Projective Geometry and its Applications

Ernie Esser
University of Washington
Advisors: Professor Jack Lee and Robert Hladky
June 2003

Abstract

This paper is a survey of the subject of projective geometry presenting both the theoretical foundation as well as historical and modern applications in mathematics and other fields. Some interesting examples regard how projective geometry is used in perspective drawing, which has applications in areas such as computer graphics and even forensic science. Equivalent definitions and models of projective spaces will be compared. A main focus of this paper will be on the elementary applications of projective geometry to algebraic geometry and why the natural space to study algebraic curves is a projective space over an algebraically closed field such as the complex projective plane. The study of equivalence, tangents and intersections of projective algebraic curves will be presented from a geometric perspective, eventually leading to a presentation of Bézout’s theorem. The group structure on a cubic will be analyzed. Finally this paper will briefly discuss the interpretation of projective curves as surfaces. Specifically, parameterizations of conic sections and elliptic curves in the complex projective plane come from model surfaces they are topologically equivalent to, which in these cases are respectively the sphere ($\mathbb{P}^1(\mathbb{C})$) and the torus ($\mathbb{C}/\Lambda$, where $\Lambda$ is a lattice).
# Contents

1 Introduction ........................................... 3

2 Some Applications of Projective Geometry ............... 3
   2.1 Projective Space in a Projective Nutshell .......... 4
   2.2 Central Projection .................................. 5
   2.3 Looking at Perspective Drawings .................. 6
   2.4 Computer Graphics .................................. 8
   2.5 Getting 3D Information from 2D pictures .......... 9
   2.6 Algebraic Geometry and Bézout’s Theorem .......... 11
   2.7 Group Structure on a Cubic and Elliptic Curves .... 12

3 Projective Space Preliminaries .......................... 14
   3.1 Definitions ........................................ 14
   3.2 Models ............................................. 15
   3.3 Projective Line .................................... 16
   3.4 Two Classical Results .............................. 17

4 Algebraic Curve Preliminaries .......................... 22
   4.1 Lines and Curves ................................... 22
   4.2 Points at Infinity .................................. 23
   4.3 Intersections ....................................... 23
   4.4 Multiplicities and Singular Points ................ 24
   4.5 Tangents .......................................... 26
   4.6 Flexes ............................................. 27
   4.7 Projective Transformations and Equivalence ...... 27

5 Classification by Projective Equivalence ............... 31
   5.1 Lines .............................................. 31
   5.2 Conics ............................................. 31
   5.3 Cubics ............................................ 31

6 Bézout’s Theorem ....................................... 32
   6.1 Resultants and Main Idea ........................... 32
   6.2 Sketch of Proof .................................... 33

7 Group Structure on a Cubic ............................. 34
   7.1 Definition of \( \ast \) Operation .................... 34
   7.2 Definition and Properties of Addition ............. 34

8 Parameterizations of Conics and Cubics ................ 35
   8.1 Elliptic Curves and Functions ..................... 35
1 Introduction

Although elements of projective geometry such as the invariance of the cross ratio under projection have been known since the time of the Greeks [1], the subject didn't start to come into its own until during the Renaissance when people such as architect/engineer Filippo Brunelleschi and artists Leon Battista Alberti and Piero della Francesca studied linear perspective in art, which is essentially an application of projective geometry to perspective drawing.

Even with this good start, the subject of projective geometry developed slowly over the next few hundred years. Major contributions were however made by Desargues, Pascal, Brianchon, and La Hire. In the 1800s Poncelet, Chasles, Steiner, Von Staudt and Cremona initiated a resurgence of the study of projective geometry by developing a sturdier mathematical foundation of the subject using more algebraic approaches and considering interesting extensions such as the meaning of imaginary points and lines.

