show that S is multiplicatively closed in R.
(2) Show that, in $R_S = \mathbb{Z}_S$, addition and multiplication of $[a, 2^m], [b, 2^n]$ agrees with the addition and multiplication of the fractions $a/2^m$ and $b/2^n$ in $\mathbb{Q}$.
(3) Let $S' = \{2, 4, 8, \ldots\} = \{2^k : k \geq 1\}$. Show that $R_{S'} \cong R_S$.

EXERCISE 4.12.15. Let R be a ring and $I \subset R$ be a prime ideal. Set $S = R - I$, which is a multiplicatively closed set in R, and consider the ring R_S.

(1) Show that R_S is a local ring. Describe its unique maximal ideal.
(2) Show that the proper ideals in R_S correspond to ideals J in R such that $J \subseteq I$.

We conclude this section by showing that the method of localization developed above gives another way to create the local ring at a point in $\mathbb{A}^n(k)$.

EXERCISE 4.12.16. Let p be a point in $\mathbb{A}^n(k)$. Let $\mathfrak{m}_p = \{f \in k[x_1, \ldots, x_n] : f(p) = 0\}$. By the Weak Nullstellensatz (Theorem 4.6.9), $\mathfrak{m}_p$ is a maximal ideal in $R = k[x_1, \ldots, x_n]$. Prove that the localization of R at $S = R - \mathfrak{m}_p$ is isomorphic to $\mathcal{O}_p(\mathbb{A}^n(k))$.

4.13. Tangent Spaces

The goal of this section is to establish the equivalence among several different notions of the tangent space T_pV of a variety V at a point p.

4.13.1. Derivations. There are several equivalent notions of a tangent space in algebraic geometry. Before developing the algebraic idea of a tangent space we will consider the familiar tangent space as it is usually defined in a multivariable calculus course, but we want to be able to work over any field k, not just $\mathbb{R}$ and $\mathbb{C}$, so we need to generalize our idea of differentiation.

To motivate this new definition let's consider the main properties of the derivative map. The derivative is linear, the derivative of a constant is zero, and the derivative obeys the Leibnitz rule. The derivative map is an example of a derivation.

DEFINITION 4.13.1. A *derivation* of a k-algebra[1] R is a map $L : R \to R$ with the following properties:

(i) L is k-linear, i.e., $L(af + bg) = aL(f) + bL(g)$ for all $a, b \in k$ and $f, g \in R$,
(ii) L obeys the Leibnitz rule, $L(fg) = gL(f) + fL(g)$ for all $f, g \in R$.

EXERCISE 4.13.1. Suppose R is a k-algebra. Show that if $L : R \to R$ is a derivation, then $L(a) = 0$ for all $a \in k$. [Hint: Show that $L(1) = 0$ and apply (i).]

EXERCISE 4.13.2. Verify that $\dfrac{d}{dx} : k[x] \to k[x]$ formally defined by

$$\frac{d}{dx}[a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0] = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

is a derivation.

4.13.2. First Definition. We will first give an extrinsic definition of the tangent space of an affine variety at a point. We will identify the tangent space to $\mathbb{A}^n$ at each point $p \in \mathbb{A}^n$ with the vector space k^n.

DEFINITION 4.13.2. Let $I \subset k[x_1, \ldots, x_n]$ be a prime ideal, $V = \mathrm{V}(I) \subset \mathbb{A}^n$ an affine variety, and $p = (p_1, p_2, \cdots, p_n) \in V$. The *tangent space* of the variety V at p is the linear subspace

$$T_pV := \left\{ (x_1, x_2, \ldots, x_n) \in k^n : \sum_{i=1}^{n} (x_i - p_i)\frac{\partial f}{\partial x_i}(p) = 0, \text{ for all } f \in I \right\},$$

where $\dfrac{\partial}{\partial x_i}$ is the derivation defined formally by

$$\frac{\partial}{\partial x_i} x_j^m = \begin{cases} m x_j^{m-1} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

and imposing that it is k-linear and satisfies the Leibnitz rule.

[1]A *k-algebra* is a k-vector space that also has a multiplication making it a ring.

If $k = \mathbb{C}$ or $\mathbb{R}$, then $\dfrac{\partial}{\partial x_i}$ can be regarded as the usual partial derivative.

In the special case that V is a hypersurface, $V = \mathrm{V}(f)$ for $f \in k[x_1, \ldots, x_n]$, the tangent space of the hypersurface $V = \mathrm{V}(f)$ at p is simply

$$T_pV := \left\{ (x_1, x_2, \ldots, x_n) \in k^n : \sum_{i=1}^{n} (x_i - p_i) \frac{\partial f}{\partial x_i}(p) = 0 \right\}.$$

Exercise 4.13.3. In $\mathbb{R}^2$ let $f(x, y) = x^2 + y^2 - 1$ and consider the curve $C = \mathrm{V}(f)$. Let $p = (a, b)$ be a point on C.

(1) Find the normal direction to C at p.
(2) How is the normal direction to C at p related to the gradient of f at p?
(3) Use Definition 4.13.2 to find T_pC.
(4) How is T_pC related to $\nabla f(p)$?

Exercise 4.13.4. Show that T_pV, as defined in Definition 4.13.2, is a vector space over k by identifying the vector $(x_1, \ldots, x_n)$ in T_pV with the vector $(x_1 - p_1, \ldots, x_n - p_n)$ in k^n.

Exercise 4.13.5. In $\mathbb{C}^2$, consider the complex curve $C = \mathrm{V}(f)$ given by

$$f(x, y) = x^4 + x^2y^2 - 2y - 4 = 0$$

(1) Find the tangent line at $p = (1, 3)$ using Definition 4.13.2.
(2) Homogenize f to obtain $F(x, y, z)$ and let $\tilde{C} = \mathrm{V}(F) \subset \mathbb{P}^2(\mathbb{C})$. Use Definition 4.13.2 to find $T_{p'}\tilde{C}$ at $p' = (1 : 3 : 1)$.
(3) Let $z = 1$ to dehomogenize the equation in part (2) and check you get the equation in part (1).
(4) Convince yourself that for any C in $\mathbb{C}^2$ given by $f(x, y) = 0$, the tangents obtained by the two methods shown in parts (1) and (2) agree.

4.13.3. Second Definition. Next, we consider another definition of an affine tangent space. Recall the definition of the local ring of a variety V at p,

$$\mathcal{O}_p(V) = \left\{ \frac{f}{g} : f, g \in \mathcal{O}(V),\ g(p) \neq 0 \right\}.$$

This local ring captures the behavior of functions on V near p. That is, $\mathcal{O}_p(V)$ gives an algebraic description of V near p. On the other hand, the tangent space to V at p gives a geometric description of V near p. With our second definition of T_pV, we connect these descriptions, using derivations on $\mathcal{O}_p(V)$ to construct T_pV.

Definition 4.13.3. The *tangent space* of the variety V at p is the linear space

$$T_pV := \{L : \mathcal{O}_p(V) \to \mathcal{O}_p(V) \ : \ L \text{ is a derivation}\}.$$

For any point $p \in \mathbb{A}^n$, $T_p\mathbb{A}^n$ is the vector space span $\left\{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right\}$, where $\frac{\partial}{\partial x_i}$ are defined formally as above. When $V = \mathrm{V}(I) \subset \mathbb{A}^n$ is an affine variety, T_pV is the subspace of linear combinations of $\frac{\partial}{\partial x_i}$ that agree on I. In other words, T_pV consists of all derivations L, $L = \sum_{i=1}^{n} \alpha_i \frac{\partial}{\partial x_i}$, such that $L(f)(p) = 0$ for all $f \in I$.

Exercise 4.13.6. In $\mathbb{R}^2$ let $f(x, y) = x^2 + y^2 - 1$, consider the curve $C = \mathrm{V}(f)$. Let $p = (a, b)$ be a point on C.

(1) Use Definition 4.13.3 to find T_pC.
(2) Find a vector space isomorphism between T_pC found in part (2) of Exercise 4.13.3 and T_pC found in part (1) of this exercise.

Exercise 4.13.7. Show that T_pV as defined in Definition 4.13.3 is a vector space over k.

Exercise 4.13.8. Show that $L(f) = L(g)$ if and only if $f - g \in I$.

Exercise 4.13.9. In $\mathbb{A}^2(\mathbb{C})$, consider the complex curve $C = \mathrm{V}(x^2 + y^2 - 1)$. At a point $p = (a, b) \in C$, show that $\mathfrak{m}_p/\mathfrak{m}_p^2$ is a 1-dimensional vector space over $\mathbb{C}$. Relate this 1-dimensional vector space to the tangent line found in Exercise 4.13.3.

Exercise 4.13.10. In this problem, let

$$\begin{array}{rcll} z_1 & = & x + iy & \in \mathbb{C}, \quad (x, y) \in \mathbb{R}, \\ z_2 & = & u + iv & \in \mathbb{C}, \quad (u, v) \in \mathbb{R} \end{array}$$

Suppose $V \in \mathbb{C}^2$ is defined via $F(z_1, z_2) = z_1 - z_2^2 = 0$.

(1) Let $P_0 = (z_{1_0}, z_{2_0}) = (-1, i)$. Is $P_0 \in V$?
(2) Find the tangent line $h(z_1, z_2) = 0$ to P_0 using
$$\frac{\partial F}{\partial z_i}(P_0) = 0.$$
(3) Show that V, viewed as a set $V_{\mathbb{R}} \in \mathbb{R}^4$ is the intersection of two surfaces,
$$\begin{array}{rcl} f(x_1, x_2, x_3, x_4) & = & 0, \\ g(x_1, x_2, x_3, x_4) & = & 0. \end{array}$$
Find f and g explicitly. Intuitively, what is the real dimension of $V_{\mathbb{R}}$?
(4) Find the point $Q_0 = (x_{1_0}, x_{2_0}, x_{3_0}, x_{4_0}) \in \mathbb{R}^4$ to which $P_0 = (z_{1_0}, z_{2_0}) \in \mathbb{C}^2$ corresponds.
(5) Find two normal vectors in $\mathbb{R}^4$ to $V_{\mathbb{R}}$ at Q_0 via $\vec{N}_1 = \vec{\nabla} f | Q_0$, $\vec{N}_2 = \vec{\nabla} g | Q_0$. The real tangent space $T_{\mathbb{R},Q_0}$ to $V_{\mathbb{R}}$ at Q_0 is the set of lines through Q_0 perpendicular to $\vec{N}_1, \vec{N}_2$. Intuitively, what is the real dimension k of $T_{\mathbb{R},Q_0}$? Is $T_{\mathbb{R},Q_0}$ a k-plane in $\mathbb{R}^4$?

(6) In Exercise 4.13.10(2), you found the tangent line equation $h(z_1, z_2)$ to V at P_0 in $\mathbb{C}^2$. Write the tangent line as a system of 2 equations in $\mathbb{R}^4$ using x, y, u, v. These equations correspond to 2 planes $Pl_1, Pl_2 \in \mathbb{R}^4$. Let $T = Pl_1 \cap Pl_2$. Find 2 linearly independent vectors $\vec{D_1}, \vec{D_2} \in \mathbb{R}^4$ parallel to T. Show that $\vec{D_1} \perp \vec{N_1}, \vec{N_2}$ and $\vec{D_2} \perp \vec{N_1}, \vec{N_2}$. Is T the same as $T_{\mathbb{R},Q_0}$? Does this convince you that if C is a curve in $\mathbb{C}^2$ and $T_{\mathbb{C},P_0}$ is the tangent line to C at P_0, then $T_{\mathbb{C},P_0}$ is the usual geometric tangent space to C at P_0 when $\mathbb{C}^2$ is thought of as $\mathbb{R}^4$?

EXERCISE 4.13.11. In $\mathbb{P}^2(\mathbb{C})$, let C be $F[x_1, x_2, x_3] = x_2x_3 - x_1^2 = 0$. Verify that $P = [2, 4, 1]$ is on C. Suppose you try to define the tangent to C at $Q_0 = [x_{1_0}, x_{2_0}, x_{3_0}]$ as

$$\sum_{i=1}^{3} \frac{\partial F}{\partial x_i}(Q_0)(x_i - x_{i_0}) = 0 \tag{4.1}$$

(1) Find the tangent line at $P = [1, 2, 4]$ using Equation 4.1.
(2) Find the tangent line at $P = [2, 4, 8]$ using Equation 4.1.
(3) Consider the line

$$\sum_{i=1}^{3} \frac{\partial F}{\partial x_i}(Q_0)(x_i) = 0 \tag{4.2}$$

(a) For C and $Q_0 = P = [1, 2, 4]$, what is Equation 4.2?
(b) For C and $Q_0 = P = [2, 4, 8]$, what is Equation 4.2?

In this case do that lines seem to be same regardless of the way you write P and whether you use Equation 4.1 or 4.2? The actual definition of the tangent is Equation 4.2, not Equation 4.1. Does this problem indicate why?

EXERCISE 4.13.12. Euler's formula says that if $F[x_0, x_1, \cdots, x_n]$ is a homogeneous polynomial of degree d, then

$$\sum_{i=1}^{n} \frac{\partial F}{\partial x_i}(Q_0)(x_i) = d \cdot F[x_0, x_1, \cdots, x_n].$$

Let $F[x_1, x_2, x_3] = x_1^3 + 5x_1^2x_2 + 7x_1x_2x_3$. Verify Euler's formula in this case.

EXERCISE 4.13.13. Returning to Exercise 4.13.11, explain why the tangent line is the same whether you use $*$ or $**$ and does not depend on the $\lambda \neq 0$ you use to define $Q_0 = [\lambda x_{1_0}, \lambda x_{2_0}, \lambda x_{3_0}]$.

4.13.4. Tangent lines of higher orders. Let V be a curve defined by a polynomial equation $f(x_0, x_1) = 0$ in $\mathbb{C}^2$. Let $P \in V$.

Let L be a line in $\mathbb{C}^2$ through P. We say L is a *tangent to V at P of order at least k* if, for some parameter α, there are points $p_1(\alpha), \ldots, p_{k+1}(\alpha) \in$ V such that

a. $\forall \alpha \neq 0$, $p_1(\alpha), \cdots, p_k(\alpha)$ are distinct;
b. $\forall \alpha \neq 0$, $p_1(\alpha), \cdots, p_k(\alpha)$ are collinear and lie on a line L_α of the form $A(\alpha)x_0 + B(\alpha)x_1 + C(\alpha) = 0$;
c. As $\alpha \to 0$, $p_1(\alpha), \cdots, p_k(\alpha) \to P$;
d. As $\alpha \to 0$, $L_\alpha \to L$, meaning $A(\alpha), B(\alpha), C(\alpha) \to A, B, C$ where L is given by $Ax_0 + Bx_1 + C = 0$.

We further say L is a *tangent of order k* if it is a tangent of order at least k but not at least $k+1$.

In the following $P = (0,0)$ and V is one of these curves.

$$\begin{aligned} C_1: &\quad x_1 = x_0^2 \\ C_2: &\quad x_1 = x_0^3 \\ C_3: &\quad x_1^2 = x_0^3 \\ C_4: &\quad x_1^2 = x_0^3 + x_0^2 \\ C_5: &\quad x_1^2 = x_0^4 + x_0^2 \end{aligned}$$

Exercise 4.13.14. Sketch the real parts of each curve near P.

Exercise 4.13.15.

(1) Show that at $P = (0,0)$, the line $x_1 = 0$ is a tangent of order
- 1 for C_1;
- 2 for C_2;
- 2 for C_3.

(2) Show $x_1 = x_0$ and $x_1 = -x_0$ are tangent of order ≥ 1 for C_4, C_5. Make a guess about their actual order.
(3) Draw pictures to convince yourself that in C_2 every line through $(0,0)$ is a tangent of order ≥ 1.

Exercise 4.13.16. Rewrite curves C_1 through C_5 in the form $g(x_0, x_1) = 0$. Go through the list and for each $g(x,y) = 0$,

(1) Write out for $C_1 - C_5$ the equations gotten from only keeping terms of degree $\geq k$ and also terms of degree equal to k;
(2) Then go through that list and modify those in reasonable ways by identifying groups of terms corresponding to $f(x_0, x_1) = 0$.

Exercise 4.13.17. Now for each curve in your list, compute the graded ring,

$$\bigoplus_{k \geq 1} \frac{m_p^k}{m_p^{k+1}}$$

4.14. Dimension

One may think of dimension of an affine variety V as the number of coordinates needed to describe V. The dimension will depend on our base field k, as we have seen in the first few chapters when we considered complex curves as surfaces over $\mathbb{R}$. To carefully introduce the definition of the dimension of a variety we will first use its corresponding function field. We will also introduce dimension of tangent space at a point to define dimension of an affine variety.

4.14.1. Dimension as Transcendence Degree of Function Field.

DEFINITION 4.14.1. Let K be an extension field of k. The *transcendence degree* of K over k is the maximum number of elements of K that are algebraically independent over k.

For example, the transcendence degree of $k(u)$, the rational functions in one variable, is one since u is algebraically independent; the transcendence degree of a field k over itself is 0.

We can now define dimension using the function field of a variety. Refer to Definition 4.9.1.

DEFINITION 4.14.2. Let $V \subseteq \mathbb{A}^n$ be an affine variety. The *dimension* of V, denoted by $dim\, V$, is the transcendence degree of its function field $\mathcal{K}_V$ over k.

Thus a point in affine space, which has function field isomorphic to k, has dimension zero. The function field of the affine line $\mathbb{A}^1$ is $k(u)$, so $\mathbb{A}^1$ has dimension one. Similarly we can show that affine $n-$space has the expected dimension.

EXERCISE 4.14.1. Let $\mathcal{K}_{\mathbb{A}^n}$ be the function field of $\mathbb{A}^n$.

(1) Show that $\mathcal{K}_{\mathbb{A}^n} \cong k(x_1, \ldots, x_n)$.
(2) Show that $\{x_1, \ldots, x_n\}$ is a maximal set of algebraically independent elements over k.
(3) Conclude that the dimension of $\mathbb{A}^n$ is n.

The next exercise will also check that our definition of dimension agrees with our intuition.

EXERCISE 4.14.2. Let $V = V(f(x, y))$ be an irreducible plane curve. Show that V has dimension one.

EXERCISE 4.14.3. Let $V = V(f(x, y))$ be an irreducible surface. Show that V has dimension two.

4.14.2. Dimension of the Tangent Space at a Point. We can also define dimension of a variety V using the tangent space at a point. Refer to Definition 4.13.2. The tangent space at a point p of a variety V, T_pV, gives a vector space of dimension at least that of V.

Definition 4.14.3. Let $V \subseteq \mathbb{A}^n$ be an irreducible variety. Then the *dimension* of V is the minimum nonzero dimension of T_pV over all points $p \in V$.

Here we define the dimension of T_pV to be its dimension as a vector space over the field k. For example, at any point p the tangent space $T_p\mathbb{A}^n$ is just $\mathbb{A}^n$, which is n-dimensional over k.

Exercise 4.14.4. Let p and q be points of a curve V. Suppose V intersects itself at p but has a well-defined tangent line at q.

(1) Show that T_pV has dimension greater than 1 at the point p.
(2) Show that T_qV has dimension 1 at the point q.

Exercise 4.14.5. Let $V = V(f)$ be an irreducible hypersurface in $\mathbb{A}^n$. Show that V has dimension $n-1$.

In fact the subset of points at which the dimension of the tangent space is greater than the dimension of the variety forms a closed subvariety. We will see in the next section that these are the *singular* points of V.

Exercise 4.14.6. In Definition 4.14.3, must V be an irreducible variety? Why?

The next exercise may help clarify.

Exercise 4.14.7. Let $V \subset \mathbb{A}^3$ be the variety defined by $V(xz, yz)$.

(1) Pick p to be the origin. Show that the dimension of the tangent space T_pV is three.
(2) Show that V is reducible.
(3) Compute the dimension of the tangent space at a point on each component of V.
(4) Use the irreducible components of V to explain why the dimension of V is two.

We define the dimension of a reducible variety to be the maximum dimension of its components. The previous exercises lead us to the definition of *smooth* and *singular* points in terms of dimension.

4.15. Singular Points

A singularity of a variety is a point where the variety exhibits unusual behavior. We saw in section 1.9 that a plane curve $V(f(x,y))$ is singular at any point p where $f, \frac{\partial f}{\partial x}$, and $\frac{\partial f}{\partial y}$ vanish simultaneously. This is equivalent to the curve having an undefined tangent at p. In a similar fashion we will use the tangent space T_pV to determine the singularities of a variety of arbitrary dimension.

DEFINITION 4.15.1. Let V be an affine variety and $p \in V$. We say that p is a *singular* point of V if $\dim T_pV > \dim V$; otherwise $\dim T_pV = \dim V$ and p is a *smooth* point.

Recall that the dimension of the tangent space satisfies $\dim T_pV \geq \dim V$. We will first verify that this definition of singular point coincides with our previous one in the case of a plane curve.

EXERCISE 4.15.1. Let $V = V(f(x,y)) \subset \mathbb{A}^2$ be an irreducible curve and let p be a point on V.

(1) Show that the tangent space T_pV as defined in section 4.12 is equivalent to the tangent line of this curve as defined in section 1.9.
(2) Suppose at least one of $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ is non-zero at p. Show that T_pV is one-dimensional and thus p is a smooth point of V.
(3) Suppose $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ both vanish at p. Show that T_pV has dimension two, thus p is a singular point of V..

EXERCISE 4.15.2. Determine the singular points of each curve.