The subject also continued to develop along with algebraic geometry, which I will not attempt to provide a history of. Projective spaces are an essential feature of algebraic geometry, i.e: the study of varieties, which are the sets defined by simultaneous polynomial equations. A reason for this is that by considering projective varieties, the zero sets of homogeneous polynomials, the variety will in general also include additional points, namely points at infinity, which allows intersections of curves to be treated in a more consistent manner.

For example, in a projective plane all lines intersect. The geometry of the projective plane is non-Euclidean because there are no parallel lines. Lines that seem parallel in an affine view actually intersect at a point at infinity. This consistency makes it possible to prove stronger results in many cases, which was why Gibson [2] presents Bézout's theorem about the intersections of curves in the complex projective plane.

There are of course many additional advanced applications of projective spaces which won't be analyzed at all in this paper. Projective spaces play an important role in algebraic topology since for example they are the characterization spaces for vector bundles. Projective spaces over the quaternions and even the octonians [6] are of recent interest since they have interesting applications to physics topics such as quantum logic.

2 Some Applications of Projective Geometry

This section introduces in greater detail some applications of projective geometry. Perspective drawing, computer graphics and forensic science examples are presented to get a feel for how real projective spaces can be used. Then applications to algebraic geometry, elliptic curves and group structure on cubics are introduced.
2.1 Projective Space in a Projective Nutshell

**Definition 2.1.** In general, for any field \( K \), the \( n \)-dimensional projective space \( PK^n \) is the set of lines through the origin in \( K^{n+1} \).

For example, consider the real projective plane \( \mathbb{P}^2 \), which is the one most related to perspective. \( \mathbb{P}^2 \) is defined as the set of lines through the origin in \( \mathbb{R}^3 \). This can also be written as the quotient

\[
\mathbb{P}^2 = (\mathbb{R}^3 - 0)/\mathbb{R}^*
\]

where \( \mathbb{R}^* \) equals the multiplicative group of non-zero real numbers. Similarly, if an equivalence relation is defined by \( x \sim y \) if \( x = \lambda y \), where \( x, y \in \mathbb{R}^3 \) and \( \lambda \in \mathbb{R} \), then \( \mathbb{P}^2 \) is exactly the set of equivalence classes [14]. The corresponding definition of higher dimensional projective spaces is analogous.

A way to visualize \( \mathbb{P}^2 \) is to consider lines through the origin in \( \mathbb{R}^3 \) that intersect an affine plane such as the one defined by \( z = 1 \). There is a one to one correspondence between points on the plane \( z = 1 \) and \( \mathbb{P}^2 \). However, \( \mathbb{P}^2 \) contains additional points at infinity, which in this picture (Figure 1) are the lines through the origin that don't intersect the plane. (In fact, there is a projective line at infinity defined by lines through the origin in \( \mathbb{R}^2 \).

![Figure 1: View of the Real Projective Plane](image)

The general definition for expressing a point in homogeneous coordinates is given below.

**Definition 2.2.** For any field \( K \), a point \( X \) in \( PK^n \) is represented in homogeneous coordinates \( (x_1 : x_2 : \ldots : x_n : z) \), which is an equivalence class of all points of the form \( \lambda(x_1, x_2, \ldots, x_n, z) \) for \( \lambda \in K \).

Thus points in \( \mathbb{P}^2 \) are written \( (x : y : z) \). A point can be represented in the affine view \( z = 1 \) by \( (x : y : 1) \) if the third coordinate is not zero. Points at infinity occur when \( z = 0 \).
A line \( L \) in \( \mathbb{P}^2 \) is defined by a plane through the origin in \( \mathbb{R}^3 \). The line at infinity is defined by the plane \( z = 0 \), which includes all the points at infinity.

### 2.2 Central Projection

Now let's return to the discussion of projective geometry in art. Perspective drawing is just the representation of three-dimensional objects on a two-dimensional plane via central projection, which for a point \( P \) and a plane \( A \) such that \( P \not\in A \) takes any point \( Q \) and defines a point \( Q' \in A \) by \( Q' = \frac{PQ}{PQ} \cap A \), the intersection of the line defined by \( P \) and \( Q \) with the plane. (See figure 2)

[3] If \( PQ \) is parallel to the plane \( A \), then it corresponds to a point at infinity. Note that a parallel projection can be obtained by letting \( P \) move infinitely far away from \( A \).

![Figure 2: Central Projection](image)

A central projection takes points and radial lines to points. It takes non radial lines to lines. This is because any two lines connecting \( P \) to the non radial line define a plane through the origin in \( \mathbb{R}^3 \). This plane by definition is a line in \( \mathbb{P}^2 \), and the intersection of this plane with the image plane \( A \) is clearly a line assuming the planes do intersect. It's worth noting that conic sections also project to conic sections.

\( A \) is actually a particular affine view of the projective plane. The central projection onto \( A \) is the set of lines through the origin in \( \mathbb{R}^3 \) that intersect \( A \). Every point on \( A \) corresponds to a unique line through the origin and therefore a unique point in \( \mathbb{P}^2 \). So \( A \) maps injectively into the projective plane missing only the points at infinity, which are the lines through the origin in \( \mathbb{R}^3 \) which are parallel to \( A \). As mentioned before, there is in fact a projective line at infinity.

Much of the sense of perspective in central projection drawings comes from the vanishing points, which are the points on the image plane \( A \) that correspond to points at infinity in \( \mathbb{P}^3 \). For example parallel train tracks in \( \mathbb{R}^3 \) intersect at a single point at infinity in \( \mathbb{P}^3 \). As figure 3 shows, the image of this point under the map of central projection onto \( A \) is the familiar vanishing point on the horizon where in the image the two rails seem to intersect. There can be
Figure 3: Vanishing point of train tracks in *O Brother, Where Art Thou?*

infinitely many vanishing points. There is one for each line in \( \mathbb{R}^3 \). For example the horizon line is actually a vanishing line for the ground plane.

2.3 Looking at Perspective Drawings

Unfortunately, naive applications of central projection to world scenes will not necessarily produce realistic looking art. For example, although a person’s field of vision is commonly modelled as a 90 degree viewcone [4], paintings do not usually include this full range of vision. This is to avoid distortion that appears on the periphery. The distorting effect of circles for example being mapped to ellipses is more pronounced away from the center of the viewcone, (which also means viewing direction can be an issue). Of course, if the observer looks at the picture from the correct location, namely the origin denoted \( P \) in figure 2, then everything will look fine, but odds are that at an art gallery the good spot will already be taken. Representing smaller fields of vision makes distortions less glaring for observers in the wrong location.

This leads to the question of what information a painting provides about this correct location of the origin \( O \). What can be seen is a foreshortening effect and the vanishing points on the image plane of lines that are parallel in the world. For simplicity, consider a drawing of a cube, which has three sets of parallel lines in mutually perpendicular directions. At least one of these directions must not be parallel to the image plane. The cube is drawn in one, two or three point perspective depending on how many of these three directions are not parallel to the image plane. \(^1\) For example, when only one direction is not parallel, the cube is in one point perspective as in figure 6. Parallel lines in the other two

\(^1\)If the size of the viewcone is greatly expanded, four, five and even six point perspective drawings of the cube are possible. [15]
directions project to parallel lines on the image planes. In this case the origin lies somewhere on the line perpendicular to the image plane through the one vanishing point, but the location on this line can't be determined unless more information, such as the real dimensions of the cube, are known.