(1) $V(y^2 - x^3 + x^2)$
(2) $V(y^2 - x^3)$

We have previously seen the nodal and cuspidal singular cubics of the last exercise. More generally we can determine when a cubic in normal form is singular.

EXERCISE 4.15.3. Let $f(x)$ be a polynomial and let $V = V(y^2 - f(x))$. (In the case where f has degree three, V is the normal form of a cubic curve.) Show that V is singular at a point (x_0, y_0) if and only if $y_0 = 0$ and x_0 is a multiple root of $f(x)$.

EXERCISE 4.15.4. Find all singular points of each surface in $\mathbb{A}^3$.

(1) $V(x^2 + y^2 - z^2)$
(2) $V(x^2 - y^2 z)$
(3) $V((x-y)^2 + z^3)$

The case of a hypersurface is similar to that of curves, in that the tangent space is defined by one equation.

EXERCISE 4.15.5. Let V be the hypersurface $f(x_1, \ldots, x_n) = 0$ in $\mathbb{A}^n$ and let p be a point on V. Recall from Exercise 4.14.5 V has dimension $n-1$.

(1) Suppose at least one of the $\frac{\partial f}{\partial x_i}$ is non-zero at p. Show that T_pV has dimension $n-1$. Conclude that p is a smooth point of V.
(2) Suppose $\frac{\partial f}{\partial x_i}(p) = 0$ for $i = 1, \ldots, n$. Show that $T_pV = \mathbb{A}^n$. Conclude that p is a singular point.

EXERCISE 4.15.6. Let $V = V(x^2 + y^2 + z^2 - 1, x - 1) \subset \mathbb{A}^3$.

(1) Show that V has dimension one, by visualizing V as the intersection of the surface $x^2 + y^2 + z^2 = 1$ and the plane $x = 1$.
(2) Show that the tangent space T_pV to V at $p = (1, 0, 0)$ is the plane $x-1 = 0$, thus T_pV has dimension two. Conclude that V is singular at p.

EXERCISE 4.15.7. Let $V = V(fg)$ and let p be a point of intersection of the hypersurfaces $V(f)$ and $V(g)$. Show that p is a singular point of V.

Alternately we can determine the singularities of a variety V using the generators of the ideal $I(V)$.

DEFINITION 4.15.2. Let $\{f_1, f_2, \ldots, f_m\}$ be a generating set for $I(V)$, with each $f_i \in k[x_1, \ldots, x_n]$, where $V = V(f_1, f_2, \ldots, f_m) \subset \mathbb{A}^n$. The *Jacobian* matrix for V at a point $p \in V$ is the $m \times n$ matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$.

This definition depends upon the set of generators for $I(V)$. We will see that the rank of the Jacobian matrix is independent of this choice, thus we can use the rank of the Jacobian to give an alternate definition of singularity.

DEFINITION 4.15.3. Let V be a variety in $\mathbb{A}^n$ of dimension d. V is non-singular at p if and only if the rank of the Jacobian matrix at p is equal to $n - d$.

EXERCISE 4.15.8. Let V be the curve $V(x - yz, xz - y^2, y - z^2) \subset \mathbb{A}^3$. Show that the Jacobian matrix has rank two at every point $p \in V$. Conclude that V is a smooth curve.

EXERCISE 4.15.9. Compute the Jacobian matrix for $V = V(x^2 + y^2 + z^2 - 1, x - 1) \subset \mathbb{A}^3$.

(1) Show the Jacobian has rank two when y or z is non-zero.
(2) Show the Jacobian has rank one when $y = z = 0$. Use this to determine the singular points of V.

EXERCISE 4.15.10. Let $V = V(x + y + z, x - y + z) \subset \mathbb{A}^3$.

(1) Compute the Jacobian matrix for V and show that V is non-singular everywhere.
(2) Show that $\{x + z, y\}$ is also a generating set for $I(V)$.
(3) Compute the Jacobian matrix using this alternate set of generators and show that it has the same rank as your matrix in part (1).

EXERCISE 4.15.11. Let $V = V(x^2 + y^2 - 1, x^2 + z^2 - 1) \subset \mathbb{A}^3$.

(1) Compute the Jacobian matrix for V and find all points where the rank is not equal to two.

(2) Show that $\{y^2 - z^2, 2x^2 + y^2 + z^2 - 2\}$ is also a generating set for $I(V)$.
(3) Compute the Jacobian matrix using this alternate set of generators and show that it has the same rank as your matrix in part (1).

EXERCISE 4.15.12. For a hypersurface $V(f) \subset \mathbb{A}^n$ the Jacobian matrix at p is

$$\left(\frac{\partial f}{\partial x_1}(p) \; \frac{\partial f}{\partial x_2}(p) \; \cdots \; \frac{\partial f}{\partial x_n}(p) \right).$$

Show that V is non-singular at p if at least one of the $\frac{\partial f}{\partial x_i}(p)$ is non-zero. Thus for hypersurfaces this definition coincides with our previous one.

In the next exercise we will show more generally that our two definitions agree.

EXERCISE 4.15.13. Let p be a point of a d-dimensional variety $V \subset \mathbb{A}^n$ and let $\{f_1, f_2, \ldots, f_m\}$ be a generating set for $I(V)$.

(1) By identifying each point $q \in \mathbb{A}^n$ with the vector $q - p$, show that the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$ defines a linear transformation from $\mathbb{A}^n$ to $\mathbb{A}^m$.
(2) Show the kernel of this transformation is the tangent space T_pV.
(3) Use the Rank-Nullity Theorem to conclude that p is a non-singular point of V if and only if the rank of the Jacobian matrix is equal to $n - d$.

In each of our examples we have seen that the singularities form a proper subvariety of V. Our next exercises will show this more generally.

EXERCISE 4.15.14. Let V be an affine variety. Prove that the set of singular points of V is a closed subset of V.

EXERCISE 4.15.15. Let $V = V(f) \subset \mathbb{A}^n$ be an irreducible hypersurface over $\mathbb{C}$. Prove that the singularities of V are a proper subvariety. (Compare with Exercise 4.14.5.)

The previous exercise shows that the singularities are a proper subvariety in the case of hypersurfaces. One can extend this result to all affine varieties using the fact that every irreducible variety is "equivalent" to a hypersurface. The equivalence is obatining using a birational morphism, which will be defined in the next section.

4.16. Morphisms

The goal of this section is to define a natural type of mapping between algebraic sets.

The world of algebraic geometry is the world of polynomials. For example, algebraic sets are defined as the set of common zeros of collections of polynomials. The morphisms, or mappings, between them should also be given by polynomials.

Suppose $X \subset \mathbb{A}^n(k)$ and $Y \subset \mathbb{A}^n(k)$ are algebraic sets. The natural mappings (*morphisms*) between X and Y are polynomial mappings:

$$\begin{aligned} \phi : X &\to Y \\ p &\mapsto (f_1(p), \ldots, f_m(p)) \end{aligned}$$

for some $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$.

The map ϕ induces a ring homomorphism

$$\begin{aligned} \mathcal{O}(Y) &\to \mathcal{O}(X) \\ f &\mapsto f \circ \phi \end{aligned}$$

Exercise 4.16.1. Show that the above map is indeed a ring homomorphism.

A ring homomorphism

$$\sigma : k[y_1, \ldots, y_m]/I(Y) = \mathcal{O}(Y) \to \mathcal{O}(X) = k[x_1, \ldots, x_n]/I(X)$$

induces a morphism

$$\begin{aligned} X &\to Y \\ p &\mapsto (f_1(p), \ldots, f_m(p)) \end{aligned}$$

where $f_i = \sigma(y_i)$.

Exercise 4.16.2. Let $X = V(y - x^2)$, the parabola, and let $Y = V(y)$, the x-axis. Then $\phi : X \to Y$ given by $\phi(x, y) = x$ is a morphism. This morphism simply projects points on the parabola onto the x-axis. Find the image of $y \in \mathcal{O}(Y)$ in $\mathcal{O}(X)$ by the above ring homomorphism $\sigma : \mathcal{O}(Y) \to \mathcal{O}(X)$.

Exercise 4.16.3. Let $X = V(v - u^2)$, and let $Y = V(z^2 - xy)$. We may think of X as a parabola and Y as a double cone. Define a morphism

$$\begin{aligned} \phi : X &\to Y \\ (u, v) &\mapsto (1, v, u) \end{aligned}$$

Show that the image of ϕ is actually in Y. The effect of this morphism is to map the parabola into the cone. Show that the corresponding ring homomorphism

$$A(Y) = \mathbb{C}[x, y, z]/(x^2 - xy) \to A(X) = \mathbb{C}[u, v]/(v - u^2)$$

is given by

$$x \mapsto 1, \quad y \mapsto v, \quad z \mapsto u.$$

Exercise 4.16.4. For each of the polynomial mappings $X \to Y$, describe the corresponding ring homomorphism $\sigma : \mathcal{O}(Y) \to \mathcal{O}(X)$.

(1)

$$\begin{aligned} \phi : \mathbb{A}^2(k) &\to \mathbb{A}^3(k) \\ (x,y) &\mapsto (y-x^2, xy, x^3+2y^2) \end{aligned}$$

(2) $X = \mathbb{A}^1(k)$ and $Y = V(y-x^3, z-xy) \subset \mathbb{A}^3(k)$.

$$\begin{aligned} \phi : X &\to Y \\ t &\mapsto (t, t^3, t^4) \end{aligned}$$

EXERCISE 4.16.5. For each of the ring homomorphisms $\sigma : \mathcal{O}(Y) \to \mathcal{O}(X)$, describe the corresponding morphism of algebraic sets, $X \to Y$.

(1)

$$\begin{aligned} \sigma : k[x,y] &\to k[t] \\ x &\mapsto t^2-1 \\ y &\mapsto t(t^2-1) \end{aligned}$$

(2)

$$\begin{aligned} \sigma : k[s,t,uw]/(s^2-w, sw-tu) &\to k[x,y,z]/(xy-z^2) \\ s &\mapsto xy \\ t &\mapsto yz \\ u &\mapsto xz \\ w &\mapsto z^2 \end{aligned}$$

The morphism constructed here is a mapping of the saddle surface to a surface in $\mathbb{A}^4(k)$.

(Note: Much of this section was taken from David Perkinson's lectures at PCMI 2008.)

4.17. Isomorphisms of Varieties

The goal of this problem set is to establish a correspondence between polynomial maps of varieties $V_1 = V(I_1) \subset \mathbb{A}^n(k)$ and $V_2 = V(I_2) \subset \mathbb{A}^m(k)$ and ring homomorphisms of their coordinate rings $k[V_1] = k[x_1, \ldots, x_n]/I_1$ and $k[V_2] = k[y_1, \ldots, y_m]/I_2$. In particular, we will show that $V_1 \cong V_2$ as varieties if and only if $k[V_1] \cong k[V_2]$ as rings.

4.17.1. Definition. Let $V_1 = V(I_1) \subset \mathbb{A}^n(k)$ and $V_2 = V(I_2) \subset \mathbb{A}^m(k)$ be algebraic sets in $\mathbb{A}^n(k)$ and $\mathbb{A}^m(k)$, respectively. We will assume in the following that each I_j is a radical ideal. As we have already seen, the ring $\mathcal{O}(V_1) = k[x_1, \ldots, x_n]/I_1$ is in a natural way the ring of (equivalence classes of) polynomial functions mapping V_1 to k. We can then define a polynomial map $P : V_1 \to V_2$ by $P(x_1, \ldots, x_n) = (P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n))$ where $P_i \in k[V_1]$. Alternatively, $P : V_1 \to V_2$ is a polynomial map of varieties if $P_i = y_i \circ P \in k[V_1]$. (Note: This is to emphasize that y_i and x_i are coordinate functions on $\mathbb{A}^m(k)$ and $\mathbb{A}^n(k)$, respectively.)

A polynomial map $P : V_1 \to V_2$ is an *isomorphism* of varieties if there exists a polynomial map $Q : V_2 \to V_1$ such that $Q \circ P = \mathrm{Id}|_{V_1}$ and $P \circ Q = \mathrm{Id}|_{V_2}$. Two varieties are isomorphic if there exists an isomorphism between them.

Exercise 4.17.1. Let $k = \mathbb{R}$. Let $V_1 = V(x) \subset \mathbb{R}^2$ and $V_2 = V(x + y) \subset \mathbb{R}^2$.

(1) Sketch V_1 and V_2.
(2) Find a one-to-one polynomial map $P(x, y) = (P_1(x, y), P_2(x, y))$ that maps V_1 onto V_2.
(3) Show $V_1 \cong V_2$ as varieties by finding an inverse polynomial map $Q(x, y)$ for the polynomial map $P(x, y)$ above. Verify that $Q \circ P = \mathrm{Id}\Big|_{V_1}$ and $P \circ Q = \mathrm{Id}\Big|_{V_2}$.

Exercise 4.17.2. Let $k = \mathbb{R}$. Let $V_1 = \mathbb{R}$ and $V_2 = V(x - y^2) \subset \mathbb{R}^2$ be algebraic sets.

(1) Sketch V_2.
(2) Find a one-to-one polynomial map $P(x)$ that maps V_1 onto V_2.
(3) Show $V_1 \cong V_2$ as algebraic sets by finding an inverse $Q(x, y)$ for the polynomial map $P(x)$ above. Verify that $Q \circ P = \mathrm{Id}\Big|_{V_1}$ and $P \circ Q = \mathrm{Id}\Big|_{V_2}$.

Exercise 4.17.3. Let $k = \mathbb{C}$. Let $V_1 = V(x^2 + y^2 - 1) \subset \mathbb{C}^2$ and $V_2 = V(x^2 - y^2 - 1) \subset \mathbb{C}^2$ be varieties.

(1) Find a one-to-one polynomial map $P(x, y)$ that maps V_1 onto V_2.
(2) Show $V_1 \cong V_2$ as varieties by finding an inverse $Q(x, y)$ for the polynomial map $P(x, y)$ above. Verify that $Q \circ P = \mathrm{Id}\Big|_{V_1}$ and $P \circ Q = \mathrm{Id}\Big|_{V_2}$.
(3) If $k = \mathbb{R}$, do you think $V(x^2 + y^2 - 1) \subset \mathbb{R}^2$ and $V(x^2 - y^2 - 1) \subset \mathbb{R}^2$ are isomorphic as varieties? Why or why not?

Exercise 4.17.4. Let k be any algebraically closed field. Let $V_1 = V(x + y, z - 1) \subset \mathbb{A}^3(k)$ and $V_2 = V(x^2 - z, y + z) \subset \mathbb{A}^3(k)$ be varieties.

(1) Find a one-to-one polynomial map $P(x, y, z)$ that maps V_1 onto V_2.

(2) Show $V_1 \cong V_2$ as varieties by finding an inverse $Q(x, y, z)$ for the polynomial map $P(x, y, z)$ above. Verify that $Q \circ P = \mathrm{Id}\Big|_{V_1}$ and $P \circ Q = \mathrm{Id}\Big|_{V_2}$.

4.17.2. Link to Ring Isomorphisms. Let's now consider the relationship between the coordinate rings $\mathcal{O}(V_1)$ and $\mathcal{O}(V_2)$ of two varieties. We will show that there is a one-to-one correspondence between polynomial maps $P : V_1 \to V_2$ of varieties and ring homomorphisms $\phi : \mathcal{O}(V_2) \to \mathcal{O}(V_1)$ of coordinate rings. First suppose $P : V_1 \to V_2$ is a polynomial map. Define $P^* : \mathcal{O}(V_2) \to \mathcal{O}(V_1)$ by $P^*(f) = f \circ P$. Next, if $\phi : \mathcal{O}(V_2) \to \mathcal{O}(V_1)$, we can construct a polynomial map $P : V_1 \to V_2$ such that $P^* = \phi$.

Exercise 4.17.5. Consider Exercise **4.17.1**.

(1) Let $f, g \in \mathbb{R}[x, y]$ agree on V_2, i.e. $f - g \in \langle x + y\rangle$. Show that $P^*(f) = P^*(g)$ in $\mathbb{R}[V_1]$.
(2) Show that P^* is a ring isomorphism by finding its inverse.

Exercise 4.17.6. Show $\mathbb{R}[x] \cong \mathbb{R}[x, y]/\langle x - y^2\rangle$ as rings.

Exercise 4.17.7. Show $\mathbb{C}[x, y]/\langle x^2 + y^2 - 1\rangle \cong \mathbb{C}[x, y]/\langle x^2 - y^2 - 1\rangle$ as rings.

Exercise 4.17.8. Show $k[x, y, z]/\langle x + y, z - 1\rangle \cong k[x, y, z]/\langle x^2 - z, y + z\rangle$ as rings.

Exercise 4.17.9. Let $V_1 = V(I_1) \subset \mathbb{A}^n(k)$, $V_2 = V(I_2) \subset \mathbb{A}^m(k)$, and $V_3 = V(I_3) \subset \mathbb{A}^i(k)$ be varieties and suppose $P : V_1 \to V_2$ and $Q : V_2 \to V_3$ are polynomial maps.

(1) Explain why $P^* : \mathcal{O}(V_2) \to \mathcal{O}(V_1)]$, i.e. explain why we define the map to go from $\mathcal{O}(V_2) \to \mathcal{O}(V_1)$ and not vice versa. In words, we "pull back" functions from $\mathcal{O}(V_2)$ to $\mathcal{O}(V_1)$ rather than "push forward" functions from $\mathcal{O}(V_1)$ to $\mathcal{O}(V_2)$.
(2) Show that $P^* : \mathcal{O}(V_2) \to \mathcal{O}(V_1)$ is well-defined, i.e. show that if $f = g \mod I_2$, then $P^*(f) = P^*(g) \mod I_1$.
(3) Show $(Q \circ P)^* = P^* \circ Q^*$.
(4) Show that if P is an isomorphism of varieties, then P^* is an isomorphism of rings.

Exercise 4.17.10. Let $V_1 = V(I_1) \subset \mathbb{A}^n(k)$ and $V_2 = V(I_2) \subset \mathbb{A}^m(k)$ be varieties. Recall that $\mathcal{O}(V_1) = k[x_1, \ldots, x_n]/I_1$ and $\mathcal{O}(V_2) = k[y_1, \ldots, y_m]/I_2$. Then x_i and y_j are coordinate <u>functions</u>, so let us consider their images in the quotient rings $\mathcal{O}(V_1)$ and $\mathcal{O}(V_2)$. Let u_i denote the image of x_i under the map $k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/I_1$ and let v_i denote the image of y_i under the map $k[y_1, \ldots, y_n] \to k[y_1, \ldots, y_n]/I_2$, i.e. $k[V_1] = k[u_1, \ldots, u_n]$ and $k[V_2] = k[v_1, \ldots, v_m]$. In general, the $u_i s$ are not algebraically independent and neither are the $v_i s$.

(1) Let $V_1 = V(x) \subset \mathbb{R}^2$ and $V_2 = V(x+y) \subset \mathbb{R}^2$. Find u_1, u_2, v_1, and v_2, such that $k[V_1] = k[u_1, u_2]$ and $k[V_2] = k[v_1, v_2]$.
(2) Let $V_1 = V(x^2 + y^2 - 1) \subset \mathbb{C}^2$ and $V_2 = V(x^2 - y^2 - 1) \subset \mathbb{C}^2$. Find u_1, u_2, v_1, and v_2, such that $k[V_1] = k[u_1, u_2]$ and $k[V_2] = k[v_1, v_2]$.
(3) Let $V_1 = V(x+y, z-1) \subset \mathbb{A}^3(k)$ and $V_2 = V(x^2 - z, y+z) \subset \mathbb{A}^3(k)$. Find u_1, u_2, u_3, v_1, v_2, and v_3 such that $\mathcal{O}(V_1) = k[u_1, u_2, u_3]$ and $\mathcal{O}(V_2) = k[v_1, v_2, v_3]$.

EXERCISE 4.17.11. Let $V_1 = V(I_1) \subset \mathbb{A}^n(k)$ and $V_2 = V(I_2) \subset \mathbb{A}^m(k)$ be varieties and suppose $\phi : \mathcal{O}(V_2) \to \mathcal{O}(V_1)]$ is a ring homomorphism. Our goal is to construct a polynomial map $P : V_1 \to V_2$ such that $P^* = \phi$. Let u_j and v_j denote the coordinate functions as above on $k[V_1]$ and $k[V_2]$, respectively. Define $P = (P_1, \ldots, P_m) : V_1 \to V_2$ such that $P_i = \phi \circ v_i$.

(1) Let $V_1 = V(x) \subset \mathbb{R}^2$ and $V_2 = V(x+y) \subset \mathbb{R}^2$. Find the corresponding polynomial map for $\phi : \mathbb{R}[V_2] \to \mathbb{R}[V_1]$ defined by $\phi(v_1) = u_1$, $\phi(v_2) = u_2$.
(2) Let $V_1 = V(x^2 + y^2 - 1) \subset \mathbb{C}^2$ and $V_2 = V(x^2 - y^2 - 1) \subset \mathbb{C}^2$. Find the corresponding polynomial map for $\phi : \mathbb{C}[V_2] \to \mathbb{C}[V_1]$ defined by $\phi(v_1) = u_1$, $\phi(v_2) = u_2$.
(3) Let $V_1 = V(x+y, z-1) \subset \mathbb{A}^3(k)$ and $V_2 = V(x^2 - z, y+z) \subset \mathbb{A}^3(k)$. Find the corresponding polynomial map for $\phi : \mathcal{O}(V_2)] \to \mathcal{O}(V_1)$ defined by $\phi(v_1) = u_1$, $\phi(v_2) = u_2$, and $\phi(v_3) = u_3$.