For a cube in three point perspective, the location of the origin can be determined from the three vanishing points: $v_1$, $v_2$ and $v_3$. Since they are the vanishing points of three sets of mutually perpendicular lines, the origin $O$ must lie at the point (unique if we restrict our attention to one side of the image plane) where $Ov_1$, $Ov_2$ and $Ov_3$ are mutually perpendicular. This follows from the fact that if lines $l_1$ and $l_2$ in the world are perpendicular to each other then since $Ov_1$ and $Ov_2$ are parallel to those lines, they must then meet at a right angle at $O$. $O$ is one of the two points obtained by taking the intersections of the three

Figure 4: Using vanishing points of perpendicular lines

spheres having as diameters the line segments $\overline{v_1v_2}$, $\overline{v_2v_3}$ and $\overline{v_1v_3}$ [3]. The three angles at which these lines meet are then each inscribed in a semicircle, thus making them right angles. In figure 5 for example, since the vanishing points
are conveniently located at the vertices of an equilateral triangle, say with sides of length one, the origin must then be located a distance of $1/\sqrt{3}$ away from the triangle's centroid in the direction perpendicular to the image plane.

Figure 5: Rectangular Prism in three point perspective

2.4 Computer Graphics

Projective geometry also plays a key role in computer graphics. Basic 3D computer graphics, (ignoring all the optimization tricks), is about projecting world scenes onto an image plane which is in this case the monitor. To move things around in the world, affine transformations, which are just linear transformations plus translations, are used [16]. A 3 by 3 matrix no longer contains enough information to perform these transformations, and this is essentially why 4 by 4 matrices are used to transform points in 3-space now represented in homogeneous coordinates $(x, y, z, 1)$. For example, a pure translation matrix $T$ that takes a column vector $\mathbf{x} = [x \ y \ z \ 1]^T$ to $\mathbf{x} + \mathbf{x}_0$ is defined by

$$T = \begin{bmatrix} 1 & 0 & 0 & x_0 \\ 0 & 1 & 0 & y_0 \\ 0 & 0 & 1 & z_0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$  

The above relationship is related to an equivalence between affine and projective transformations that will be discussed later. Affine transformations in
\( \mathbb{R}^3 \) extend to projective transformations in \( P\mathbb{R}^3 \), so \((x, y, z, 1)\) can be thought of as a point in \( P\mathbb{R}^3 \). Also, projective maps in \( P\mathbb{R}^3 \) arise from invertible linear maps in \( \mathbb{R}^4 \), of which \( T \) above is an example.

### 2.5 Getting 3D Information from 2D pictures

Projective geometry techniques can also be used to get information about a three dimensional scene from its projection onto an image plane. This usually requires knowing or assuming some measurements or ratios of line segments of the actual objects being depicted. For example, in figure 6 if we only assume the object is a rectangular prism drawn in one point perspective, then as stated above, the line the origin lies on is determined, but the distance from the image plane is not. However, if we instead assume the picture is of a cube, then the location of the origin is determined. A trick for determining this is to look at the vanishing point of the diagonal line through \( a \) and \( b \) in figure 6 [18]. The

![Figure 6: Cube in one point perspective](image)

plane the left side of the cube lies on has a vertical vanishing line \( l \) which goes through \( v \). The diagonal line through \( a \) and \( b \), since it also on this plane, must have a vanishing point \( v_d \) somewhere on \( l \). As is clear in figure 4 the angle \( \theta \) that diagonal line makes with the ground in the world is the same as the angle
the line through the origin and $v$ makes with a plane parallel to the ground. This angle is determined by the width to height ratio of the cube, which is just 1. Thus $\theta$ is a 45 degree angle. So if $h$ is the image distance between $v_d$ and $v$, then the origin must be a distance of $h$ away from the image plane.

One of the applications of determining how measurements in a photo correspond to real life is forensic science. (Actually computer vision and robotics is probably a more significant application, but it will be more entertaining to consider a forensic science example.) As an example forensic science problem done geometrically, consider a possible criminal investigation into the kidnapping of Kermit the Frog. Suppose figure 7 is a photo of the kidnapper's escape from

Figure 7: Kermit's kidnapper is photographed making his escape

Kermit's cubical home.