EXERCISE 4.17.12. Let $V_1 = V(I_1) \subset \mathbb{A}^n(k)$ and $V_2 = V(I_2) \subset \mathbb{A}^m(k)$ be varieties and suppose $\phi : \mathcal{O}(V_2) \to \mathcal{O}(V_1)$ is a ring homomorphism. Let u_j and v_j denote the coordinate functions as above on $k[V_1]$ and $k[V_2]$, respectively. Define $P = (P_1, \ldots, P_m) : V_1 \to V_2$ such that $P_i = \phi \circ v_i$.

(1) Verify that P is a well-defined map from V_1 to V_2.
(2) Verify that P is a polynomial map.
(3) Verify that $P^* = \phi$.
(4) Show that if Q is another polynomial map $V_1 \to V_2$ such that $Q^* = \phi$, then $Q = P$ (in $k[V_1]$).
(5) Show that $P : V_1 \to V_2$ is an isomorphism of varieties if and only if $P^* : \mathcal{O}(V_2) \to \mathcal{O}(V_1)$ is an isomorphism of rings.

EXERCISE 4.17.13. Let $V_1 = \mathbb{A}^1(k)$ and $V_2 = V(x^3 - y^2) \subset \mathbb{A}^2(k)$.

(1) Sketch V_2 for the case when $k = \mathbb{R}$. Note the cusp at the point (0,0) in $\mathbb{R}^2$.
(2) Verify that $P(x) = (t^2, t^3)$ is a one-to-one polynomial map that maps V_1 onto V_2.
(3) Show that P does not have a polynomial inverse.

(4) Show that the map P does not have a *polynomial* inverse.

(5) Show that $k[t] \ncong k[x,y]/\langle x^3 - y^2\rangle$ as rings. [Hint: Showing that P^* is not an isomorphism is not enough. You must show that there is *no* isomorphism between these rings. Show that $k[t] \cong k[t^2,t^3]$ and that $k[t^2,t^3] \ncong k[t]$.]

4.18. Rational Maps

The goal of this section is to define a the second most natural type of mapping between algebraic sets: rational maps.

There are two natural notions of equivalence in algebraic geometry: isomorphism (covered earlier in this chapter) and birationality (the topic for this section). Morally two varieties will be birational if there is a one-to-one map, with an inverse one-to-one map, from one of the varieties to the other, allowing though for the maps to be undefined possibly at certain points. Instead of having maps made up of polynomials, our maps will be made up of ratios of polynomials; hence the maps will not be defined where the denominators are zero. We will first define the notion of a *rational* map, then birationality.

4.18.1. Rational Maps.

Definition 4.18.1. A *rational map*

$$F : \mathbb{A}^n(k) \dashrightarrow \mathbb{A}^m(k)$$

is given by

$$F(x_1,\dots,x_n) = \left(\frac{P_1(x_1,\dots,x_n)}{Q_1(x_1,\dots,x_n)},\dots,\frac{P_m(x_1,\dots,x_n)}{Q_m(x_1,\dots,x_n)}\right)$$

where each P_i and Q_j is a polynomial in $k[x_1,\dots,x_n]$ and none of the Q_j are identically zero.

It is common to use a "$\dashrightarrow$" instead of a '$\rightarrow$" to reflect that F is not defined at all points in the domain.

Exercise 4.18.1. Let $F : \mathbb{C}^2 \to \mathbb{C}^3$ be given by

$$F(x_1,x_2) = \left(\frac{x_1+x_2}{x_1-x_2}, \frac{x_1^2+x_2}{x_1}, \frac{x_1x_2^3}{x_1+3x_2}\right).$$

The rational map F is not defined on three lines in $\mathbb{C}^2$. Find these three lines. Draw these three lines as lines in $\mathbb{R}^2$.

Let $V = V(I) \subset \mathbb{A}^n(k)$ and $W = V(J) \subset \mathbb{A}^m(k)$ be two algebraic varieties, with defining prime ideals $I \subset k[x_1,\dots,x_n]$ and $J \subset k[x_1,\dots,x_m]$, respectively.

Definition 4.18.2. A rational map

$$F : V \dashrightarrow W$$

is given by a rational map $F : \mathbb{A}^n(k) \dashrightarrow \mathbb{A}^m(k)$ with

$$F(x_1, \ldots, x_n) = \left(\frac{P_1(x_1, \ldots, x_n)}{Q_1(x_1, \ldots, x_n)}, \ldots, \frac{P_m(x_1, \ldots, x_n)}{Q_m(x_1, \ldots, x_n)}\right)$$

such that

(1) The variety V is not contained in any of the hypersurfaces $V(Q_i)$. (This means that for almost all points $p \in V$ we have $Q_i(p) \neq 0$ for all i. We say that the rational map F is defined at such points p.)

(2) For each point p where F is defined, and for all polynomials $g(x_1, \ldots, x_m) \in J$, we have

$$g\left(\frac{P_1(x_1, \ldots, x_n)}{Q_1(x_1, \ldots, x_n)}, \ldots, \frac{P_m(x_1, \ldots, x_n)}{Q_m(x_1, \ldots, x_n)}\right) = 0.$$

Thus a rational map from V to W sends almost all points of V to points in W.

Exercise 4.18.2. Show that the rational map

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

is a rational map from the line $\mathbb{C}$ to the circle $V(x^2 + y^2 - 1)$. Find the points on the line $\mathbb{C}$ where F is not well-defined.

Exercise 4.18.3. The above rational map $F(t) = \left(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$ was not made up out of thin air but reflects an underlying geometry. Let L be any line in the plane $\mathbb{C}^2$ through the point $(0, 1)$ with slope t. Then the equation for this line is $y = tx + 1$. First, draw a picture in $\mathbb{R}^2$ of the circle $V(x^2 + y^2 - 1)$ and the line L. Using the quadratic equation, show that the two points of intersection are $(0, 1)$ and $\left(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$, for a fixed slope t. Explain the underlying geometry of the map F for when the slope t is zero.

4.18.2. Birational Equivalence.

Definition 4.18.3. An algebraic variety $V \subset \mathbb{A}^n(k)$ is *birationally equivalent* to an algebraic variety $W \subset \mathbb{A}^m(k)$ if there are rational maps

$$F : V \dashrightarrow W$$

and

$$G : W \dashrightarrow V$$

such that the compositions

$$G \circ F : V \dashrightarrow V$$

and

$$F \circ G : W \dashrightarrow W$$

are one-to-one functions, where defined. We then say that V and W are *birational*. The rational map G is called the *inverse* of the map F.

Intuitively two varieties are birational if they are actually isomorphic, save possibly off of certain proper subvarieties.

EXERCISE 4.18.4. Show that the complex line $\mathbb{C}$ is birational to the circle $V(x^2+y^2-1)$ by finding an inverse to the rational map $F(t) = \left(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$. Thus you must find a rational map

$$G(x,y) = \frac{P(x,y)}{Q(x,y)}$$

such that for all but finitely many $(x,y) \in V(x^2+y^2-1)$,we have

$$(x,y) = \left(\frac{-2\frac{P(x,y)}{Q(x,y)}}{1+(\frac{P(x,y)}{Q(x,y)})^2}, \frac{1-(\frac{P(x,y)}{Q(x,y)})^2}{1+(\frac{P(x,y)}{Q(x,y)})^2} \right) = F \circ G(x,y)$$

and for all but finitely many t we have

$$t = \frac{P(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2})}{Q(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2})} = G \circ F(x,y)$$

As a hint, recall that the map F corresponds geometrically with starting with a slope t for the line $y = tx + 1$ through the point $(0,1)$ and then finding the line's second point of intersection with the circle.

EXERCISE 4.18.5. Consider the curve $V(y^2 - x^3)$ in the plane $\mathbb{C}^2$.

Picture

(1) Show that this curve has a singular point at the origin $(0,0)$
(2) Show that the map $F(t) = (t^2, t^3)$ maps the complex line $\mathbb{C}$ to the curve $V(y^2 - x^3)$.
(3) Find a rational map $G : V(y^2 - x^3) \dashrightarrow \mathbb{C}$ that is the inverse to the map F

Thus $\mathbb{C}$ and $V(y^2 - x^3)$ are birational, even though $\mathbb{C}$ is smooth and $V(y^2 - x^3)$ is singular.

4.18.3. Birational Equivalence and Field Isomorphisms. The goal is

THEOREM 4.18.6. Let $V = V(I) \subset \mathbb{A}^n(k)$ and $W = W(J) \subset \mathbb{A}^m(k)$ be two algebraic varieties. Then V and W are birational if and only if the function fields $\mathcal{K}_V$ and $\mathcal{K}_W$ are field isomorphic.

Fields being isomorphic is a natural algebraic notion of equivalence. Thus the intuition behind this theorem is that birational equivalence precisely corresponds to the corresponding function fields being isomorphic.

EXERCISE 4.18.7. The goal of this exercise is to show that the function fields for the line $\mathbb{C}$ and the curve $V(y^2 - x^3)$ in the plane $\mathbb{C}^2$ are field isomorphic.

(1) Show that $y = \left(\frac{y}{x}\right)^3$ and $x = \left(\frac{y}{x}\right)^2$ in the field $\mathbb{C}(x, y)/(y^2 - x^3)$.
(2) Show that for any $F(x, y) \in \mathbb{C}(x, y)/(y^2-x^3)$, there exists two one-variable polynomials $P(t), Q(t) \in \mathbb{C}[t]$ such that
$$F(x, y) = \frac{P\left(\frac{y}{x}\right)}{Q\left(\frac{y}{x}\right)}$$
in the field $\mathbb{C}(x, y)/(y^2 - x^3)$.
(3) Show that the map
$$T : \mathbb{C}(t) \to \mathbb{C}(x, y)/(y^2 - x^3)$$
defined by setting
$$Tf(t) = f\left(\frac{y}{x}\right)$$
is onto.
(4) Show that the above map T is one-to-one. This part of the problem is substantially harder than the first three parts. Here are some hints. We know for a field morphism that one-to-one is equivalent to the kernel being zero. Let $P(t), Q(t) \in \mathbb{C}([t]$ be polynomials such that
$$T\left(\frac{P(t)}{Q(t)}\right) = 0$$
in $\mathbb{C}(x, y)/(y^2 - x^3)$. Now concentrate on the numerator and use that $(y^2 - x^3)$ is a prime ideal in the ring $\mathbb{C}[x, y]$.

The next series of exercises will provide a proof that algebraic varieties V and W are birational if and only if the function fields $\mathcal{K}_V$ and $\mathcal{K}_W$ are isomorphic.

EXERCISE 4.18.8. For algebraic varieties V and W, consider the rational map
$$F : V \dashrightarrow W$$
given by
$$F(x_1, \ldots, x_n) = \left(\frac{P_1(x_1, \ldots, x_n)}{Q_1(x_1, \ldots, x_n)}, \ldots, \frac{P_m(x_1, \ldots, x_n)}{Q_m(x_1, \ldots, x_n)}\right).$$

Show that there is a natural map

$$F^*\mathcal{K}_W \to \mathcal{K}_V.$$

EXERCISE 4.18.9. Let

$$F : V \dashrightarrow W \text{ and } G : W \dashrightarrow V$$

be two rational maps. Then $G \circ F : V \dashrightarrow V$ is a rational map from V to V, Show that

$$(G \circ F)^* : \mathcal{K}_V \to \mathcal{K}_V$$

equals

$$F^* \circ G^* : \mathcal{K}_V \to \mathcal{K}_V.$$

EXERCISE 4.18.10. Let

$$F : V \dashrightarrow W \text{ and } G : W \dashrightarrow V$$

be two rational maps. Suppose that

$$(G \circ F)^* = \text{Identity map on } \mathcal{K}_V$$

and

$$(F \circ G)^* = \text{Identity map on } \mathcal{K}_W$$

Show that

$$F^* : \mathcal{K}_W \dashrightarrow \mathcal{K}_V$$

and

$$G^* : \mathcal{K}_V \dashrightarrow \mathcal{K}_W$$

are one-to-one and onto.

4.18.4. Blow-ups and rational maps. In section XXX we saw that the blow-up of the origin $(0, 0)$ in $\mathbb{C}^2$ is the replacing the origin by the set of all complex lines in $\mathbb{C}^2$ through the origin. In coordinates, the blow-up consists of two copies of $\mathbb{C}^2$ that are patched together correctly. This section shows how these patchings can be viewed as appropriate birational maps.

Let $U = \mathbb{C}^2$, with coordinates u_1, u_2, and $V = \mathbb{C}^2$, with coordinates v_1, v_2 be the two complex planes making up the blow-up. Denote by $Z = \mathbb{C}^2$, with coordinates z_1, z_2, the original $\mathbb{C}^2$ whose origin is to be blown-up.

From section XX, we have the maps polynomial maps

$$\pi_1 : U \to Z \quad \text{and} \quad \pi_2 : V \to Z$$

given by

$$\pi_1(u_1, u_2) = (u_1, u_1u_2) = (z_1, z_2)$$

and

$$\pi_2(v_1, v_2) = (v_1v_2, v_2) = (z_1, z_2).$$

EXERCISE 4.18.11. Find the inverse maps

$$\pi_1^{-1} : Z \dashrightarrow U \text{ and } \pi_2^{-1} : Z \dashrightarrow V.$$

Find the points Z where the maps π_1^{-1} and π_2^{-1} are not defined. Show that U and Z are birational, as are V and Z.

EXERCISE 4.18.12. Find the maps

$$\pi_2^{-1} \circ \pi_1 : U \dashrightarrow V$$

and

$$\pi_1^{-1} \circ \pi_2 : V \dashrightarrow U.$$

Show that U and V are birational.

4.19. Products of Affine Varieties

The goal of this section is to show that the Cartesian product of affine varieties is again an affine variety. We also study the topology and function theory of the product of two affine varieties.

4.19.1. Product of affine spaces. In analytic geometry, the familiar xy-plane, $\mathbb{R}^2$, is constructed as the Cartesian product of two real lines, $\mathbb{R}\times\mathbb{R}$, and thus is coordinatized by ordered pairs of real numbers. It is natural to ask whether the same construction can be used in algebraic geometry to construct higher-dimensional affine spaces as products of lower-dimensional ones.

Clearly we can identify $\mathbb{A}^2(k)$ with $\mathbb{A}^1(k) \times \mathbb{A}^1(k)$ as sets. However, this identification is insufficient to prove that $\mathbb{A}^2(k)$ is isomorphic to $\mathbb{A}^1(k) \times \mathbb{A}^1(k)$, for isomorphisms must also take into account the topologies and functions for each.

EXERCISE 4.19.1. Let $k[\mathbb{A}^n(k)] = k[x_1, \ldots, x_n]$ and $k[\mathbb{A}^m(k)] = k[y_1, \ldots, y_m]$. Show that $k[\mathbb{A}^{n+m}] \cong k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, where the latter is, by definition, the ring of regular functions on the product $\mathbb{A}^n(k) \times \mathbb{A}^m(k)$.

Frequently, when we form the product of topological spaces X and Y, the new space $X \times Y$ is endowed with the product topology. This topology has as its basis all sets of the form $U \times V$ where $U \subset X$ and $V \subset Y$ are open. In these exercises, the Zariski topology on the product $X \times Y$ will be compared to the product topology to determine if they are the same or different (and if different, which is finer).

EXERCISE 4.19.2. (This is very similar to [Hartshorne1977], Exercise I.1.4.) In Exercise 1, you have shown that $\mathbb{A}^n(k) \times \mathbb{A}^m(k) \cong \mathbb{A}^{n+m(k)}$. In particular, $\mathbb{A}^1(k) \times \mathbb{A}^1(k) \cong \mathbb{A}^2(k)$.

(1) Describe an open set in the product topology on $\mathbb{A}^1(k) \times \mathbb{A}^1(k)$.

(2) Is an open set in the product topology on $\mathbb{A}^1(k) \times \mathbb{A}^1(k)$ also open in the Zariski topology of $\mathbb{A}^1(k) \times \mathbb{A}^1(k) \cong \mathbb{A}^2(k)$?
(3) Is every open set of the Zariski topology of $\mathbb{A}^1(k) \times \mathbb{A}^1(k) \cong \mathbb{A}^2$ also open in the product topology?
(4) Conclude that the Zariski topology is *strictly finer* than the product topology on $\mathbb{A}^1(k) \times \mathbb{A}^1(k) \cong \mathbb{A}^2(k)$.

4.19.2. Product of affine varieties. Let $X \subset \mathbb{A}^n(k)$ and $Y \subset \mathbb{A}^m(k)$ be affine varieties. The Cartesian product of X and Y, $X \times Y$, can naturally be viewed as a subset of the Cartesian product $\mathbb{A}^n(k) \times \mathbb{A}^m(k)$.

EXERCISE 4.19.3. Let $X = V(x_2 - x_1) \subset \mathbb{A}^2(k)$ and $Y = V(y_1) \subset \mathbb{A}^2(k)$. Describe $X \times Y$ and show that it is a closed subset of $\mathbb{A}^4(k)$.

EXERCISE 4.19.4. If $X = V(I) \subset \mathbb{A}^n(k)$ and $Y = V(J) \subset \mathbb{A}^m(k)$ are algebraic sets, show that $X \times Y \subset \mathbb{A}^{n+m}(k)$ is also an algebraic set.

Let $X \subset \mathbb{A}^n(k)$ and $Y \subset \mathbb{A}^m(k)$ be affine subvarieties. Then $X \times Y$ is an algebraic subset of $\mathbb{A}^{n+m}(k)$. Endow $X \times Y$ with the subspace topology for the Zariski topology on $\mathbb{A}^{n+m}(k)$. This is called the **product** of the affine varieties X and Y.

We now want to prove that the product of affine varieties is again an affine variety, which requires that we prove the product of irreducible sets is irreducible.

EXERCISE 4.19.5. Let $x_0 \in X$ be a (closed) point. Show that $\{x_0\} \times Y = \{(x_0, y) \in X \times Y : y \in Y\}$ is a subvariety of $X \times Y$ isomorphic to Y as a variety. Similarly, for any closed point $y_0 \in Y$, $X \times \{y_0\}$ is a subvariety of $X \times Y$ isomorphic to X.

In particular, if X is irreducible, so is $X \times \{y_0\}$ for each $y_0 \in Y$.

EXERCISE 4.19.6. If X and Y are irreducible, show that $X \times Y$ is irreducible.

Thus, if X and Y are affine varieties, so is their product, $X \times Y$.

4.19.3. Products and morphisms.

EXERCISE 4.19.7. Let $X \subset \mathbb{A}^n(k)$ and $Y \subset \mathbb{A}^m(k)$ be affine varieties.

(1) Show that $(x, y) \mapsto x$ is a morphism of affine varieties $\rho_X : X \times Y \to X$, called projection on the first factor.
(2) Similarly, show that $(x, y) \mapsto y$ is a morphism, which we will denote by $\rho_Y : X \times Y \to Y$ and call projection on the second factor.

EXERCISE 4.19.8. Show that $\rho_X : X \times Y \to X$ and $\rho_Y : X \times Y \to Y$ are both *open morphisms*, i.e., if $U \subset X \times Y$ is an open subset, then $\rho_X(U)$ is an open subset of X and $\rho_Y(U)$ is an open subset of Y.

Must ρ_X and ρ_Y also be *closed morphisms*, i.e., must the images of a closed set C in $X \times Y$ be closed in X and in Y?

EXERCISE 4.19.9. Suppose $\varphi : Z \to X$ and $\psi : Z \to Y$ are morphisms of affine varieties. Show that there is a well-defined morphism $\pi : Z \to X \times Y$ so that $\varphi = \rho_X \circ \pi$ and $\psi = \rho_Y \circ \pi$, where $\rho_X : X \times Y \to X$ and $\rho_Y : X \times Y \to Y$ are the projection morphisms.

This is the *universal property* for the product of varieties: Given X and Y, a variety P with morphisms $\pi_X : P \to X$ and $\pi_Y : P \to Y$ is the **product** of X and Y if, for any variety Z with morphisms $\alpha : Z \to X$ and $\beta : Z \to Y$, there is a unique morphism $\gamma : Z \to P$ so that

$$\begin{tikzcd} Z \arrow[dr, dotted, "\gamma"] \arrow[drr, bend left, "\beta"] \arrow[ddr, bend right, "\alpha"'] & & \\ & P \arrow[r, "\pi_Y"'] \arrow[d, "\pi_X"] & Y \\ & X & \end{tikzcd}$$

is a commutative diagram.

Therefore, if Q is another variety having this property, there are unique maps $\delta : P \to Q$, $\zeta : Q \to P$, $\pi : P \to P$ and $\varepsilon : Q \to Q$ by the universal property. Clearly, π, ε must both be the identity morphisms of P and Q, respectively. However, $\zeta \circ \delta : P \to P$ also satisfies the property of the arrow from P to itself, so that $\zeta \circ \delta = \pi$ is the identity on P. Similarly, $\delta \circ \zeta : Q \to Q$ is the identity morphism of Q, so ζ and δ are invertible morphisms which establish an isomorphism $P \cong Q$. Hence the product of two varieties is unique up to isomorphism.

EXERCISE 4.19.10. Suppose $\pi : X \times Y \to Z$ is a morphism. Must there be morphisms $\xi : X \to Z$ and $\eta : Y \to Z$ such that $\pi = \xi \circ \rho_X$ and $\pi = \eta \circ \rho_Y$? That is, must we always be able to complete the following commutative diagram?

$$\begin{tikzcd} X \times Y \arrow[r, "\rho_Y"] \arrow[d, "\rho_X"'] \arrow[dr, "\pi"] & Y \arrow[d, dotted, "\eta"] \\ X \arrow[r, dotted, "\xi"'] & Z \end{tikzcd}$$

EXERCISE 4.19.11. Suppose $\xi : X \to Z$ and $\eta : Y \to Z$ are morphisms of affine varieties. Is there is a well-defined morphism $\zeta : X \times Y \to Z$ induced by ξ and η?

CHAPTER 5

Projective Varieties

The key to this chapter is that projective space $\mathbb{P}^n$ is the natural ambient space for much of algebraic geometry. We will be extending last chapter's work on affine varieties to the study of algebraic varieties in projective space $\mathbb{P}^n$. We will see that in projective space we can translate various geometric objects into the language not of rings but that of graded rings. Instead of varieties corresponding to ideals in commutative rings, we will show that varieties in $\mathbb{P}^n$ will correspond to homogeneous ideals. This will allow us to define the notion of "projective isomorphisms."

5.1. Definition of Projective n-space $\mathbb{P}^n(k)$

In Chapter 1, we saw that all smooth conics in the complex projective plane $\mathbb{P}^2$ can be viewed as the "same". In Chapter 2, we saw that all smooth cubics in $\mathbb{P}^2$ can be viewed as describing toruses. In Chapter 3, we saw that curves of degree e and curves of degree f must intersect in exactly ef points, provided we work in $\mathbb{P}^2$. All of this suggests that affine space $\mathbb{A}^n$ is not the natural place to study geometry; instead, we want to define some notion of projective n- space.

Let k be a field. (You can comfortably replace every k with the complex numbers $\mathbb{C}$, at least for most of this book.)

Definition 5.1.1. Let $a = (a_0, \ldots, a_n), b = (b_0, \ldots, b_n) \in \mathbb{A}^n(k) - (0, \ldots, 0)$. We say that *$a$ is equivalent to b*, denoted $a \sim b$, if there exists a $\lambda \neq 0$ in the field k such that

$$(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n).$$

Exercise 5.1.1. In $\mathbb{A}^5 - (0, \ldots, 0)$, show

(1) $(1,3,2,4,5) \sim (3,9,6,12,15)$
(2) $(1,3,2,4,5) \not\sim (3,9,6,13,15)$

Exercise 5.1.2. Show that the above '$\sim$' is an equivalence relation on $\mathbb{A}^n(k) - (0, \ldots, 0)$, meaning that for all $a, b, c \in \mathbb{A}^n(k) - (0, \ldots, 0)$ we have

(1) $a \sim a$.
(2) If $a \sim b$ then $b \sim a$.
(3) If $a \sim b$ and $b \sim c$, then $a \sim c$

DEFINITION 5.1.2. Projective n-space over the field k is

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

EXERCISE 5.1.3. Referring back to Exercise 1.4.7, explain why $\mathbb{P}^n(k)$ can be thought of as the set of all lines through the origin in $\mathbb{A}^{n+1}(k)$.

We denote the equivalence class corresponding to a point $(a_0, \ldots, a_n)$ (with at least one $a_i \neq 0$ by

$$(a_0 : a_1 : \cdots : a_n).$$

We call the $(a_0 : a_1 : \cdots : a_n)$ the *homogeneous coordinates* for $\mathbb{P}^n(k)$.

We now want to exampine the relationship between $\mathbb{A}^n(k)$ and $\mathbb{P}^n(k)$. There is a natural way, to consider $\mathbb{P}^n$ as $n+1$ copies of $\mathbb{A}^n(k)$.

EXERCISE 5.1.4. Let $(a_0, a_1, a_2, a_3, a_4, a_5) \in \mathbb{P}^5$. Suppose that $a_0 \neq 0$. Show that

$$(a_0, a_1, a_2, a_3, a_4, a_5) \sim \left(1, \frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}, \frac{a_4}{a_0}, \frac{a_5}{a_0}\right).$$

DEFINITION 5.1.3. Let $(x_0 : x_1 : \cdots : x_n)$ be homogeneous coordinates on $\mathbb{P}^n$. Define the i^{th} *affine chart* to be

$$\begin{aligned} U_i &= \mathbb{P}^n \backslash V(x_i) \\ &= \{(x_0 : x_1 : \cdots : x_n) : x_i \neq 0\}. \end{aligned}$$

EXERCISE 5.1.5. Prove that every element in $\mathbb{P}^n(k)$ is contained in at least one U_i. (Thus the $(n+1)$ sets U_i, for $i = 0, \ldots, n$, will cover $\mathbb{P}^n(k)$.)

EXERCISE 5.1.6. Show that there is exactly one point in $\mathbb{P}^n(k)$ that is not in $U_1, U_2, \ldots, U_n$. Identify this point.

In the affine case, there is a natural way to link spaces with different dimensions: $\mathbb{A}^n$ can be embedded in $\mathbb{A}^{n+1}$ by mapping an n-tuple to an $(n+1)$-tuple with the last coordinate set equal to 0. Let's extend this so we can inbed a orojective space into a higher dimensional one.

EXERCISE 5.1.7. Show that we can map $\mathbb{P}^1(k)$ to the set of all points in $\mathbb{P}^n(k)$ that are not in $U_2, U_3, \ldots, U_n$.

EXERCISE 5.1.8. Show that we can map $\mathbb{P}^2(k)$ to the set of all points in $\mathbb{P}^n(k)$ that are not in $U_3, U_4, \ldots, U_n$.

Since there are $n+1$ copies of $\mathbb{A}^n$ embedded in $\mathbb{P}^n$, we need a way to move from one chart to another.

DEFINITION 5.1.4. For $0 \leq i \leq n$, define maps $\phi_i : U_i \to \mathbb{A}^n(k)$ by

$$\phi_i(x_0 : x_1 : \cdots : x_n) = \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \widehat{x_i}, \ldots, \frac{x_n}{x_i}\right),$$

where $\widehat{x_i}$ means that x_i is omitted.

EXERCISE 5.1.9. For $\mathbb{P}^n(k)$, show for each i that $\phi_i : U_i \to \mathbb{A}^n$ is

(1) one-to-one
(2) onto.

Since ϕ_i is one-to-one and onto, there is a well- defined inverse

$$\phi_i^{-1} : \mathbb{A}^n(k) \to \mathbb{P}^n(k).$$

EXERCISE 5.1.10. For $\phi_2^{-1} : \mathbb{A}^5(k) \to \mathbb{P}^5(k)$, show that

$$\phi_2^{-1}(7, 3, 11, 5, 6) = (14 : 6 : 2 : 22 : 10 : 12).$$

EXERCISE 5.1.11. Define maps $\psi_{ij} : \phi_j(U_i \cap U_j) \to \phi_i(U_i \cap U_j)$ by $\psi_{ij} = \phi_i \circ \phi_j^{-1}$. Explain how this is a map from $\mathbb{A}^n$ to $\mathbb{A}^n$.

EXERCISE 5.1.12. Show that the map $\psi_{02} : \mathbb{A}^2 \to \mathbb{A}^2$ is

$$\psi_{02}(x_1, x_2) = \left(\frac{x_2}{x_1}, \frac{1}{x_1}\right).$$

Describe the set on which ψ_{02} is undefined.

EXERCISE 5.1.13. Explicitly describe $\psi_{12} : \mathbb{A}^2 \to \mathbb{A}^2$. In other words, find $\psi_{12}(x_1, x_2)$. Describe the set on which ψ_{12} is undefined.

EXERCISE 5.1.14. Write explicitly the map $\psi_{02} : \phi_2(U_0 \cap U_2) \subset \mathbb{A}^n \to \phi_0(U_0 \cap U_2) \subset \mathbb{A}^n$ in coordinates $(x_1, x_2, \ldots, x_n)$. Describe the set on which ψ_{02} is undefined.

EXERCISE 5.1.15. Show that $\psi_{ij} \circ \psi_{jk} = \psi_{ik}$.

EXERCISE 5.1.16. Show that $\psi_{ij} \circ \psi_{jk} \circ \psi_{ki} = 1$

For those who have had topology, the above exercises show that $\mathbb{P}^n$ is a manifold.

We are not interested, though, in $\mathbb{P}^n(k)$, save as a place in which to do geometry. We want to see why we cannot naively look at zero loci of polynomials in $\mathbb{P}^n(k)$.

EXERCISE 5.1.17. Let

$$P(x_0, x_1, x_2, x_3, x_4, x_5) = x_0 - x_1x_2x_3x_4x_5.$$

(1) Show that

$$P(1, 1, 1, 1, 1, 1) = 0.$$

(2) Show that
$$P(2,2,2,2,2,2) \neq 0.$$
(3) Show that
$$(1,1,1,1,1,1) \sim (2,2,2,2,2,2)$$
so that the two points will define the same point in $\mathbb{P}^5$.
(4) Conclude that the set $\{(x_0,\ldots,x_5) \in \mathbb{P}^5 : P(x_0,\ldots,x_5) = 0\}$ is not a well-defined set.

As we have seen before, the key is to consider a special subset of polynomials.

EXERCISE 5.1.18. Let
$$P(x_0,x_1,x_2,x_3,x_4,x_5) = x_0^5 - x_1x_2x_3x_4x_5.$$
(1) Show that
$$P(1,1,1,1,1,1) = 0.$$
(2) Show that
$$P(2,2,2,2,2,2) = 0.$$
(3) Show that if $P(x_0,\ldots,x_5) = 0$, then for all $\lambda \in \mathbb{C}$ we have
$$P(\lambda x_0,\ldots,\lambda x_5) = 0.$$
(4) Conclude that the set $\{(x_0,\ldots,x_5) \in \mathbb{P}^5 : P(x_0,\ldots,x_5) = 0\}$ is a well-defined set.

The reason why the zero locus of $x_0^5 - x_1x_2x_3x_4x_5$ is a well- define subset of $\mathbb{P}^5$ is that both terms x_0^5 and $x_1x_2x_3x_4x_5$ have degree five.

DEFINITION 5.1.5. A polynomial for which each of its terms has the same degree is called *homogeneous*.

The next section starts the algebraic development of homogeneous polynomials, which will allow us to apply algebraic geometry in projective space.

5.2. Graded Rings and Homogeneous Ideals

Exercises 5.1.17 and 5.1.18 suggest that we should consider only homogenous polynomials (Definition 1.4.3) to do algebraic geometry in projective space. It is easy to show:

EXERCISE 5.2.1. If $f \in k[x_0,\ldots,x_n]$ is a homogeneous polynomial of degree d, then $f(\lambda x_0, \lambda x_1,\ldots,\lambda x_n) = \lambda^d f(x_0,x_1,\ldots,x_n)$ for every $\lambda \neq 0$ in the base field k.

Thus, even though the value of f at a point $P \in \mathbb{P}^n$ is not well defined, the points, P, at which f vanishes are well defined. Hence, we restrict our attention to the zero locus of homogeneous polynomials when working in projective space $\mathbb{P}^n$.

First, we notice that when we work with homogeneous polynomials we gain additional structure on the ring $k[x_0, x_1, \ldots, x_n]$. We prove we can break up, in a natural way, the polynomial ring $k[x_0, x_1, \ldots, x_n]$. Define R_d to be the set of all homogeneous polynomials of degree d in $k[x_0, x_1, \ldots, x_n]$.

Exercise 5.2.2. Let $R = k[x, y, z]$.

(1) Let $f = x + 2y$ and $g = x - z$. Show $f + g$ and $f - g$ are in R_1 and $fg \in R_2$.
(2) Let $h = x^2 + yz$. Show fh and gh are in R_3 and $h^2 \in R_4$.

Exercise 5.2.3. Let $R = k[x_0, x_1, \ldots, x_n]$.

(1) What is R_0?
(2) Show that if $f \in R_0$ and $g \in R_d$, then $fg \in R_d$.
(3) Show that for $f, g \in R_1$, $f + g \in R_1$ and $fg \in R_2$.
(4) Show that for $f, g \in R_d$, $f + g \in R_d$ and $fg \in R_{2d}$.

We can generalize exercises 5.2.2 and 5.2.3 to show that $k[x_0, x_1, \ldots, x_n]$ is a *graded* ring.

Definition 5.2.1. A graded ring is a ring R together with a collection of subgroups R_d, $d \geq 0$, of the additive group R, such that $R = \bigoplus_{d \geq 0} R_d$ and for all $d, e \geq 0$, $R_d \cdot R_e \subseteq R_{d+e}$.

Exercise 5.2.4. As before, let $R = k[x_0, x_1, \ldots, x_n]$ with R_d the homogeneous polynomials of degree d.

(1) Prove that R_d is a group under addition.
(2) Prove for any $d, e \geq 0$, $R_d \cdot R_e \subseteq R_{d+e}$.
(3) Prove $k[x_0, x_1, \ldots, x_n] = \bigoplus_{d \geq 0} R_d$.

This notion of grading of a ring extends to ideals in the ring. Since we are interested in projective space and hence homogeneous polynomials, we define the related notion of a graded ideal.

Definition 5.2.2. An ideal I of a graded ring $R = \bigoplus_{d \geq 0} R_d$ is called *homogeneous* or *graded* if and only if $I = \bigoplus (I \cap R_d)$.

Exercise 5.2.5. Determine whether each ideal of $k[x, y, z]$ is homogeneous.

(1) $I(P) = \{f \mid f(P) = 0\}$ where f is a homogeneous polynomial
(2) $\langle x - yz \rangle$
(3) $\langle x^2 - yz \rangle$

(4) $\langle x - yz, x^2 - yz \rangle$

(5) $\langle x^2 - yz, y^3 - xz^2 \rangle$

The next exercise gives us two alternate descriptions for a homogeneous ideal.

EXERCISE 5.2.6. Prove that the following are equivalent.

(1) I is a homogeneous ideal of $k[x_0, \ldots, x_n]$.

(2) I is generated by homogeneous polynomials.

(3) If $f = \sum f_i \in I$, where each f_i is homogeneous, then $f_i \in I$ for each i.

The exercises in the rest of this section provide practice working with and general results about graded rings.

EXERCISE 5.2.7. Let I be a homogeneous ideal in $R = k[x_0, \ldots, x_n]$. Prove the quotient ring R/I is a graded ring.

EXERCISE 5.2.8. Let $R = k[x, y, z]$ and $I = \langle x^2 - yz \rangle$. Show how to write R/I as a graded ring $\bigoplus R_d$.

EXERCISE 5.2.9. Let $R = k[x, y, z, w]$ and $I = \langle xw - yz \rangle$. Show how to write R/I as a graded ring $\bigoplus R_d$.

EXERCISE 5.2.10. Let $R = k[x, y, z]$ and let $I = \langle x, y \rangle$, $J = \langle x^2 \rangle$. Determine whether each ideal is homogeneous.

(1) $I \cap J$

(2) $I + J$

(3) IJ

(4) $\mathrm{Rad}(I)$

(Recall that the radical of I is the ideal $\mathrm{Rad}(I) = \{f : f^m \in I \text{ for some } m > 0\}$.)

We can generalize these results to the intersections, sums, products, and radicals of any homogeneous ideals.

EXERCISE 5.2.11. Let I and J be homogeneous ideals in $k[x_0, \ldots, x_n]$.

(1) Prove $I \cap J$ is homogeneous.

(2) Prove $I + J$ is homogeneous.

(3) Prove IJ is homogeneous.

(4) Prove $\mathrm{Rad}(I)$ is homogeneous.

We will see that, as in the affine case, prime ideals correspond to irreducible varieties. The next exercise shows that to prove a homogeneous ideal is prime, it is sufficient to restrict to homogeneous elements.

EXERCISE 5.2.12. Let I be a homogeneous ideal in $R = k[x_0, \ldots, x_n]$. Prove that I is a prime ideal if and only if $fg \in I$ implies $f \in I$ or $g \in I$ for all homogeneous polynomials f, g.

5.3. Projective Varieties

In chapter 4, we studied algebraic varieties in affine space, $\mathbb{A}^n$. We did not deal with homogeneous polynomials and ideals. In this section we will see that the $V - I$ correspondence for affine varieties developed in chapter 4 extends to projective varieties. In order for this to work, there is a need to require that the set S be a set of homogeneous polynomials.

5.3.1. Algebraic Sets. To define varieties in $\mathbb{P}^n$, we start with the zero sets of homogeneous polynomials.

Definition 5.3.1. Let S be a set of homogeneous polynomials in $k[x_0, \ldots, x_n]$. The zero set of S is $V(S) = \{P \in \mathbb{P}^n \mid f(P) = 0\ \forall f \in S\}$. A set X in $\mathbb{P}^n$ is called an *algebraic set* if it is the zero set of some set of homogeneous polynomials.

Exercise 5.3.1. Describe the zero sets $V(S)$ in $\mathbb{P}^2$ for each set S.

(1) $S = \left\{x^2 + y^2 - z^2\right\}$.
(2) $S = \left\{x^2, y\right\}$.
(3) $S = \left\{x^2 + y^2 - z^2, x^2 - y^2 + z^2\right\}$.

Exercise 5.3.2. Describe the algebraic sets in $\mathbb{P}^1$.

Exercise 5.3.3. Show that each set of points X is an algebraic set by finding a set of polynomials S so that $X = V(S)$.

(1) $X = \{(0 : 1)\} \subset \mathbb{P}^1$.
(2) $X = \{(0 : 0 : 1), (0 : 1 : 0), (1 : 0 : 0)\} \subset \mathbb{P}^2$.
(3) $X = \{(1 : 1 : 1 : 1)\} \subset \mathbb{P}^3$.

While in this book we are interested in varieties over $\mathbb{C}$, it is interesting to see how the algebraic sets vary when we vary the base field k.

Exercise 5.3.4. Let $I = \langle x^2 + y^2 \rangle \subset k[x, y]$.

(1) Find $V(I)$ for $k = \mathbb{C}$.
(2) Find $V(I)$ for $k = \mathbb{R}$.
(3) Find $V(I)$ for $k = \mathbb{Z}_2$.

Exercise 5.3.5. Let S be a set of homogeneous polynomials and let I be the ideal generated by the elements in S. Prove that $V(I) = V(S)$. This shows that every algebraic set is the zero set of a homogeneous ideal.

Exercise 5.3.6. Prove that every algebraic set is the zero set of a finite number of homogeneous polynomials. (The Hilbert Basis Theorem (check section in chapter 4) will be useful here.)

EXERCISE 5.3.7. We call the ideal $\langle x_0, x_1, \ldots, x_n \rangle \subset k[x_0, x_1, \ldots, x_n]$ the "irrelevant" maximal ideal of $k[x_0, x_1, \ldots, x_n]$. Prove that this is a maximal ideal and describe $V(\langle x_0, x_1, \ldots, x_n \rangle)$. Why do we say that $\langle x_0, x_1, \ldots, x_n \rangle$ is irrelevant?

EXERCISE 5.3.8. Let I and J be homogeneous ideals in $R = k[x_0, x_1, \ldots, x_n]$.

(1) Prove $V(I \cap J) = V(I) \cup V(J)$.
(2) Prove $V(I + J) = V(I) \cap V(J)$.

EXERCISE 5.3.9. Let I be a homogeneous ideal. Prove that $V(\mathrm{Rad}(I)) = V(I)$.

5.3.2. Ideals of algebraic sets.

DEFINITION 5.3.2. Let V be an algebraic set in $\mathbb{P}^n$. The ideal of V is

$$I(V) = \{f \in k[x_0, \ldots, x_n] \mid f \text{ is homogeneous, } f(P) = 0 \text{ for all } P \in V\}.$$

EXERCISE 5.3.10. Let V be an algebraic set in $\mathbb{P}^n$. Prove that $I(V)$ is a homogeneous ideal.

EXERCISE 5.3.11. Find the ideal $I(S)$ for each projective algebraic set S.

(1) $S = \{(1:1)\}$ in $\mathbb{P}^1$.
(2) $S = V(\langle x^2 \rangle)$ in $\mathbb{P}^2$.
(3) $S = V(\langle x_0x_2 - x_1x_3, x_0 - x_3 \rangle)$ in $\mathbb{P}^3$.

In chapter 4 we proved Hilbert's Nullstellensatz: for an affine algebraic variety $V(I)$ over an algebraically closed field k, $I(V(I)) = \mathrm{Rad}(I)$. To prove the projective version of this result, we will compare the corresponding projective and affine ideals and varieties. For a homogeneous ideal $J \subseteq k[x_0, \ldots, x_n]$, let

$$V_a(J) = \left\{P \in \mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\} : f(P) = 0 \ \forall f \in J\right\},$$

the affine zero set of the ideal J.

EXERCISE 5.3.12. Let J be a homogeneous ideal in $k[x_0, \ldots, x_n]$.

(1) Let $\varphi : \mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\} \to \mathbb{P}^n$ be the map
$$\varphi((a_0, \ldots, a_n)) = (a_0 : \cdots : a_n).$$
Describe $\varphi^{-1}(a_0 : \cdots : a_n)$.
(2) Prove that $(a_0, \ldots, a_n) \in V_a(J)$ if and only if $(\lambda a_0, \ldots, \lambda a_n) \in V_a(J)$ for all $\lambda \in k^*$.
(3) Let $I(V_a(J)) = \{f \in k[x_0, \ldots, x_n] : f(P) = 0 \ \forall P \in V_a(J)\}$ the ideal of polynomials vanishing on the affine variety $V_a(J)$. Note that we do not require the polynomials in $I(V_a(J))$ to be homogeneous, since $V_a(J)$ is an affine variety. Prove that $I(V_a(J))$ is in fact homogeneous, and $I(V_a(J)) = I(V(J))$.