Figure 8: Kermit the Frog

Figure 8: Kermit the Frog

10
The detective wants to use the height $h$ of the house to measure the height of the criminal off in the distance. As luck would have it, the front of the home is parallel to the image plane so the cube is in one point perspective. This is not necessary to determine the person’s height, but it simplifies some computations that will later be done with this example. Geometrically, if we assume the person is standing vertically on the ground, we know that the line $\overline{BB}$ is on the ground plane and therefore has a vanishing point on the horizon, ie: the vanishing line of the ground plane. Now by construction the line $\overline{vt}$ is parallel to $\overline{BB}$ and shifted vertically upward by exactly the height of the person. By finding the intersection $t'$ with the edge of Kermit's house, we see how tall the person is relative to that edge. Thus in this picture, the kidnapper's height is $8h$. Although it seems strange that this person is taller than even the door, it makes sense given that this is house is scaled to Kermit's dimensions and Kermit, being a frog, is rather short.

Some information about the 3D scene has been reconstructed from a single photo, (which will hopefully lead to Kermit’s safe return). Similar reconstruction techniques are also being used to create 3D models that correspond to famous Renaissance paintings such as Masaccio’s Trinità and Piero della Francesca’s "La Flagellazione di Cristo."

Cross ratios and more generalized algebraic techniques can also be used to reconstruct these 3D scenes. [5] If more photos, ie: more than one affine view of a scene are provided, then much more information can be determined. For example, if nothing in any picture blocks the view of something else, then four affine views should be enough to recover all the three dimensional information. In general, $n+1$ affine views of curves in $\mathbb{P}^n$ contain all the information necessary to reconstruct the curves.

### 2.6 Algebraic Geometry and Bézout’s Theorem

The previous digressions provide a good feel for how real projective spaces function, but the algebraic geometry applications worked out in this paper will for the most part be done in the complex projective plane $\mathbb{P}^2$. With minimal background on properties of $\mathbb{P}^2$ and on curves, tangents, multiplicities and intersection numbers in $\mathbb{P}^2$ it is possible to state and prove Bézout’s Theorem as presented in [2].

**Theorem 2.1. (Bézout’s Theorem)**

Let $F$, $G$ be curves in $\mathbb{P}^2$ of degrees $m$ and $n$ with no common component. Then the sum of the intersection numbers at the points of intersection (ie: the number of intersections counted with multiplicity) is exactly $mn$.

This theorem implies a useful weaker form for curves in projective planes over arbitrary fields.

**Corollary 2.1.** For any field $K$, if $F$ and $G$ are curves of degree $m$ and $n$ in $\mathbb{P}^2(K)$ having no common component, then they intersect in no more than $mn$ distinct points.
This weaker corollary also illustrates the benefit of working in a projective plane over an algebraically closed field like the complex numbers. For example, in $P\mathbb{R}^2$, the parabola $y^2 - xz = 0$ does not intersect the line $x + z = 0$. Figure 9 shows an affine view of this situation for $z = 1$. In $P\mathbb{C}^2$ there are exactly two points of intersection represented in homogeneous coordinates as $(-1; i; 1)$ and $(-1; -i; 1)$. This of course is consistent with Bézout's theorem.

2.7 Group Structure on a Cubic and Elliptic Curves

Bézout's theorem is a powerful result that among other things leads to the ability to define a group structure on a cubic. The key operation $\ast$ in defining this group structure, as will be discussed later, is take two simple points $P$ and $Q$ on a cubic and produce a third $P \ast Q$ determined by the intersection of a line through those two points with the cubic. The intersections of a line and a cubic is a special case of the scenario Bézout's theorem describes, so the theorem implies that this line intersects the cubic three times counting with appropriate multiplicity.