(4) Use Hilbert's Nullstellensatz to conclude that $I(V(J)) = \text{Rad}(J)$.

EXERCISE 5.3.13. Let $J = \langle x_0 - x_1 \rangle \subseteq k[x_0, x_1]$.

(1) Find the affine zero set $V_a(J) \subset \mathbb{A}^2$.
(2) Find $I(V_a(J))$ and show that this ideal is homogeneous.
(3) Show that $I(V(J)) = \text{Rad}(J)$.

EXERCISE 5.3.14. Let $J = \langle x_0 - x_1, x_1 + x_2 \rangle \subseteq k[x_0, x_1, x_2]$.

(1) Find the affine zero set $V_a(J) \subset \mathbb{A}^3$.
(2) Find $I(V_a(J))$ and show that this ideal is homogeneous.
(3) Show that $I(V(J)) = \text{Rad}(J)$.

EXERCISE 5.3.15. Let $J = \langle x_0x_2, x_0x_2, x_1x_2 \rangle \subseteq k[x_0, x_1, x_2]$.

(1) Find the affine zero set $V_a(J) \subset \mathbb{A}^3$.
(2) Find $I(V_a(J))$ and show that this ideal is homogeneous.
(3) Show that $I(V(J)) = \text{Rad}(J)$.

EXERCISE 5.3.16. Let I be a homogeneous ideal. Prove that $V(I) = \emptyset$ if and only if $\langle x_0, x_1, \ldots, x_n \rangle \subseteq \text{Rad}(I)$.

5.3.3. Irreducible algebraic sets and projective varieties. As in Chapter 4, we say that an algebraic set V is *reducible* if $V = V_1 \cup V_2$, where V_1 and V_2 are algebraic sets with $V_1 \subsetneq V$ and $V_2 \subsetneq V$. An algebraic set that is not reducible is said to be *irreducible*. A *projective variety* is defined to be an irreducible algebraic subset of $\mathbb{P}^n$, for some n.

EXERCISE 5.3.17. Determine whether each algebraic set in $\mathbb{P}^n$ is irreducible (and thus a projective variety).

(1) $V(\langle x_0 \rangle)$
(2) $V(\langle x_0x_1 \rangle)$
(3) $V(\langle x_1, x_2, \ldots, x_n \rangle)$

EXERCISE 5.3.18. Let $V \subset \mathbb{P}^n$ be an algebraic set.

(1) Suppose that V is reducible, say $V = V_1 \cup V_2$ where V_1 and V_2 are algebraic sets with $V_1 \subsetneq V$ and $V_2 \subsetneq V$. Show that there are polynomials $P_1 \in I(V_1)$ and $P_2 \in I(V_2)$ such that $P_1P_2 \in I(V)$ but $P_1, P_2 \notin I(V)$. Conclude that $I(V)$ is not a prime ideal.
(2) Prove that if $I(V)$ is not a homogeneous prime ideal in $k[x_0, x_1, \ldots, x_n]$, then V is a reducible algebraic set in $\mathbb{P}^n$.

Therefore, a projective variety V in $\mathbb{P}^n$ corresponds to a homogeneous prime ideal I in the graded ring $R = k[x_0, x_1, \ldots, x_n]$, other than the ideal $J = \langle x_0, x_1, \ldots, x_n \rangle$. (Recall that J is called the irrelevant ideal, since $V(J) = \emptyset$.)

EXERCISE 5.3.19. Determine whether each algebraic set V is a projective variety in $\mathbb{P}^2$ by determining whether $I(V)$ is prime.

(1) $V(\langle x_0x_1\rangle)$
(2) $V(\langle x_0x_1 - x_2^2\rangle)$
(3) $V(\langle x_0^2\rangle)$

EXERCISE 5.3.20. Suppose $V = V_1 \cup V_2$ is a reducible algebraic set. Show that $I(V) = I(V_1) \cap I(V_2)$.

EXERCISE 5.3.21. Suppose V is a reducible algebraic set. Show that V is the union of a finite number of projective varieties.

5.3.4. The Zariski topology. As we saw with affine varieties, the collection of algebraic sets are the closed sets for a topology on $\mathbb{P}^n$, the *Zariski topology.*

EXERCISE 5.3.22. (1) Show that $\emptyset$ and $\mathbb{P}^n$ are algebraic sets in $\mathbb{P}^n$.
(2) Show that the union of a finite number of algebraic sets in $\mathbb{P}^n$ is again an algebraic set.
(3) Show that the intersection of an arbitrary collection of algebraic sets in $\mathbb{P}^n$ is again an algebraic set.

Conclude that the algebraic sets in $\mathbb{P}^n$ form the collection of closed sets for a topology on $\mathbb{P}^n$. This is the *Zariski topology* on $\mathbb{P}^n$.

EXERCISE 5.3.23. The Zariski topology on $\mathbb{P}^1$.

(1) Show that $\{(0:1),(1:0)\}$ is a closed set.
(2) Find an open neighborhood of $\{(1:1)\}$.
(3) Describe the closed sets in $\mathbb{P}^1$.
(4) Find a basis of open sets for $\mathbb{P}^1$

EXERCISE 5.3.24. The Zariski topology on $\mathbb{P}^n$.

(1) Show that the sets $\mathbb{P}^n \backslash V(f)$, for homogeneous $f \in k[x_0,\ldots,x_n]$, form a basis for the Zariski topology on $\mathbb{P}^n$.
(2) Show that this topology is not Hausdorff. (Recall that a topological space is Hausdorff if for every pair of distinct points there exist disjoint open neighborhoods containing them.)

5.4. Functions on Projective Varieties

5.4.1. The rational function field and local ring. As we did for curves in section 3.12 we now define a field of functions on a projective variety. Suppose $V \subset \mathbb{P}^n$ is a projective variety. We'd like to work with functions on V and as we have previously seen, polynomial functions are not well-defined on projective space.

Instead we consider ratios $\frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}$ where f and g are homogeneous polynomials of the same degree.

EXERCISE 5.4.1. Let f and g be homogeneous polynomials of the same degree. Show that

$$\frac{f(\lambda x_0,\ldots,\lambda x_n)}{g(\lambda x_0,\ldots,\lambda x_n)} = \frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}.$$

Thus $\frac{f}{g}$ is a well-defined function at all points $P \in \mathbb{P}^n$ with $g(P) \neq 0$.

DEFINITION 5.4.1. Let $V \subset \mathbb{P}^n$ be a projective variety with ideal $I(V)$. The function field of V, $\mathcal{K}(V)$, is the set of all ratios

$$\frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}$$

such that

(1) f and g are homogeneous polynomials of the same degree
(2) $g \notin I(V)$
(3) $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ if $f_1g_2 - f_2g_1 \in I(V)$.

EXERCISE 5.4.2. Prove that $\sim$ is an equivalence relation and that $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ if and only if $\frac{f_1}{g_1}$ and $\frac{f_2}{g_2}$ are identical functions on V.

EXERCISE 5.4.3. Prove that $\mathcal{K}(V)$ is a field.

EXERCISE 5.4.4. Let $V = V(\langle x^2 - yz\rangle)$ in $\mathbb{P}^2$.

(1) Show that $\frac{x}{z} = \frac{y}{x}$ in $\mathcal{K}(V)$.
(2) Show that $\frac{x}{z}$ is defined on an open subset U of V, and thus $\frac{x}{z}$ defines a function from U to the base field k.

EXERCISE 5.4.5. Let $V = V(\langle x_0x_2 - x_1^2, x_1x_3 - x_2^2, x_0x_3 - x_1x_2\rangle)$ in $\mathbb{P}^3$.

(1) Show that $\frac{x_0}{x_2} = \frac{x_1}{x_3}$ in $\mathcal{K}(V)$.
(2) Show that $\frac{x_0}{x_2}$ is defined on an open subset U of V, and thus defines a function from U to the base field k.

EXERCISE 5.4.6. Let V be a projective variety in $\mathbb{P}^n$ and let $h = \frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}$ where f and g are homogeneous polynomials of the same degree. Show that h is defined on an open subset U of V, and thus defines a function from U to the base field k.

What we call a function on a projective variety V is often only defined on an open subset of V. We also will be interested in functions defined at a particular point of our variety, which leads to the next definition.

DEFINITION 5.4.2. Let V be a projective variety and $P \in V$. The *local ring* of V at P, $\mathcal{O}_{V,P}$, is the set of all rational functions $h \in \mathcal{K}(V)$ such that at P, we can write $h = \frac{f}{g}$ where f, g are homogenous polynomials of the same degree and $g(P) \neq 0$.

EXERCISE 5.4.7. Let $V = V(\langle xz - y^2 \rangle)$ and let $P = (0 : 0 : 1)$. Show that the rational function $h = \frac{x}{y}$ is in $\mathcal{O}_{V,P}$ by finding homogeneous polynomials f and g with $g(P) \neq 0$ and $h = \frac{f}{g}$.

EXERCISE 5.4.8. Verify that $\mathcal{O}_{V,P}$ is a ring.

EXERCISE 5.4.9. In abstract algebra a ring is called local if it has a unique maximal ideal. In this exercise we will show that $\mathcal{O}_{V,P}$ satisfies this property.

(1) Let $m_P = \{h \in \mathcal{O}_{V,P} \mid h(P) = 0\}$. Prove that m_P is a maximal ideal.
(2) Let I be any ideal in $\mathcal{O}_{V,P}$. Prove that $I \subseteq m_P$.

5.4.2. Rational functions. As we have seen in the previous exercises, an element h of $\mathcal{K}(V)$ is defined on an open set U of V and defines a function from U to k. We will write $V \dashrightarrow k$ for this function to indicate that h is not defined on all of V. Taking elements $h_0, h_1, \ldots, h_m \in \mathcal{K}(V)$ we can define a function $h : V \dashrightarrow \mathbb{P}^m$ by

$$h(p) = (h_0(p) : h_1(p) : \ldots : h_m(p))$$

at each point $p \in V$ where each h_i is defined and at least one of the $h_i(p)$ is non-zero. We call such a function a *rational map* on V.

EXERCISE 5.4.10. Prove that the above definition of h gives a well-defined function from an open subset of V to $\mathbb{P}^m$.

EXERCISE 5.4.11. Let $V = V(\langle x_0x_2 - x_1x_3 \rangle)$ in $\mathbb{P}^3$, and let $h_0 = \frac{x_0}{x_3}$, $h_1 = \frac{x_1}{x_2}$, $h_2 = \frac{x_3}{x_1}$. Determine the domain of the rational map $h : V \dashrightarrow \mathbb{P}^2$ defined by $h(p) = (h_0(p) : h_1(p) : h_2(p))$.

EXERCISE 5.4.12. Let $h : \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ be defined by

$$h((p_0 : p_1)) = \left(\frac{p_0^2}{p_1^2} : \frac{p_0}{p_1} : 1 \right).$$

(1) Determine the domain U of h, that is the points where h is regular.
(2) Show that the function $a((p_0 : p_1)) = (p_0^2 : p_0p_1 : p_1^2)$ agrees with h on U and is defined on all of $\mathbb{P}^1$.

EXERCISE 5.4.13. Let $V = V(\langle x_0^2 + x_1^2 - x_2^2 \rangle)$ in $\mathbb{P}^2$, and let $h_0 = \frac{x_0}{x_2}$, $h_1 = \frac{x_1}{x_2}$.

(1) Determine the domain of the rational map $h : V \dashrightarrow \mathbb{P}^1$ defined by $h(p) = (h_0(p) : h_1(p))$.
(2) Show that the function $(x_0 : x_1 : x_2) \mapsto (x_0 : x_1)$ is equal to h.

EXERCISE 5.4.14. Let h be a rational map $h : V \dashrightarrow \mathbb{P}^m$, so h is defined as

$$h(p) = (h_0(p) : h_1(p) : \ldots : h_m(p))$$

where $h_i = \frac{f_i}{g_i}$ with f_i, g_i homogeneous polynomials of degree d_i, for $0 \leq i \leq m$.

(1) Show that

$$(h_0(p) : h_1(p) : \ldots : h_m(p)) = (g(p)h_0(p) : g(p)h_1(p) : \ldots : g(p)h_m(p))$$

for any homogeneous polynomial g.

(2) Prove that any rational map $h : V \dashrightarrow \mathbb{P}^m$ can be defined by

$$h(p) = (a_0(p) : a_1(p) : \ldots : a_m(p))$$

where $a_0, a_1, \ldots, a_m$ are homogeneous polynomials of the same degree.

As we see in the previous exercises, a rational function can have more than one representation. By changing to an equivalent expression we can often extend the domain of our function.

A rational function $h : V \dashrightarrow \mathbb{P}^m$ is called *regular* at a point P if locally near P, h can be represented by rational functions $\frac{f_0}{g_0}, \frac{f_1}{g_1}, \ldots \frac{f_m}{g_m}$ such that $g_i(P) \neq 0$ for each i and $f_i(P) \neq 0$ for at least one i. A rational function that is regular at all points of the variety V is called a *morphism*.

EXERCISE 5.4.15. Let $V = V(\langle x_0x_2 - x_1x_3 \rangle)$ in $\mathbb{P}^3$, and let $h_0 = \frac{x_0}{x_3}$, $h_1 = \frac{x_1}{x_2}$, $h_2 = \frac{x_3}{x_1}$. Determine the regular points of the rational map $h : V \dashrightarrow \mathbb{P}^2$ defined by $h(p) = (h_0(p) : h_1(p) : h_2(p))$.

EXERCISE 5.4.16. Let $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ be defined by $(x_0x_1 : x_0x_2 : x_1x_2)$.

(1) Find all points P where f is regular.
(2) Describe the pre-images of each of the points $(0 : 0 : 1), (0 : 1 : 0)$, and $(1 : 0 : 0)$.

So far we have considered functions from a variety to projective space, but we are often interested in functions to another projective variety. We write

$$f : V \dashrightarrow W$$

when the image of f lies in the projective variety W.

EXERCISE 5.4.17. Prove that the rational map $f : \mathbb{P}^1 \to \mathbb{P}^2$ defined by

$$f((a_0 : a_1)) = (a_0 : a_1 : a_1)$$

is a morphism and that the image lies in the line $x_1 - x_2 = 0$ in $\mathbb{P}^2$.

EXERCISE 5.4.18. Prove that the rational map $f : \mathbb{P}^1 \to \mathbb{P}^2$ defined by

$$f((a_0 : a_1)) = (a_0^2 : a_0a_1 : a_1^2)$$

is a morphism and that the image lies in the conic $x_0x_2 - x_1^2 = 0$.

EXERCISE 5.4.19. Let $f : \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$ be defined by

$$f((a_0 : a_1)) = (a_0^3 : a_0^2a_1 : a_0a_1^2 : a_1^3).$$

Prove that f is a morphism and that the image lies in the variety $W = V(\langle x_0x_3 - x_1x_2, x_0x_2 - x_1^2, x_1x_3 - x_2^2\rangle)$.

EXERCISE 5.4.20. Let $V = V(\langle x_0x_3 - x_1x_2\rangle) \subset \mathbb{P}^3$ and let $f : V \dashrightarrow \mathbb{P}^1$ be defined by $f((x_0 : x_1 : x_2 : x_3)) = (x_0 : x_2)$. Prove that f is a morphism and that the image is all of $\mathbb{P}^1$.

5.4.3. Birationality.

DEFINITION 5.4.3. Let $\phi : V \dashrightarrow W$ be a rational map between projective varieties such that there is a rational map $\psi : W \dashrightarrow V$ with the property $\psi \circ \phi(P) = P$ for all points P in an open subset of V. We say that ϕ is a birational map with rational inverse ψ, and the varieties V and W are birational.

EXERCISE 5.4.21. Let $V = V(\langle x_0\rangle) \subset \mathbb{P}^2$ and let $f : V \dashrightarrow \mathbb{P}^1$ be defined by $f((x_0 : x_1 : x_2)) = (x_1 : x_2)$. Prove that f is birational.

EXERCISE 5.4.22. Let $V = V(\langle x_0x_2 - x_1^2\rangle) \subset \mathbb{P}^2$ and let $f : V \dashrightarrow \mathbb{P}^1$ be defined by $f((x_0 : x_1 : x_2)) = (x_0 : x_1)$. Prove that f is birational.

EXERCISE 5.4.23. Let $V = V(\langle x_0 + x_1 + x_2 + x_3\rangle) \subset \mathbb{P}^3$. Show that V and $\mathbb{P}^2$ are birational.

EXERCISE 5.4.24. Let $V = V(\langle y^2z - x^3 - xz^2\rangle) \subset \mathbb{P}^2$. Show that V and $\mathbb{P}^1$ are not birational.

5.5. Examples

EXERCISE 5.5.1. Define a rational map $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ by $\varphi((x_0 : x_1)) = (x_0^2 : x_0x_1 : x_1^2)$.

(1) Show that the image of φ is a plane conic.
(2) Find the rational inverse of φ.

EXERCISE 5.5.2. Define a rational map $\varphi : \mathbb{P}^1 \to \mathbb{P}^3$ by $\varphi((x_0 : x_1)) = (x_0^3 : x_0^2x_1 : x_0x_1^2 : x_1^3)$.

(1) Find the image V of φ. (This image is called a twisted cubic curve.)
(2) Find the rational inverse from V to $\mathbb{P}^1$.

We now generalize the previous two exercises to construct morphisms from $\mathbb{P}^1$ to various projective spaces. The next two exercises follows Hartshorne, Exercise I.2.12.

EXERCISE 5.5.3.
(1) Fix a degree $d > 0$. How many monomials in the variables x_0 and x_1 of degree d exist? Call this number N and list the monomials in some order, $m_1, \ldots, m_N$.
(2) Show that $(x_0 : x_1) \mapsto (m_1 : \cdots : m_N)$ is a well defined function from $\mathbb{P}^1$ to $\mathbb{P}^N$. This is called the *d-uple embedding* of $\mathbb{P}^1$.
(3) Let Y be the image of the 4-uple embedding of $\mathbb{P}^1$. Show that Y is an algebraic set.

EXERCISE 5.5.4. We generalize further to construct morphisms from $\mathbb{P}^n$.
(1) Fix a degree $d > 0$. How many monomials in the variables $x_0, x_1, \ldots, x_n$ of degree d exist? Call this number N and list the monomials in some order, $m_1, \ldots, m_N$.
(2) Show that $(x_0 : x_1 : \cdots : x_n) \mapsto (m_1 : \cdots : m_N)$ is a well defined function from $\mathbb{P}^n$ to $\mathbb{P}^N$. This is called the *d-uple embedding* of $\mathbb{P}^n$.
(3) Let Y be the image of the 2-uple embedding of $\mathbb{P}^2$ in $\mathbb{P}^5$. This is called the *Veronese surface*. Show that Y is an algebraic set in $\mathbb{P}^5$.

In the next two exercises we will show that the product of projective spaces is again a projective algebraic set, which in fact is a projective variety.

EXERCISE 5.5.5. Define the *Segre embedding* of the product, $\mathbb{P}^1 \times \mathbb{P}^1$, by

$$\psi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$$

by $\psi((a_0 : a_1), (b_0 : b_1)) = (a_0b_0 : a_0b_1 : a_1b_0 : a_1b_1)$.
(1) Show that ψ is well defined.
(2) Let Y be the image of ψ in $\mathbb{P}^3$. Show that Y is an algebraic set.

EXERCISE 5.5.6. We now consider the product of the projective spaces $\mathbb{P}^k$ and $\mathbb{P}^\ell$. Define the *Segre embedding* of $\mathbb{P}^k \times \mathbb{P}^\ell$,

$$\psi : \mathbb{P}^k \times \mathbb{P}^\ell \to \mathbb{P}^{(k+1)(\ell+1)-1}$$

$\psi((a_0 : a_1 : \cdots : a_k), (b_0 : b_1 : \cdots : b_\ell)) = (a_0b_0 : a_0b_1 : \cdots : a_0b_\ell : a_1b_0 : a_1b_1 : \cdots : a_kb_\ell)$.
(1) Show that ψ is well defined from $\mathbb{P}^k \times \mathbb{P}^\ell$ to $\mathbb{P}^{(k+1)(\ell+1)-1}$.
(2) Let Y be the image of ψ in $\mathbb{P}^{(k+1)(\ell+1)-1}$. Show that Y is an algebraic set.

5.5.1. Proj. We next define the projective counterpart of the prime spectrum Spec(R). The *Proj* construction is an important initial step in the study of projective schemes associated to graded rings. We will only state the definition and look at several examples of how this construction relates back to projective varieties.

Let R be a graded ring, which for our purposes will be mainly $k[x_0, \ldots, x_n]$ or a quotient of this polynomial ring. As before, for projective varieties we are interested in *homogeneous* ideals, apart from the irrelevant ideal. (Recall that the irrelevant ideal of $k[x_0, \ldots, x_n]$ is $\langle x_0, x_1, \ldots, x_n \rangle$; for a general graded ring R we call the ideal generated by all elements of positive degree irrelevant.)

Define Proj(R) to be the set of all homogeneous prime ideals in R that do not contain the irrelevant maximal ideal. This plays the role for projective varieties that *Spec* plays for affine varieties, providing a dictionary between graded rings and their homogeneous ideals and the projective varieties and their algebraic sets.

The set Proj(R) is given the Zariski topology as follows. For any homogeneous ideal H in R, define

$$V(H) = \{I \in \mathrm{Proj}(R) : H \subseteq I\}$$

the set of homogeneous prime ideals containing H (again excluding the irrelevant ideal). As in the construction of the Zariski topology on Spec(R), we say that the sets $V(H)$ are *closed* in Proj(R). Recall then that open sets are defined to be complements of closed sets, thus of the form $\mathrm{Proj}(R) - V(H)$ for some homogeneous ideal H. In the next exercise we show that this defines a topology on Proj(R).

Exercise 5.5.7. (1) Show that the empty set and Proj(R) are open.

(2) Prove that the arbitrary union of open sets of Proj(R) is also open.
(3) Prove that the intersection of a finite number of open sets is also open.

Exercise 5.5.8. Let $R = \mathbb{C}[x]$. Show that Proj(R) is a point.

Exercise 5.5.9. In this exercise we show how to obtain the projective line $\mathbb{P}^1$ as Proj(R) for the ring $R = \mathbb{C}[x_0, x_1]$.

(1) Let I be a homogeneous prime ideal in R such that I does not contain the irrelevant ideal $\langle x_0, x_1 \rangle$. Prove that either $I = \{0\}$ or I is generated by one linear polynomial.
(2) Show how the ideal $\langle x_0 \rangle$ corresponds to the point $(0 : 1) \in \mathbb{P}^1$. Prove that this ideal is maximal among those in Proj(R).
(3) Find the prime ideal I that corresponds to the point $(1 : 2)$, and prove that the set $\{I\}$ is closed in Proj(R).
(4) Find the prime ideal I that corresponds to the point $(a : b)$, and prove that the set $\{I\}$ is closed in Proj(R).
(5) Prove that every closed point of Proj(R) is a prime ideal in R that is maximal among those in Proj(R).

(6) Show that $\text{Proj}(R)$ corresponds to $\mathbb{P}^1$.

EXERCISE 5.5.10. In this exercise we show how to obtain the projective plane $\mathbb{P}^2$ as $\text{Proj}(R)$ for the ring $R = \mathbb{C}[x_0, x_1, x_2]$.

(1) Show that the ideal $I = \langle x_0, x_1 \rangle$ corresponds to the point $(0 : 0 : 1) \in \mathbb{P}^2$. Prove that this ideal is maximal among those in $\text{Proj}(R)$, so that $V(I) = \{I\}$.
(2) Show that $V(I) \neq \{I\}$ for the ideal $I = \langle x_0^2 + x_1^2 + x_2^2 \rangle$, by finding a point $P \in V(I)$ with $P \neq I$.
(3) Find the prime ideal I that corresponds to the point $(1 : 2 : 3)$, and prove that the set $\{I\}$ is closed in $\text{Proj}(R)$.
(4) Find the prime ideal I that corresponds to the point $(a : b : c)$, and prove that the set $\{I\}$ is closed in $\text{Proj}(R)$.
(5) Prove that every closed point of $\text{Proj}(R)$ corresponds to a point in $\mathbb{P}^2$.

EXERCISE 5.5.11. In this exercise we show how to obtain $\mathbb{P}^n$ as $\text{Proj}(R)$ for $R = \mathbb{C}[x_0, x_1, \ldots, x_n]$.

(1) Show that the ideal $I = \langle x_0, x_1, \ldots, x_{n-1} \rangle$ corresponds to the point $(0 : 0 : \cdots : 0 : 1) \in \mathbb{P}^n$. Prove that this ideal is maximal among those in $\text{Proj}(R)$, so that $V(I) = \{I\}$.
(2) Show that $V(I) \neq \{I\}$ for the ideal $I = \langle x_0^2 + x_1^2 + \cdots + x_n^2 \rangle$, by finding a point $P \in V(I)$ with $P \neq I$.
(3) Find the prime ideal I that corresponds to the point $(1 : 2 : \cdots : n)$, and prove that the set $\{I\}$ is closed in $\text{Proj}(R)$.
(4) Find the prime ideal I that corresponds to the point $(a_0 : a_1 : \cdots : a_n)$, and prove that the set $\{I\}$ is closed in $\text{Proj}(R)$.
(5) Prove that every closed point of $\text{Proj}(R)$ corresponds to a point in $\mathbb{P}^n$.

As an extension of the previous exercises we next use the Proj construction to obtain a description of the parabola $x_0x_1 - x_2^2$ in $\mathbb{P}^2$. While this exercise provides some practice in using the definitions, it is not a recommended method for studying a parabola!

EXERCISE 5.5.12. Let $S = \mathbb{C}[x_0, x_1, x_2]/I$, where $I = \langle x_0x_1 - x_2^2 \rangle$.

(1) As a brief review of some commutative algebra, prove that the homogeneous ideals of S correspond to homogeneous ideals of $\mathbb{C}[x_0, x_1, x_2]$ containing I.
(2) Show that the ideal $\langle x_0, x_2 \rangle \subset S$ corresponds to the point $(0 : 1 : 0)$ on the parabola. Prove that the class of this ideal in $\text{Proj}(S)$ is maximal among those not containing the irrelevant ideal, so that $V(I) = \{I\}$.

(3) Find the prime ideal J that corresponds to the point $(-1 : -1 : 1)$ on the parabola, and prove that the set $\{J\}$ is closed in $\mathrm{Proj}(S)$.

(4) For an arbitrary point $(a : b : c)$ on the parabola, find the corresponding prime ideal J in S and prove that the set $\{J\}$ is closed in $\mathrm{Proj}(S)$.

(5) Show that the points of the parabola correspond to the closed points of $\mathrm{Proj}(S)$.

EXERCISE 5.5.13. some motivation for studying Proj!

CHAPTER 6

Sheaves and Cohomology

The goal of this chapter is to introduce sheaf theory to algebraic geometry. We will recast our study of divisors into the language of invertible sheaves. Finally, we will recast the statement of Riemann-Roch into the language of Cech cohomology of invertible sheaves. The underlying motivation for this chapter is to develop the needed tools to pass from local to global information.

6.1. Intuition and Motivation for Sheaves

The goal of this section is to motivate our eventual definition of sheaves in terms of local versus global properties of curve intersections, of Riemann-Roch and to the Mittag-Leffler problem of finding rational functions with prescribed poles on a curve.

6.1.1. Local versus Global. We started this text with problems about conics in the plane $\mathbb{R}^2$ but saw that we needed to pass to the complex projective plane $\mathbb{P}^2$. The rhetoric is that the conic in $\mathbb{R}^2$ (or in $\mathbb{C}^2$) is local, while the homogenized conic in $\mathbb{P}^2$ is global. The language is used since we form the complex projective plane $\mathbb{P}^2$ by patching (or gluing) together three copies of $\mathbb{C}^2$.

This patching or gluing is a powerful idea. With sheaves, we will again perform gluing operations, but this time we will be gluing functions rather than spaces together. The idea is almost the same. We need to describe how the functions overlap and be sure that they agree where they should. One of the roles sheaves will have to play for us is to record how functions can be pieced together from local parts to form larger wholes.

6.1.2. Local versus Global Curve Intersections. Bezout's Theorem is the quintessential global result. Here is why:

Exercise 6.1.1. Find a curve in $\mathbb{C}^2$ that intersects the curve C

$$y = x^2$$

picture

in exactly one point, counting multiplicity.

This is an example of a local intersection, as in it is happening in $\mathbb{C}^2$.

EXERCISE 6.1.2. Homogenize the two curves from the previous problem. Show that the two curves now must intersect in more than one point.

The homogenized curve in $\mathbb{P}^2$ is the global version. The fact that the total intersection number must be at least two is thought of as a global type result.

This is common. In $\mathbb{C}^2$, curves of degree d and e can intersect in any number of points, from zero to de, while the corresponding curves in $\mathbb{P}^2$ must intersect in inexactly de points.

6.1.3. Local versus Global for Riemann-Roch. Let $\mathcal{C}$ be a smooth curve in $\mathbb{P}^2$. For any divisor D on $\mathcal{C}$, we have the Riemann-Roch theorem from chapter three, which states that

$$l(D) - l(K - D) = \deg(D) - g + 1.$$

Here $l(D)$ is the dimension of the vector space of all $f \in \mathcal{K}_{\mathcal{C}}$ such that

$$(f) + D \geq 0.$$

Thus $l(D)$ is a measure of how many rational functions there are on the curve $\mathcal{C}$ with certain prescribed poles and zeros.

There is nothing to prevent us from trying to find affine analogs, namely for any affine curve $\mathcal{C}$ to ask for the dimension of the vector space of all $f \in \mathcal{K}_{\mathcal{C}}$ such that

$$(f) + D \geq 0,$$

for a divisor D on $\mathcal{E}$. But these vector spaces are quite different from the projective case, and no clean analog to Riemann-Roch exists.

EXERCISE 6.1.3. Let $\mathcal{C}$ be the curve in $\mathbb{C}^2$ given by

$$y = x^2.$$

Let D be the divisor $-(0, 0)$. Show that there is an $f \in \mathcal{K}_{\mathcal{C}}$ such that

$$(f) + D \geq 0.$$

EXERCISE 6.1.4. Let $\mathcal{C}$ be the curve in $\mathbb{P}^2$ given by

$$yz = x^2$$

(the homogenization of the affine curve from the previous problem). Let D be the divisor $-(0 : 0 : 1)$. Show that there is no $f \in \mathcal{K}_{\mathcal{C}}$ such that

$$(f) + D \geq 0.$$

6.1.4. Local Versus Global for the Mittag-Leffler Problem. (This subsection requires a bit of complex analysis. If you want, whenever you see the term "meromorphic," just think ratios of polynomials.)

We will begin with a motivating example. Suppose f is a function whose Laurent series centered at a is given by $f(z) = \sum_{k=-\infty}^{\infty} c_k(z-a)^k$. The *principal part* of f at a is $\sum_{k=-\infty}^{-1} c_k(z-a)^k$. The function f has a *pole of order m at a* if the principal part of f at a is $\sum_{k=-m}^{-1} c_k(z-a)^k$, that is, if the principal part of f at a is a finite sum.

Let Ω be an open subset of $\mathbb{C}$ and let $\{a_j\}$ be a sequence of distinct points in Ω such that $\{a_j\}$ has no limit point in Ω. For each integer $j \geq 1$ consider the rational function

$$P_j(z) = \sum_{k=1}^{m_j} \frac{c_{j,k}}{(z-a_j)^k}.$$

The Mittag-Leffler Theorem states that there exists a meromorphic function f on Ω, holomorphic outside of $\{a_j\}$, whose principal part at each a_j is $P_j(z)$ and which has no other poles in Ω. This theorem allows meromorphic functions on $\mathbb{C}$ to be constructed with an arbitrarily preassigned discrete set of poles.

Exercise 6.1.5. Find a meromorphic function f that has a pole of order 2 at the origin such that the residue of the origin is 0.

Exercise 6.1.6. Let $\omega_1, \omega_2 \in \mathbb{C}$ such that $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Find a meromorphic function that has a pole at every point in the lattice $\Lambda = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$.

Since we can construct functions with arbitrarily preassigned discrete sets of poles on $\mathbb{C}$, it is natural to ask the same question on a complex curve (which we know can be viewed as a real surface). Suppose X is a Riemann surface. Given a discrete set of points $\{a_j\}$ and a principal part $P_j(z)$ at each a_j, where z is a local affine coordinate, does there exist a rational function f on X, defined outside $\{a_j\}$, whose principal part at each a_j is $P_j(z)$? Locally, there is such a function provided by the Mittag-Leffler Theorem, but whether there exists such a function defined globally is more subtle. This requires passing from local information to global information. The primary virtue of sheaves is that they provide a mechanism to deal with problems passing from local information to global information.

6.1.5. Local Versus Global: the Sheaf of Regular Functions. Prior to giving the definition of sheaves, we will look a concrete example of a sheaf that has the virtue of its ubiquitousness. In the next section, the reader will prove that the object we encounter here is indeed a sheaf.

Let X be an algebraic variety, either affine or projective. There is always the sheaf $\mathcal{O}_X$ of regular functions on X, defined by setting for each Zariski open set U in X the ring of functions

$$\mathcal{O}_X(U) = \{\text{regular function on } U\}$$

and letting $r_{V,U}$, for $U \subset V \subset X$, be the restriction map. In fact, we have already been using the notation $\mathcal{O}_X$ throughout this book.

Exercise 6.1.7. Consider the projective line $\mathbb{P}^1$ with homogeneous coordinates $(x_0 : x_1)$. Let $U_0 = \{(x_0 : x_1) \mid x_0 \neq 0\}$. Show that the ring $\mathcal{O}_X(U_0)$ is isomorphic to the ring $\mathbb{C}[t]$. Show that $\mathcal{O}_X(\mathbb{P}^1)$ is isomorphic to $\mathbb{C}$, the constant functions.

The functions making up $\mathcal{O}_X(U_0)$ are viewed as local, while those making up $\mathcal{O}_X(\mathbb{P}^1)$ are global. This of course extends to any projective variety, as seen in the following example for curves.

Exercise 6.1.8. In $\mathbb{P}^2$, let

$$X = \{(x_0 : x_1 : x_2) : x_0^2 + 3x_1^2 - x_2^2 = 0\},$$

and let $U_0 = \{(x_0 : x_1 : x_2) \in X : x_0 \neq 0\}$. Show that $\mathcal{O}_X(U_0)$ is isomorphic to the ring $\mathbb{C}[s,t]/(3s^2 - t^2 + 1)$ but that $\mathcal{O}_X(X)$ is isomorphic to $\mathbb{C}$, the constant functions.

6.2. The Definition of a Sheaf

The definition of a sheaf is given, after first defining presheaves.

Suppose X is a topological space. Being interested in both the local and global structure of X, we wish to assign to each open set U of X a collection of data that is somehow characteristic of U. Since different kinds of algebraic structures can encode geometric information about a topological space, it is useful to introduce a concept that encompasses different ways of assigning algebraic structures to the space.

Definition 6.2.1. A *presheaf* $\mathcal{F}$ of rings of functions (or modules over rings) on X consists of a ring of functions (resp. module, etc.) $\mathcal{F}(U)$ for every open set $U \subset X$ and the ring homomorphism given by the restriction map (resp. module homomorphism, etc.) $r_{V,U} : \mathcal{F}(V) \to \mathcal{F}(U)$ for any two nested open subsets $U \subset V$ satisfying the following two conditions:

i) $r_{U,U} = \mathrm{id}_{\mathcal{F}(u)}$

ii) For open subsets $U \subset V \subset W$ one has $r_{W,U} = r_{V,U} \circ r_{W,V}$.

The elements of $\mathcal{F}(U)$ are called the *sections* of $\mathcal{F}$ over U and the map $r_{V,U}$ is called the *restriction map*, and $r_{V,U}(s)$ is often written $s\big|_U$.

For almost all of our examples, each $\mathcal{F}(U)$ will consist of some specified type of function defined on the open set U. In this type of case, when $U \subset V$, if f is a function with domain V, then $r_{V,U}(f)$ is simply the same function f, but now with domain restricted to the smaller open set U. Then the first axiom can be interpreted as requiring that the restriction of a function from a space to itself always returns the same function. That is, a trivial restriction should not change functions. The second axiom, in turn, says that the result of a sequence of restrictions should be identical to the single restriction from the initial to the final subspace. Again, in the context of restrictions of functions, this axiom is very natural. This also mean that for the following exercises, where you are asked to show that various objects are presheaves, you just have to show that if $f \in \mathcal{F}(V)$, then f with domain restricted to a smaller open set U is in $\mathcal{F}(U)$, or in other words, that the restriction map $r_{V,U}$ really does map elements of $\mathcal{F}(V)$ to elements of $\mathcal{F}(U)$. (This also means that the answers will not be that long.)

The building block for almost all sheaves in algebraic geometry is the sheaf of regular functions $\mathcal{O}_X$ on an algebraic variety X . We first show that $\mathcal{O}_X$ is at the least a presheaf.

Exercise 6.2.1. Suppose X is a variety, affine or projective. Show that its sheaf of regular functions, $\mathcal{O}_X$, is a presheaf as just defined.

Exercise 6.2.2. Suppose X is a topological space. For open U define

$$\mathcal{F}(U) = \{f : U \to \mathbb{Z} \mid f \text{ constant on connected components of } U\}$$

and let $r_{W,U} = r_{V,U} \circ r_{W,V}$ be the restriction of f to U. Show that $\mathcal{F}$ is a presheaf of rings.

Exercise 6.2.3. Suppose X is a topological space. Define

$$C(U) = \{f : U \to \mathbb{C} \mid f \text{ is continuous}\}$$

and let $r_{V,U}(f)$ be the restriction of f to U. Show that C is a presheaf of rings.

Exercise 6.2.4. Suppose $X = \mathbb{C}$. Define

$$\mathcal{B}(U) = \{f : U \to \mathbb{C} \mid f \text{ is a bounded holomorphic function}\}$$

and let $r_{V,U}(f)$ be the restriction of f to U. Show that $\mathcal{B}(U)$ is a presheaf of rings.

Presheaves enable us to assign to each open set of a topological space X an algebraic structure that describes the open set and how it fits inside of X. However, presheaves are top-down constructions; we can restrict information from larger to smaller sets. The problem of globalizing local data is not within the scope of the definition of a presheaf. That is, presheaves do not provide the means to deduce global properties from the properties we find locally in the open sets of X. The definition of a sheaf below is meant to resolve this, enabling us to pass data from global to local settings but also to patch local information together to establish global results when possible.

DEFINITION 6.2.2. A presheaf $\mathcal{F}$ of rings of functions (or modules over rings) on $X$is called a *sheaf* rings of functions (or modules over rings) if, for every collection U_i of open subsets of X with $U = \bigcup_i U_i$, the following two additional conditions are satisfied.

iii) If $s, t \in \mathcal{F}(U)$ and $r_{U,U_i}(s) = r_{U,U_i}(t)$ for all i, then $s = t$.
iv) If $s_i \in \mathcal{F}(U_i)$ and if for $U_i \cap U_j \neq \emptyset$ we have

$$r_{U_i,U_i\cap U_j}(s_i) = r_{U_j,U_i\cap U_j}(s_j),$$

for all i, j, then there exists $s \in \mathcal{F}(U)$ such that $r_{U,U_i}(s) = s_i$.

In light of the interpretation of functions and their restrictions, the new axioms for a sheaf are essential ingredients for inferring global information from local data. Axiom (iii) requires that two functions must be the same if they agree everywhere locally, i.e., if for every subset W of U, $s\big|_W = t\big|_W$, then $s = t$. Were this not true, then it would be impossible to construct a single global function on U from the parts of it we have on each of the U_i. Hence, axiom (iii) has to do with the uniqueness of global functions that we might construct from local data. Axiom (iv), in turn, has to do with the existence of such functions. Whenever we are given a collection of functions defined on various parts of X, we can patch them together to form a unique (due to axiom (iii)) function on X so long as this is feasible, i.e., two constituent functions s_i and s_j must agree wherever both are defined in X.

For our above presheaves, the patching is clear. The only reason that all of the above the presheaves are not automatically sheaves is if the patched together function on the open set U is not an element of the corresponding presheaf.

EXERCISE 6.2.5. Let our presheaf $\mathcal{F}$ be a presheaf of functions, with $r_{V,U}(f)$ being the restriction map $f\big|U$. Show that (iii) is equivalent to the following. If $s \in \mathcal{F}(U)$ such that $r_{U,U_i}(s) = 0$ for all i, then $s = 0$.

EXERCISE 6.2.6. Show that the presheaf $\mathcal{F}$ from Exercise 6.2.2 is a sheaf.

EXERCISE 6.2.7. Show that the presheaf C from Exercise 6.2.3 is a sheaf.

EXERCISE 6.2.8. Suppose X is a variety, affine or projective. Show that its sheaf of regular functions, $\mathcal{O}_X$, is a sheaf as just defined. (This is the key example for this section.)

EXERCISE 6.2.9. Show that the presheaf $\mathcal{B}$ from Exercise 6.2.4 is not a sheaf.

As we found in the last exercise, not all presheaves are sheaves. There is a construction, which we will describe now, that associates a sheaf to any presheaf in a universal way. The key distinction between a sheaf and a presheaf is the ability with a sheaf to assemble local data together to construct global results. Thus we first need to focus on the local data in a presheaf and force the construction of global information from it to construct the associated sheaf. To be as local as possible, we want to study the essense of a presheaf at a point.

As in the examples above, let us suppose that the elements of a presheaf $\mathcal{F}$ on X are functions. That is, an element $s \in \mathcal{F}(U)$ is a function on the open set U. Then the value $s(x)$ alone will not capture the essence of this function at x, for it is very likely that several distinct functions may have the same value at x. Hence we want to keep track of not only the value of s at x, but all of the values of s near x. This can be done by keeping track of the pair (U, s), where U is the open set containing x and $s \in \mathcal{F}(U)$. However, if V is any other open set containing x, then $U \cap V$ is one too and $(U \cap V, s|_{U\cap V})$ is really the same function near x that (U, s) was. So these two "local functions" at x should be identified with one another. In general, the pairs (U, s) and (V, t) are *equivalent* whenever there is a third open set W with $W \subset U \cap V$, $x \in W$, and $s|_W = t|_W$ in $\mathcal{F}(W)$.