There are also a few subtler details surrounding the $\ast$ operation. $P$ and $Q$ are chosen to be simple, i.e. of multiplicity 1, so that the tangent is defined at $P$ and $Q$. (These definitions will be made more precise later.) The reason this is necessary is that if $P$ and $Q$ coincide and the point is not simple (i.e. singular), then the tangent is not uniquely defined there and there is no way to uniquely determine a third point. Of course, if the line is tangent to $P$ or $Q$ than one of the intersections occurs with multiplicity 2 and $P \ast Q$ is just $P$ or $Q$. There is also the special case when $P$ or $Q$ is a point of inflection, at which the tangent line intersects the point with multiplicity 3. This will be made more precise
later. The upshot is that addition of points on a cubic can be defined in terms of the above operation $\star$ and the identity $O$, which is chosen to be a point of inflection.

$$P + Q = (P \star Q) \star O$$

The set of simple points on a cubic then becomes an abelian group with that definition of addition. The group structure of irreducible cubics with one singular point, namely cuspidal cubics and nodal cubics, which are defined later in the paper, are respectively isomorphic to $\mathbb{C}^+$ and $\mathbb{C}^*$.

Elliptic curves are non-singular cubics in the projective plane. Non-singular means all points are simple and also implies the curve is irreducible. Here for simplicity we will work in the complex projective plane. The group structure on an elliptic curve is isomorphic to a quotient group $\mathbb{C}/\Lambda$ where $\Lambda$ is a lattice.

![Figure 10: Lattice generated by w1 and w2](image)

**Definition 2.3.** A lattice $\Lambda$ is a subgroup of $\mathbb{C}^+$ generated by two complex numbers $\lambda_1$ and $\lambda_2$ with non-real quotient.

Thus it consists of all complex numbers of the form $n_1\lambda_1 + n_2\lambda_2$ where $n_1, n_2$ are integers.

The case where $\lambda_1$ and/or $\lambda_2$ is zero corresponds to cuspidal and nodal cubics respectively, which aren't elliptic curves because they are singular. However, their associated groups are still isomorphic to $\mathbb{C}/\Lambda$ where $\Lambda$ is now a degenerate lattice. If only one of $\lambda_1$ or $\lambda_2$ is zero, the group is $\mathbb{C}^*$. If both are zero, then the group is $\mathbb{C}^+$. The difficult case is when neither is zero. In this general case for elliptic curves, which Gibson classifies as general non-singular cubics, a
parameterization can be defined in terms of the Weierstrass \( \wp \) function and its
derivative that gives a correspondence between points of \( \mathbb{C}/\Lambda \) and points on the
elliptic curve. [17] Addition defined by the group structure of \( \mathbb{C}/\Lambda \) corresponds
exactly to the addition rules already sketched for points of elliptic curves.

3 Projective Space Preliminaries

3.1 Definitions

Projective spaces over arbitrary fields have already been defined in terms of
radial lines through the origin 2.1. However, there is also a purely axiomatic
definition.

Definition 3.1. A projective space can be defined by the following three axioms:
[6]

- For any two distinct points \( p, q \), there is a unique line \( \overline{pq} \) on which they
  both lie.
- For any line, there are at least three points lying on this line.
- If \( a, b, c, \) and \( d \) are distinct points and there is a point lying on both \( \overline{ab} \)
  and \( \overline{cd} \), then there is a point lying on both \( \overline{ac} \) and \( \overline{bd} \).

Axioms for the projective plane are equivalent to the above axioms in two
dimensions, but are worth writing down because they are slightly simpler and
can also be made self-dual.

Definition 3.2. A projective plane can be defined by the following axioms: [6]

- For any two distinct points, there is a unique line on which they both lie.
- For any two distinct lines, there is a unique point which lies on both of
  them.
- There exist four points, no three of which lie on the same line.
- There exist four lines, no three of which have the same point lying on
  them.

Actually the fourth axiom listed for projective planes is superfluous since it
follows from the first three, but with it included, definition 3.2 is more apparently
self-dual. The definition remains the same with 'point' and 'line' interchanged
as long as the syntax is also updated to correct what lies on what.

Projective space also could have been defined axiomatically in terms of the
projective plane axioms by defining it be a linear space having the property that
and 2-dimensional linear variety is a projective plane [12]. A linear space is a
set that satisfied the first two projective plane axioms listed. A subset \( V \) of a
linear space is a linear variety if given two distinct points \( x \) and \( y \) of \( V \), the line
\( \overline{xy} \) is also a subset of \( V \).
An example that makes it easy to visualize the axioms is the smallest projective plane $PZ_2^2$, a projective plane over the field $Z_2$ having only two elements. $PZ_2^2$ is also known as the Fano plane. There are seven points, namely: $(0 : 0 : 1)$, $(1 : 0 : 1)$, $(0 : 1 : 1)$, $(1 : 1 : 1)$, $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(1 : 1 : 0)$. There are also seven lines, namely: $x = 0$, $y = 0$, $z = 0$, $x = y$, $y = z$, $z = x$, $z = x + y$ [2]. This can be summed up in the picture shown in figure 11. Of course, $PZ_2^2$ can also be thought of as the set of lines through the origin in $Z_2^3$.

The rest of this paper will be concerned with mainly real and complex projective spaces, and the more useful definition for our purposes is definition 2.1 and the equivalence class definition, both of which certainly satisfy the above axioms. The reason for this is that an algebraic treatment of curves in projective space relies on working with points written in homogeneous coordinates (as defined in definition 2.2).

3.2 Models

Two useful ways to view the real projective plane are the sphere and hemisphere models. Since $P\mathbb{R}^2$ is defined by lines through the origin in $\mathbb{R}^3$ and each such line intersects the sphere $x^2 + y^2 + z^2 = 1$ in diametrically opposite points, $P\mathbb{R}^2$ turns out to be homeomorphic to quotient space defined by the 2-sphere with diametrically opposite points identified. Compactness of the
sphere immediately implies that $\mathbb{P}\mathbb{R}^2$ is compact. Equivalently, lines through the origin in $\mathbb{R}^3$ intersect the hemisphere defined by taking $z \geq 0$ on the unit sphere once everywhere except on the boundary where they again interest in diametrically opposite points. So the hemisphere model is just the hemisphere with diametrically opposite points on its boundary identified.

The representation of the n-dimensional projective space over a field $\mathbb{K}$ as points in $\mathbb{K}^n$ plus points at infinity, as was done for $\mathbb{P}\mathbb{R}^2$ in figure 1, is useful for seeing what these points at infinity are in terms of lower dimensional projective spaces. The points at infinity are points of the form $(x_1 : x_2 : \ldots : x_n : 0)$, namely the lines through the origin in $\mathbb{K}^n$, which is the definition of $\mathbb{P}\mathbb{K}^{n-1}$. For example $\mathbb{P}\mathbb{C}^1$ is the complex plane plus the point at infinity $\mathbb{C} \cup \infty$. $\mathbb{P}\mathbb{C}^2$ is then $\mathbb{C}^2 \cup \mathbb{P}\mathbb{C}^1$.

One final interesting way of representing a projective plane is via a surface representation, namely the unit square with sides identified as in figure 12. Since

\[
\begin{array}{c}
\begin{array}{c}
\text{a} \\
\text{b}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\text{b} \\
\text{a}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\text{c}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\text{c}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\text{PR}^2
\end{array}
\end{array}
\end{array}

Figure 12: Surface Representation for $\mathbb{P}\mathbb{R}^2$

diametrically opposite points on the boundary are clearly identified, this can be easily seen to be homeomorphic to the hemisphere model of $\mathbb{P}\mathbb{R}^2$ by mapping the open square to the open hemisphere and the edges to the boundary of the hemisphere with antipodal points identified.