EXERCISE 6.2.10. Let $\mathcal{F}$ be a presheaf of functions on a space X. Let $x \in X$ and let U and V be open sets containing the point x. Suppose $s \in \mathcal{F}(U)$ and $t \in \mathcal{F}(V)$. Set

$$(U, s) \sim (V, t)$$

whenever there is a third open set W with $W \subset U \cap V$, $x \in W$, and $s|_W = t|_W$ in $\mathcal{F}(W)$. Show that this is an equivalence relation.

DEFINITION 6.2.3. If $\mathcal{F}$ is any presheaf on a topological space X and x is any point in X, the equivalence class of (U, s), where U is an open set of X containing x and $s \in \mathcal{F}(U)$, is denoted by s_x and is called the *germ* of the section s at x.

DEFINITION 6.2.4. Let X be a topological space and let $\mathcal{F}$ be a presheaf on X. For a point $x \in X$, the *stalk* of $\mathcal{F}$ at x, denoted $\mathcal{F}_x$, consists of the germs s_x of sections at x for all open sets U containing x and all $s \in \mathcal{F}(U)$.

We can now define how to extend any presheaf to an actual sheaf.

DEFINITION 6.2.5. Using the stalks of a presheaf $\mathcal{F}$ on X, we construct the *sheaf associated to* $\mathcal{F}$, denoted $\mathcal{F}^+$, as follows. For any open set U, $\mathcal{F}^+(U)$ consists of all functions s from U to the union $\bigcup_{x\in U}\mathcal{F}_x$ of the stalks of $\mathcal{F}$ over points of U such that

(1) for each $x \in U$, $s(x) \in \mathcal{F}_x$
(2) for each $x \in U$, there is a neighborhood V of x, contained in U, and an element $\hat{s} \in \mathcal{F}(V)$, such that for all $y \in V$, the germ $\hat{S}_y$ of $\hat{s}$ at y is equal to $s(y)$.

This is an admittedly complicated definition. What we want is for our candidate sheaf $\mathcal{F}^+(U)$ to contain the $\mathcal{F}(U)$ plus whatever extra that is needed to make it a sheaf. The next problem is showing how to interpret elements of $\mathcal{F}(U)$ as also being in the new $\mathcal{F}^+(U)$.

EXERCISE 6.2.11. Let $\mathcal{F}$ be a presheaf on a topological space X. Let $s \in \mathcal{F}(U)$. Interpret s as an element of $\mathcal{F}^+(U)$.

EXERCISE 6.2.12. Let $\mathcal{F}$ be a presheaf on a topological space X. Prove that $\mathcal{F}^+$ is a sheaf on X.

EXERCISE 6.2.13. Let $\mathcal{F}$ be a sheaf of on a topological space X. Show that this sheaf is the same as our newly constructed sheaf $\mathcal{F}^+$.

EXERCISE 6.2.14. For the presheaf $\mathcal{B}$ of Exercise 6.2.4, show that its associated sheaf, $\mathcal{B}^+$, on $X = \mathbb{C}$ is the sheaf of holomorphic function on $\mathbb{C}$. (The sheaf of holomorphic function $\mathcal{H}$ on $\mathbb{C}$ is the defined by setting for all open U; to work this problem you will need to know that two holomorphic functions that agree on any open set in $\mathbb{C}$ agree everywhere where the functions are defined.)

6.3. The Sheaf of Rational Functions

The second most important sheaf in algebraic geometry is the sheaf of rational functions $\mathcal{K}'_X$, whose definition is the goal of this section.

Let X be an algebraic variety, either affine or projective. Then X is equipped with its sheaf of regular functions, $\mathcal{O}_X$.

There is another basic sheaf for every algebraic variety X, namely the function field sheaf $\mathcal{K}_X$, which plays the "sheaf-theoretic" role of the function field. Morally we want to think of $\mathcal{K}_X$ as the ratio of the functions in $\mathcal{O}_X$. The actual definition, though, is mildly subtle, as we will see. It is here, in fact, that we will need to use the difference between a presheaf and a sheaf.

We start with defining a presheaf $\mathcal{K}'_X$. For each open U in X, let $\mathcal{K}'_X(U)$ be the function field of the ring $\mathcal{O}_X(U)$, with the standard restriction map for functions.

(Here we are using the Zariski topology; thus the various open U are complements of the zero loci for various polynomials.) Thus $\mathcal{K}'_X(U)$ consists of all ratios

$$\frac{f}{g},$$

with $f, g\mathcal{O}(U)$ and g not the zero function. The goal of the next series of exercises is to see why $\mathcal{K}'_X$ is only a presheaf and to motivate why we actually want to look at its associated sheaf.

Exercise 6.3.1. Let X be an algebraic variety, either affine or projective. Verify that $\mathcal{K}'_X$ is a presheaf of a field of functions on X.

We now concentrate on the space $\mathbb{P}^1$, which is covered by the two open sets $U_0 = \{(x_0 : x_1) \mid x_1 \neq 0\}$ and $U_1 = \{(x_0 : x_1) \mid x_1 \neq 0\}$. Then on U_0 we let $s = (x_0/x_1)$ be our affine coordinate, and on U_1 we let $t = (x_1/x_0)$ be our affine coordinate. On the overlap, $U_0 \cap U_1$, we have $s = (1/t)$.

Exercise 6.3.2. Show that $\mathcal{K}'_{\mathbb{P}^1}(U_0)$ is isomorphic to the field $\mathbb{C}(s)$ and that $\mathcal{K}'_{\mathbb{P}^1}(U_1)$ is isomorphic to the field $\mathbb{C}(t)$.

Exercise 6.3.3. Show that $\mathcal{K}'_{\mathbb{P}^1}(\mathbb{P}^1)$ is isomorphic to the field $\mathbb{C}$.

Exercise 6.3.4. Using that $(1/t) \in \mathcal{K}'_{\mathbb{P}^1}(U_1)$ and condition (iii) in the definition of a sheaf, show that $\mathcal{K}'$ cannot be a sheaf.

Definition 6.3.1. The function field sheaf $\mathcal{K}_X$ for an algebraic variety X is the sheaf associated to the presheaf $\mathcal{K}'_X$

Exercise 6.3.5. Show that $\mathcal{K}_{\mathbb{P}^1}(\mathbb{P}^1)$ is isomorphic to the field $\mathbb{C}(s)$.

6.4. Divisors

The goal of this problem set is to generalize the notion of divisor from being the finite formal sum of points on a complex curve to being the finite formal sum of co-dimension one subvarieties of an algebraic variety.

In this section, we revisit a familiar tool, divisors, from Chapter 3. We will see how divisors are intimately related to the special class of invertible sheaves in the next section and how this can be used to give a new presentation of the Riemann-Roch Theorem at the end of the chapter.

Recall from Chapter 3, a divisor D on a curve $\mathcal{C}$ is a formal finite linear combination of points on $\mathcal{C}$ with integer coefficients, $D = n_1p_1 + n_2p_2 + \cdots + n_kp_k$ with $n_1, \ldots, n_k \in \mathbb{Z}$ and $p_1, \ldots, p_k \in \mathcal{C}$. One might think a divisor on a variety X would be a formal finite sum of points as before. However, this turns out not to be the correct generalization. Recall the purpose of a divisor on a curve was to keep track of the zeros and poles of a single function. On a variety X, a function's zeros constitute an algebraic subvariety usually of dimension one less than the dimension of X. Thus, rather than adding points, we should add subsets that look like the zero sets of single functions on X. To be precise:

Definition 6.4.1.

A *codimension-one subvariety* of a variety X is a proper irreducible algebraic subset $Y \subset X$ such that there are no other proper irreducible algebraic subsets Z satisfying $Y \subsetneq Z \subsetneq X$.

Definition 6.4.2. Let X be an algebraic variety. A *divisor* D on X is a finite formal sum over the integers $\mathbb{Z}$ of codimension-one subvarieties of X.

Let X be a curve in $\mathbb{P}^2$ and let $p, q, r \in X$ be points on X. Then an example of a divisor is

$$D = 3p - 5q + r.$$

The coefficients $3, -5, 1$ are just integers, while the points p, q, r are the codimension-one subvarieties of X. We need to use the term "formal sum" since adding points makes no real sense.

An example of a divisor on $\mathbb{P}^2$, using the homogeneous coordinates x_0, x_1, x_2, would be

$$3(x_0^2 + x_1x_2 = 0) - 7(x_0^4 + x_2^3x_2^2 = 0) = 3\mathrm{V}(x_0^2 + x_1x_2) - 7\mathrm{V}(x_0^4 + x_2^3x_2^2).$$

As divisors are formal sums, we should be able to add them. Thus if $D_1 = 3p - 5q + r$ and $D_2 = 8q + 4s - 4t$ are two divisors on the curve X, define

$$D_1+D_2 = 3p-5q+r+8q+4s-4t = 3p+(-5+8)q+r+4s-4t = 3p+3q+r+4s-4t.$$

Exercise 6.4.1. Let X be an algebraic curve. Let $D_1 = \sum_{p\in X} n_p p$ and $D_2 = \sum_{p\in X} m_p p$, where the $n_p, m_p \in \mathbb{Z}$, be two divisors on X. If we define

$$D_1 + D_2 = \sum_{p\in X}(n_p + m_p)p,$$

show that $\mathrm{Div}(X)$ is an abelian group. (Note in the above sums for the divisors D_1 and D_2, that even though the sums are over all points $p \in X$, we are assuming that $n_p = m_p = 0$ for all but a finite number of points on X; this is what is meant in the definition of a divisor by the phrase "finite formal sum.")

Exercise 6.4.2. Let X be an algebraic variety. Let $D_1 = \sum n_V V$ and $D_2 = \sum m_V V$, where the $n_V, m_V \in \mathbb{Z}$, be two divisors on X. Here both sums are over all codimension-one subvarieties of X. If we define

$$D_1 + D_2 = \sum(n_V + m_V)V,$$

show that $\mathrm{Div}(X)$ is an abelian group.

DEFINITION 6.4.3. A divisor $D = \sum n_V V$ is *effective* if, for all codimension-one subvarieties V of X, we have $n_V \geq 0$. In this case we write $D \geq 0$.

We now want to link divisors with both the geometry of the variety X and functions defined on X. In particular, we want to associate to every element $f \in \mathcal{O}_X$ a divisor, which we will denote by (f). This in turn will allow us to define, for every rational function $f/g \in \mathcal{K}_X$ (where $f, g \in \mathcal{O}_X$). the divisor

$$\left(\frac{f}{g}\right) = (f) - (g).$$

Let X be a curve in $\mathbb{P}^2$. Let $C = \mathrm{V}(P(x_0, x_1, x_2))$ be another curve in $\mathbb{P}^2$ that shares no components with X. Then define

$$D = X \cap C = \sum_{p \in X \cap C} m_p p,$$

where m_p is the intersection multiplicity of the intersection point. Since C shares no components with X, their intersection is a finite set of points, so D is a divisor on X. Since C is defined as the zero locus of the homogeneous polynomial P, then we can think of P as an element of $\mathcal{O}_X$. Then we use the notation

$$(P) = \sum_{p \in X \cap C} m_p p.$$

EXERCISE 6.4.3. Let $X = V(x^2 + y^2 - z^2)$ be a conic in $\mathbb{P}^2$. If $C_1 = \mathrm{V}(x - y)$ and $C_2 = \mathrm{V}(y - z)$. Show that the two corresponding divisors are

$$\begin{aligned} D_1 &= X \cap C_1 = \left(\frac{1}{\sqrt{2}} : \frac{1}{\sqrt{2}} : 1\right) + \left(-\frac{1}{\sqrt{2}} : -\frac{1}{\sqrt{2}} : 1\right) \\ D_2 &= X \cap C_2 = 2(0 : 1 : 1). \end{aligned}$$

Give a geometric interpretation for the coefficients in D_1 and D_2.

In the next few sections, we will see that the following definition for linear equivalence for divisors will be important:

DEFINITION 6.4.4. Let X be a projective variety. Divisors D_1 and D_2 are said to be *linearly equivalent* if there are two homogeneous polynomials f and g of the same degree such that

$$D_1 + \left(\frac{f}{g}\right) = D_2.$$

We denote this by

$$D_1 \sim D_2.$$

EXERCISE 6.4.4. On $\mathbb{P}^1$, show that $D_1 = (1 : 1)$ is linearly equivalent to $D_2 = (1 : 0)$.

EXERCISE 6.4.5. Let $\mathbb{P}^2$ have homogeneous coordinates x_0, x_1, x_2. Show that the divisors $D_1 = \mathrm{V}(x_0^2 + 3x_2^2)$ and

$$D_2 = \mathrm{V}(x_0^2)$$

are linearly equivalent.

EXERCISE 6.4.6. Let $f(x_0, \ldots, x_n)$ be any homogeneous polynomial of degree d. Show that the divisors $D_1 = \mathrm{V}(f)$ and $D_2 = \mathrm{V}(x_0^d)$ are linearly equivalent.

EXERCISE 6.4.7. Let $f(x_0, \ldots, x_n)$ and $g(x_0, \ldots, x_n)$ be any two homogeneous polynomials of degree d. Show that the divisors $D_1 = \mathrm{V}(f)$ and $D_2 = \mathrm{V}(g)$ are linearly equivalent.

EXERCISE 6.4.8. Show that linear equivalence is indeed an equivalence relation on the group $\mathrm{Div}(X)$.

DEFINITION 6.4.5. The group $\mathrm{Div}(X)$ divided out by the equivalence relation of linear equivalence is called the *Picard group*, or the *divisor class group*, of X.

EXERCISE 6.4.9. Let D_1 and D_2 be two divisors on $\mathbb{P}^1$. Show that $D_1 \sim D_2$ if and only if they have the same degree.

EXERCISE 6.4.10. Let D_1 and D_2 be two divisors on $\mathbb{P}^n$. Show that $D_1 \sim D_2$ if and only if they have the same degree.

EXERCISE 6.4.11. Show that the map

$$\deg : \mathrm{Div}(\mathbb{P}^n) \to \mathbb{Z}$$

given by

$$\deg(\sum n_V V) = \sum n_V$$

is a group homomorphism, treating $\mathbb{Z}$ as a group under addition.

EXERCISE 6.4.12. Show that the Picard group for $\mathbb{P}^n$ is the group $\mathbb{Z}$ under addition.

6.5. Invertible Sheaves and Divisors

In this section we link divisors with a special type of sheaf, namely invertible sheaves.

In this section we link divisors with sheaves.

DEFINITION 6.5.1. On an algebraic variety X, an *invertible sheaf* $\mathcal{L}$ is any sheaf so that there is an open cover $\{U_i\}$ of X such that $\mathcal{L}(U_i)$ is a rank-one $\mathcal{O}_X(U_i)$-module.[1]

Thus for each open set U_i, we have $\mathcal{L}(U_i)$ is isomorphic to $\mathcal{O}_X(U_i)$ as a $\mathcal{O}_X(U_i)$-module.

We will first see how to intuitively associate a divisor D to an invertible sheaf, which we will denote by $\mathcal{L}_D$. Let $D = \sum n_V V$ be a divisor, where the V are codimension-one subvarieties of X. We know that $n_V = 0$ for all but a finite number of V. We can cover X by open affine sets U_i so that for each i there is a rational function $f_i \in \mathcal{K}(U_i)$ such that

$$(f_i) = D \cap U_i.$$

In other word, the zeros and poles (infinities) of f_i agree with the coefficients n_V of D.

EXERCISE 6.5.1. For the conic $X = V(x^2 + y^2 - z^2)$ in $\mathbb{P}^2$, consider the divisor

$$D = (\frac{1}{\sqrt{2}} : \frac{1}{\sqrt{2}} : 1) + (-\frac{1}{\sqrt{2}} : -\frac{1}{\sqrt{2}} : 1) - (1 : i : 0).$$

On the open set $U = \{(x : y : z) \mid z \neq 0\}$, show that if

$$f(x, y, z) = \frac{x}{z} - \frac{y}{z}$$

then

$$(f) \cap U = D \cap U.$$

Thus each divisor D can be thought of as not only a finite formal sum of codimension-one subvarieties but also as some collection (U_i, f_i), where the $\{U_i\}$ are an open affine cover of X and each $f_i \in \mathcal{K}_X(U_i)$. Working out that these two methods are exactly equivalent when X is a smooth variety but are not necessarily the same when singular is non-trivial. We will take them as the same. Further, this definition of D depends on the choice of open cover, which is hardly unique. The key is that if we write D as some (U_i, f_i) or as some (V_j, g_j), for some other open cover $\{V_j\}$ with $g_j \in \mathcal{K}_X(V_j)$, we require on the overlaps $U_i \cap V_j$ that $\frac{f_i}{g_j}$ have no zeros or poles.

Thus we can write a divisor D as

$$D = (U_i, f_i).$$

[1] Modules are similar to vector spaces, which are always defined over a field of scalars such as $\mathbb{C}$. The scalars for modules, however, may be taken from an arbitrary ring, which is the key difference in the definition. The notion of dimension translates into that of rank for modules. A more detailed account of modules and rank can be found in [**?**] or [**?**].

Definition 6.5.2. Given $D = (U_i, f_i)$, define the invertible sheaf $\mathcal{L}_D$ by setting

$$\mathcal{L}_D(U_i) = \left\{ \frac{g}{f_i} \mid g \in \mathcal{O}_X(U_i) \right\}.$$

Exercise 6.5.2. Suppose that

$$\frac{g}{f_i}, \frac{h}{f_i} \in \mathcal{L}_D(U_i).$$

Show that

$$\frac{g}{f_i} + \frac{h}{f_i} \in \mathcal{L}_D(U_i).$$

For any $\alpha \in \mathcal{O}_X(U_i)$, show that

$$\frac{\alpha g}{f_i} \in \mathcal{L}_D(U_i).$$

(This problem is explicitly showing that each $\mathcal{L}_D(U_i)$ is an $\mathcal{O}_X(U_i)$-module; it is not hard.)

For a divisor $D = (U_i, f_i)$, let

$$g_{ij} = \frac{f_i}{f_j}.$$

We know that on the intersection $U_i \cap U_j$, the functions g_{ij} have no zeros or poles

Exercise 6.5.3. Show that on $U_i \cap U_j \cap U_k$, we have

$$g_{ij} g_{jk} g_{ki} = 1.$$

(For those who know about vector bundles, this means that the invertible sheaf $\mathcal{L}_D$ (or, for that matter, the divisor D) can be though of as a complex line bundle.)

There is another, equivalent, way of associating an invertible sheaf to a divisor D. Again let $D = \sum n_V V$, where each V is a codimension-one subvariety of X. Let U be an open subset of X. Then we define

$$D\big|_U = \sum n_V (V \cap U).$$

For any $f \in \mathcal{K}_X(U)$, define $(f)\big|_U$ to be the divisor of zeros and poles of f on the open set U.

Definition 6.5.3. Define a sheaf $\mathcal{L}_D$ by setting, for each open set U of X,

$$\mathcal{L}_D(U) = \{ f \in \mathcal{K}_X(U) \mid ((f) + D) \cap U \geq 0 \}.$$

More colloquially, $\mathcal{L}_D(U)$ consists of those rational functions on U whose poles are no worse than $-D$.

EXERCISE 6.5.4. Let $D = (U_i, f_i)$ be a divisor on X. Let $\mathcal{L}_D$ be the invertible sheaf associated to D as constructed in Definition 6.5.2 and let $\mathcal{L}'_D$ be the invertible sheaf associated to D as described in Definition 6.5.3. Show that for each open set U in X, $\mathcal{L}_D(U) = \mathcal{L}'_D(U)$. Thus the definitions give two ways to associate the same invertible sheaf to D.

EXERCISE 6.5.5. For $\mathbb{P}^1$ with homogeneous coordinates $(x : y)$, let $D = (1 : 0)$. Let $U_1 = \{(x : y) \mid x \neq 0\}$ and $U_2 = \{(x : y) \mid y \neq 0\}$. Show that $\mathcal{L}_D(U_1)$ is isomorphic to all rational functions of the form $\frac{f(t)}{t}$, where $f(t) \in \mathbb{C}[t]$. (Here let $t = y/x$.) By letting $s = x/y$, show that $\mathcal{L}_D(U_2)$ is isomorphic to $\mathbb{C}[s]$. Finally show that $\mathcal{L}_D(\mathbb{P}^1)$ is not empty.

EXERCISE 6.5.6. For $\mathbb{P}^1$ with homogeneous coordinates $(x : y)$, let $D = -(1 : 0)$. Let $U_1 = \{(x : y) \mid x \neq 0\}$ and $U_2 = \{(x : y) \mid y \neq 0\}$. Show that $\mathcal{L}_D(U_1)$ is isomorphic to the ideal $\{f(t) \in \mathbb{C}[t] : f(0) = 0\}$. (Here let $t = y/x$.) By letting $s = x/y$, show that $\mathcal{L}_D(U_2)$ is isomorphic to $\mathbb{C}[s]$. Finally show that $\mathcal{L}_D(\mathbb{P}^1)$ is empty.

6.6. Basic Homology Theory

Homology and cohomology theories permeate a large part of modern mathematics. There is a serious start-up cost to understanding this machinery, but it is well worth the effort.

Suppose we have a collection of objects $\{M_i\}$, such as a bunch of rings of functions, modules, abelian groups or vector spaces, for $i = 0, 1, 2, \ldots$. Suppose that we have maps

$$d_i : M_i \to M_{i-1}$$

where each d_i is an appropriate map, meaning that if the M_i are rings, then the d_i are ring homomorphisms and if the M_i are vector spaces, then the d_i are linear transformations. We write these out as a sequence

$$\cdots \to M_{i+1} \to M_i \to M_{i-1} \to \cdots,$$

with the map from $M_i \to M_{i-1}$ given by d_i. We require for all i that $\text{Image}(d_i) \subset \text{Kernel}(d_{i-1})$. In other words, $d_{i-1} \circ d_i = 0$, for all i. We call this a *complex*. Frequently the index i is left off, which leads $d_{i-1} \circ d_i = 0$ to be written as the requirement

$$d \circ d = 0.$$

DEFINITION 6.6.1. A sequence

$$\cdots \to M_{i+1} \to M_i \to M_{i-1} \to \cdots$$

is *exact* if for all i we have

$$\text{Image}(d_i) = \text{Kernel}(d_{i-1}).$$

EXERCISE 6.6.1. Let

$$0 \to A_3 \to A_2 \to A_1 \to 0$$

be an exact sequence of either rings or vector spaces, with 0 denoting either the zero ring or the vector space of one point. Show that the map $A_3 \to A_2$ must be one-to-one and the map $A_2 \to A_1$ must be onto.

EXERCISE 6.6.2. Find group homomorphisms so that the corresponding sequence

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

is exact.

In the above, $\mathbb{Z}/2\mathbb{Z}$ denotes the "quotienting" of the integers by the even integers, and hence is the group of two elements $\{0, 1\}$.

DEFINITION 6.6.2. Let

$$\cdots \to M_{i+1} \to M_i \to M_{i-1} \to \cdots$$

be a sequence of abelian groups or vector spaces. Then the i-th *homology* is

$$H_i = \text{Kernel}(d_{i-1})/\text{Image}(d_i).$$

EXERCISE 6.6.3. Show that a sequence of abelian groups, commutative rings or vector spaces is exact if and only if for all i we have $H_i = 0$. (This is just an exercise in applying definitions; there really is not much to show.)

Thus homology is a way of measuring the exactness of a complex.

6.7. Cech Cohomology

In the above section we discussed homology theory. To some extent, there is a dual theory called cohomology. It too is a measure of the non-exactness of a complex. We will not be concerned with the relation between homologies and cohomologies, but will instead just explicitly define the Cech cohomology of an invertible sheaf $\mathcal{L}$ on an algebraic variety X.[2]

Start with a finite open affine cover $\mathcal{U} = \{U_i\}$ of X, for $i = i, \ldots, N$. For any collection $0 \leq i_0 < i_1 < \cdots < i_p \leq N$, let

$$U_{i_0 i_1 \cdots i_p} = U_{i_0} \cap U_{i_1} \cap \cdots \cap U_{i_p}.$$

[2] This whole section is heavily under the influence of Chapter III.4 in Hartshorne [**Har77**].

We know that $\mathcal{L}(U_{i_0 i_1 \cdots i_p})$ is isomorphic to a rank-one $\mathcal{O}_X(U_{i_0 i_1 \cdots i_p})$-module. Then for each p, define

$$\mathcal{C}^p(\mathcal{U}, \mathcal{L}) = \prod_{(0 \le i_0 < i_1 < \cdots < i_p \le N)} \mathcal{L}(U_{i_0 i_1 \cdots i_p}).$$

We want to define a map

$$d : \mathcal{C}^p(\mathcal{U}, \mathcal{L}) \to \mathcal{C}^{p+1}(\mathcal{U}, \mathcal{L})$$

such that

$$d \circ d : \mathcal{C}^p(\mathcal{U}, \mathcal{L}) \to \mathcal{C}^{p+2}(\mathcal{U}, \mathcal{L})$$

is the zero map, which allows us to form a complex whose exactness we can measure. Following notation in Hartshorne [**Har77**], let $\alpha \in \mathcal{C}^p(\mathcal{U}, \mathcal{L})$. This means that $\alpha = (\alpha_{i_0 i_1 \cdots i_p})$. To define $d(\alpha)$ we need to specify, for each $(p+2)$-tuple $(i_0, i_1, \cdots, i_{p+1})$ with $0 \le i_0 < i_1 < \cdots < i_{p+1} \le N$, what the element $d(\alpha)_{i_0 i_1 \cdots i_{p+1}}$ should be. We set

$$d(\alpha)_{i_0 i_1 \cdots i_{p+1}} = \sum_{k=0}^{p+1} (-1)^k \alpha_{i_0 i_1 \cdots \check{i}_k \cdots i_{p+1}},$$

where the $\check{i}_k$ means that we delete the i_k term. Here $\alpha_{i_0 i_1 \cdots \check{i}_k \cdots i_{p+1}}$ stands for the restriction map

$$r_{U_{i_0 i_1 \cdots \check{i}_k \cdots i_{p+1}}, U_{i_0 i_1 \cdots i_k \cdots i_{p+1}}}$$

which exists since $\mathcal{L}_D$ is a sheaf.

In order to make this a bit more concrete, suppose that $\mathcal{U}$ consists of just three open sets U_0, U_1, U_2.

Exercise 6.7.1. Using

$$\begin{aligned} \mathcal{C}^0(\mathcal{U}, \mathcal{L}) &= \mathcal{L}(U_0) \times \mathcal{L}(U_1) \times \mathcal{L}(U_2) \\ \mathcal{C}^1(\mathcal{U}, \mathcal{L}) &= \mathcal{L}(U_{01}) \times \mathcal{L}(U_{02}) \times \mathcal{L}(U_{12}) \\ \mathcal{C}^2(\mathcal{U}, \mathcal{L}) &= \mathcal{L}(U_{012}), \end{aligned}$$

show that

$$d \circ d : \mathcal{C}^0(\mathcal{U}, \mathcal{L}) \to \mathcal{C}^2(\mathcal{U}, \mathcal{L})$$

is the zero map.

Exercise 6.7.2. Let $\alpha = (\alpha_0, \alpha_1, \alpha_2) \in \mathcal{C}^0(\mathcal{U}, \mathcal{L})$ be an element such that $d(\alpha) = 0$. Show that there must be a single element of $\mathcal{L}(X)$ that restricts to α_0 on the open set U_0, to α_1 on the open set U_1 and to α_2 on the open set U_2. This is why we say that something in the kernel of d acting on $\mathcal{C}^0(\mathcal{U}, \mathcal{L})$ defines a global section of the sheaf.

We return to the more general situation. Now that we have a definition for the map d, we have a complex

$$0 \to \mathcal{C}^0(\mathcal{U}, \mathcal{L}) \to \cdots \to \mathcal{C}^N(\mathcal{U}, \mathcal{L}) \to 0,$$

where the first map $0 \to \mathcal{C}^0(\mathcal{U}, \mathcal{L})$ just sends 0 to the zero element of $\mathcal{C}^0(\mathcal{U}, \mathcal{L})$ and the last map $\mathcal{C}^N(\mathcal{U}, \mathcal{L}) \to 0$ sends everything in $\mathcal{C}^N(\mathcal{U}, \mathcal{L})$ to zero.

DEFINITION 6.7.1. The p-th *Cech cohomology group* for the sheaf $\mathcal{L}$ with respect to the open cover $\mathcal{U}$ is

$$H^p(\mathcal{U}, \mathcal{L}) = \left(\ker(d : \mathcal{C}^p(\mathcal{U}, \mathcal{L}) \to \mathcal{C}^{p+1}(\mathcal{U}, \mathcal{L}))/\mathrm{Im}(d : \mathcal{C}^{p-1}(\mathcal{U}, \mathcal{L}) \to \mathcal{C}^p(\mathcal{U}, \mathcal{L}))\right).$$

Thus Cech cohomology is a measure of the failure of exactness for the complex $0 \to \mathcal{C}^0(\mathcal{U}, \mathcal{L}) \to \cdots \to \mathcal{C}^N(\mathcal{U}, \mathcal{L}) \to 0$. This is highly dependent on the choice of open cover $\mathcal{U}$. If this choice really mattered, then Cech cohomology would not be that useful. Luckily, if each of the open sets $U_i \in \mathcal{U}$ is affine, we will always find that the Cech cohomology groups are isomorphic. (See Hartshorne III.4.5 [**Har77**], though if you go to this source directly from this section, it will be rough going, or see Griffiths and Harris [**Gri94**], Chapter 0, section 3, which is still not a "walk in the park".)

One final theoretical point. It is the case that if D_1 and D_2 are linearly equivalent divisors on X, then the corresponding Cech cohomology groups must be isomorphic. This is usually written as

THEOREM 6.7.3. If $D_1 \sim D_2$ for divisors on X, then for all d, we have

$$H^d(X, \mathcal{L}_{D_1}) = H^d(X, \mathcal{L}_{D_2}).$$

We do not prove this but will have some exercises showing this property. Recall in an earlier exercise that divisors up to linear equivalence on projective space $\mathbb{P}^r$ are classified by degree. It is common to replace $\mathcal{L}_D$, for a divisor D of degree n on $\mathbb{P}^r$ by the notation

$$\mathcal{O}(n).$$

Thus people frequently consider the Cech cohomology groups

$$H^d(\mathbb{P}^r, \mathcal{O}(n))$$

which equals $H^d(\mathbb{P}^r, \mathcal{L}_D)$ for any divisor D of degree n.

We spend some time on $\mathbb{P}^1$. Let $(x_0 : x_1)$ be homogeneous coordinates on $\mathbb{P}^1$. There is a natural open cover $\mathcal{U} = \{U_0, U_1\}$ by setting

$$\begin{aligned} U_0 &= \{(x_0 : x_1) : x_0 \neq 0\} \\ U_1 &= \{(x_0 : x_1) : x_1 \neq 0\}. \end{aligned}$$

On U_0, let $s = \frac{x_1}{x_0}$ and on U_1, let $t = \frac{x_0}{x_1}$. On the overlap $U_0 \cap U_1$ we have

$$s = \frac{1}{t}.$$

Now consider the divisor $D = 2(1:0)$.

EXERCISE 6.7.4. Show that $D \cap U_0$ is described by $\mathrm{V}(s^2)$ and that $D \cap U_1$ is described by $\mathrm{V}(1)$ (which is a fancy way of writing the empty set). Show that $2(1:0)$ has an equivalent description as $\{(U_0, s^2), (U_1, 1)\}$.

EXERCISE 6.7.5. Keep with the notation of the above problem. Using that

$$\mathcal{L}_D(U) = \{f(s) \in \mathbb{C}(s) \mid ((f) + D) \cap U \geq 0\}$$

show that

$$\begin{aligned} \mathcal{L}_{2(1:0)}(U_0) &= \left\{\frac{a_0 + a_1 s + \cdots + a_n s^n}{s^2} \mid a_0, \ldots, a_n \in \mathbb{C}\right\} \\ \mathcal{L}_{2(1:0)}(U_1) &= \{b_0 + b_1 t + \cdots + b_m t^m \mid b_0, \ldots, b_m \in \mathbb{C}\}. \end{aligned}$$

On the overlap $U_{01} = U_0 \cap U_1$, we will write the restriction maps as

$$r_{U_0, U_{01}}(f(s)) = f(s)$$

and

$$r_{U_1, U_{01}}(g(t)) = g\left(\frac{1}{s}\right).$$

EXERCISE 6.7.6. Show that

$$d : \mathcal{C}^0(\mathcal{U}, \mathcal{L}_{2(1:0)}) \to \mathcal{C}^1(\mathcal{U}, \mathcal{L}_{2(1:0)})$$

is given by

$$d\left(\frac{a_0 + a_1 s + \cdots + a_n s^n}{s^2}, b_0 + b_1 t + \cdots + b_m t^m\right)$$
$$= \frac{b_1}{s} + \cdots + \frac{b_m}{s^m} + \frac{a_0}{s^2} - \frac{a_1}{s} - a_2 - a_3 s + \cdots - a_n s^{n-2}.$$

EXERCISE 6.7.7. Show that

$$\left(\frac{a_0 + a_1 s + \cdots + a_n s^n}{s^2}, b_0 + b_1 s + \cdots + b_m t^m\right)$$

is in the kernel of the map d if and only if $a_k = 0$ and $b_k = 0$ for $k > 2$ and $a_0 = b_2, a_1 = b_1, a_2 = b_0$.

EXERCISE 6.7.8. Based on the previous exercise, explain why we can consider $H^0(\mathbb{P}^1, \mathcal{L}_{2(1:0)})$ as the set of all degree homogeneous polynomials in x_0 and x_1, or in other words

$$H^0(\mathbb{P}^1, \mathcal{L}_{2(1:0)}) = \{a x_0^2 + b x_0 x_1 + c x_1^2 \mid a, b, c \in \mathbb{C}\}.$$

EXERCISE 6.7.9. By similar reasoning, show that for all $d > 0$, we have

$$H^0(\mathbb{P}^1, \mathcal{L}_{d(1:0)}) = \{b_d x_0^d + b_{d-1} x_{d-1} x_1 + \cdots + b_0 x_1^d \mid a_k \in \mathbb{C}\}.$$

(This problem requires you to generalize the last five exercises. Thus it will take a bit to write up.)

EXERCISE 6.7.10. Show that

$$H^0(\mathbb{P}^1, \mathcal{L}_{-2(1:0)}) = 0.$$

(This involves showing that $\mathcal{L}_{(-2)1:0)}(\mathbb{P}^1)$ is empty.)

EXERCISE 6.7.11. By similar reasoning, show that for all $d > 0$, we have

$$H^0(\mathbb{P}^1, \mathcal{L}_{-d(1:0)}) = 0.$$

The next step in the development of Cech cohomology for divisors would be to put Riemann-Roch Theorem into the this language. We will simply state the theorem:

THEOREM 6.7.12 (Riemann-Roch Theorem). Let X be a smooth curve and let D be a divisor on X. Then

$$\dim H^0(X, \mathcal{L}_D) - \dim H^1(X, \mathcal{L}_D) = \deg(D) + 1 - g.$$

The right hand side is exactly what we had in Chapter 3. The key is showing that the left hand side is equivalent to what we had earlier. Thus we would need to how that

$$(D) = \dim H^0(X, \mathcal{L}_D),$$

which is not that hard, and

$$(K - D) = \dim H^1(X, \mathcal{L}_D),$$

which does take work.

As the above is only true for curves, this is only the beginning. For example, there is a Riemann-Roch for surfaces:

THEOREM 6.7.13 (Riemann-Roch for Surfaces). Let X be a smooth projective surface and let D be a divisor on X. Then

$$\dim H^0(X, \mathcal{L}_D) - \dim H^1(X, \mathcal{L}_D) + \dim H^2(X, \mathcal{L}_D) = \left(\frac{D \cdot D - D \cdot K}{2}\right) + 1 + p_a.$$

The right hand side means the following. Since in general divisors are linear combinations of co-dimension one subvarieties, divisors on surfaces are curves. The $D \cdot D$ denotes the intersection number of D with itself (such numbers have to be carefully defined). The divisor K is the surface analog of the canonical divisor;

thus $D \cdot K$ is the intersection number of the curves D and K. The p_a is something called the arithmetic genus. I

The left hand side, namely the alternating sum of the various dimensions of the Czech cohomology groups, is called the Euler characteristic of the divisor. In general, we have:

DEFINITION 6.7.2. For a smooth projective variety X of dimension n, the Euler characteristic of a divisor D is

$$\chi(D) = \sum_{i=0}^{n} (-1)^k \dim H^k(X, \mathcal{L}_D).$$

All generalizations of Riemman-Roch have the form

$$\chi(D) = \text{some formula capturing geometry and topology.}$$

In this section, we saw how computations of Czech cohomology on $\mathbb{P}^1$ come down to the manipulation of polynomials, which is precisely how we started this book. The power of this section's machinery lies in how many different areas of math (even those far from the joys of polynomial manipulation) can be recast and informed by the language of cohomology . For example, much of the work in algebraic geometry in the last part of the 20th century was developing the correct generalizations of Riemann-Roch. We predict mathematicians in the 21st century will continue this path, but now with an emphasis on the correct generalizations of cohomology theories. (For the expert, we are thinking "motives.") To the student, you are now on the cusp of the beginnings of current algebraic geometry.

APPENDIX A

A Brief Review of Complex Analysis

One rationale for this little excursion is the idea behind the saying, "If you don't use it, in this case complex analysis, you lose it." We would like to make the reading of the book as painless as possible.

A.1. Visualizing Complex Numbers

A complex number $z = a + bi$ is plotted using rectangular coordinates as distance a away (left or right depending on the sign of a) from the the origin and distance b away (up or down depending on the sign of b) from the origin. We can also graph complex numbers by using polar coordinates where $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$. This means that the equations $a = r\cos\theta$ and $b = r\sin\theta$ facilitate an easy conversion from polar to rectangular and vice versa.

A.2. Power Series

A power series about a, is any series that can be written in the form,

$$\sum_{n=0}^{\infty} c_n(x-a)^n$$

where c_n are called the coefficients of the series.

Once we know that a power series has a radius of convergence, we can use it to define a function.

A.3. Residues

Let C be a Jordan curve about 0. Now, consider the contour integral

$$\oint_C \frac{e^z}{z^3}\,dz$$

A.4. Liouville's Theorem

A bounded entire function is constant, i.e., a bounded complex function $f : \mathbb{C} \to \mathbb{C}$ which is holomorphic on the entire complex plane is always a constant function. Let us define in a very brief and hopefully intuitive manner some of the words used in Liouville's Theorem. "Bounded" means that the function f satisfies the so-called polynomial bound condition,

$$|f(z)| = c|z^n|$$

for some $c \in \mathbb{R}$, $n \in \mathbb{Z}$, and all $z \in C$ with sufficiently large.

"Holomorphic functions" are complex functions defined on an open subset of the complex plane which are differentiable, in fact infinitely differentiable.

Bibliography

[AG06] Avner Ash and Robert Gross. *Fearless Symmetry. Exposing the Hidden Patterns of Numbers*. Princeton University Press, Princeton, NJ, 2006. With a foreword by Barry Mazur.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, 3rd edition, 2007.

[Ful69] William Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry*. Mathematics Lecture Notes Series. W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes written with the collaboration of Richard Weiss.

[Gib98] C. G. Gibson. *Elementary Geometry of Algebraic Curves: an Undergraduate Introduction*. Cambridge University Press, Cambridge, 1998.

[Gri94] Joseph Griffiths, Phillip; Harris. *Principles of Algebraic Geometry*. Wiley Classics Library. John Wiley & Sons, New York, 1994. Reprint of the 1978 original.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[Kir92] Frances Kirwan. *Complex Algebraic Curves*, volume 23 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1992.

Index

R_d, 203
Spec$R$, 168
j-invariant, 70, 71, 73

absolutely convergent, 96
affine
  chart, 200
affine change of coordinates, 7
affine space, 149
algebra, 176
algebraic Set, 151

canonical form, 72
Cech cohomology, 234
cells, 96
change of coordinates
  complex, 16
  equivalent, 14, 16
  projective, 23
chord-tangent composition law, 57
closed, 166
conics, 1
coordinate ring, 154
cubic
  canonical form, 72
  Weierstrass normal form, 68
cubic curve, 47
curve
  degree, 100
  irreducible, 100
  singular, 33, 48
  smooth, 33

degree
  curve, 100
  divisor, 120

derivation, 176
dimension, 182
  of a variety, 181
Diophantine equation, 30
discriminant, 41
divisor, 120, 226
  degree, 120
  effective, 120, 227
  hyperplane, 125
  linearly equivalent, 124, 227
  principal, 121

ellipse, 2
elliptic curve, *see also* cubic
equivalence relation, 91, 114, 116

flex, 49, 53
formal power series, 157
function field, 164

general position, 62
genus
  arithmetic, 104
  topological, 103
group, 57, 77, 93
  Abelian, 57

Hessian, 53
  curve, 54
homeomorphism, 25
homogeneous, 20, 51
homogeneous coordinates, 20
hyperbola, 3

ideal, 153
  maximal, 159, 165, 168

of X, 170
prime, 159, 168
radical, 154
inflection point, 49, 53

Jacobian matrix, 184

lattice, 94
local ring, 173
localization, 175

map
birational, 192
matrix
equivalence, 39
symmetric, 37
moduli space
cubic, 71
multiplicatively closed set, 174
multiplicity
intersection, 52
of f at p, 107
of a root, 105
root, 50, 51

normal subgroup, 92

open, 166
order
group element, 63

parabola, 2
parameterization
rational, 26
parametrization
cubic, 71
partition, 91
point
geometric, 169
point of inflection, 63
point:rational, 80
points of inflection, 54
polynomial
homogeneous, 202
presheaf, 220
associated sheaf, 224
prime
spectrum, 168
projective
line, 24
plane, 19
Pythagorean Theorem, 28

quadratic form, 38
quotient group, 91

radical, 154, 158
rational map, 191
resultant, 110
ring
formal power series, 157
graded, 203
homogeneous, 203
local, 174
local at p, 173
Noetherian, 156
of regular functions, 114
root, 50
multiplicity, 50

sheaf, 222
germ, 223
invertible, 229
stalk, 223
singular, 183
six-to-one correspondence
cubic
canonical form, 73
Spec(R), 168
spectrum, 168

tangent
space, 176, 177
topology, 166
finite complement, 167
Hausdorff, 167
standard on $\mathbb{C}^n$, 167
standard on $\mathbb{R}$, 166
Zariski, 168, 170
torus, 94
transcendence degree, 181

uniformly convergent, 97

variety
affine, 159

reducible, 159

Weierstrass $\wp$-function, 95, 96

Zariski
closure, 170
topology, 170
zero set, 1