3.3 Projective Line

So far we’ve completely skipped over the discussion of projective lines, which are interesting in their own right. $\mathbb{P}\mathbb{R}^1$ can be thought of as a copy of $\mathbb{R}$ plus a single point at infinity. Figure 13, the analogue to figure 1 shows that there is indeed only one point at infinity and it’s represented by the line $z = 0$ through the origin in $\mathbb{R}^2$.

Analogous to the sphere model for $\mathbb{P}\mathbb{R}^2$, the real projective line is homeomorphic to a circle with opposite points identified. But this circle with identifications is the same as a semicircle with endpoints identified, which is then homeomorphic to a circle with no identifications made. One can see directly why the real projective line is equivalent to a circle by looking at the stereographic projection (figure 14) which defines a bijection between, say, the circle $x^2 + (z - 1)^2 = 1$ without the pole $(0, 2)$ and the real line $z = 0$. This becomes a bijection between the circle and $\mathbb{P}\mathbb{R}^1$ if we map $(0, 2)$ to the point at infinity.

The complex projective line $\mathbb{P}\mathbb{C}^1$ is even more interesting. It is called the...
Riemann sphere since it is homeomorphic to the 2-sphere. Consider the sphere \( x^2 + y^2 + (z - 1)^2 = 1 \). A bijection \( B(z) \) can be defined between \( \mathbb{C} \) and the sphere minus the north pole \((0, 0, 2)\) by the stereographic projection

\[
\begin{align*}
x &= \frac{4v}{|z|^2 + 4} \\
y &= \frac{4v}{|z|^2 + 4} \\
z &= \frac{2u}{|z|^2 + 4}
\end{align*}
\]

where \( z = u + iv \). This becomes a bijection between the 2-sphere and \( \mathbb{P}^1 \) by taking the point at infinity to the north pole. To prove they are homeomorphic, it can be shown that the one point compactification of \( \mathbb{R}^2 \), \( \mathbb{R}^2 \cup \{\infty\} \), is homeomorphic both to the 2-sphere and to \( \mathbb{P}^1 \) thus making \( \mathbb{P}^1 \) homeomorphic to \( S^2 \).

### 3.4 Two Classical Results

Two classical results about projective spaces that must be mentioned under penalty of law are Desargues Theorem and the invariance of the cross ratio.

**Theorem 3.1. (Desargues)**

If two triangles \( \triangle ABC \) and \( \triangle A'B'C' \) have the property that \( \overline{AA'} \), \( \overline{BB'} \) and \( \overline{CC'} \) intersect at a point \( O \), then the points \( P = \overline{AB} \cap \overline{A'B'} \), \( Q = \overline{AC} \cap \overline{A'C'} \) and \( R = \overline{BC} \cap \overline{B'C'} \) lie on the same line \([3]\).

The proof of Desargues' Theorem will be presented for the three dimensional case although it is also true in the Euclidean plane.

**Proof.** [13] Triangles \( \triangle ABC \) and \( \triangle A'B'C' \) having the property that \( \overline{AA'} \), \( \overline{BB'} \) and \( \overline{CC'} \) intersect at a point \( O \), are in perspective where one triangle is the image of the central projection of the other where \( O \) is the origin. This situation is depicted in figure 15. Call the plane \( \triangle ABC \) is on the image plane \( I \) and call the plane defined by \( \triangle A'B'C' \) \( I' \). Suppose \( I \) and \( I' \) are not the same plane. \( I = \)
Figure 14: Stereographic Projection in 2 dimensions

$I'$ corresponds to the more difficult 2-dimensional version of the theorem.) The two planes $I$ and $I'$ intersect on a line $l$, and this will turn out to be the line that $P$, $Q$ and $R$ lie on. Consider $P = \overline{AB} \cap \overline{A'B'}$. $\overline{BB'}$ and $\overline{AA'}$ are two different lines through the origin that therefore define a plane. $\overline{AB}$ and $\overline{A'B'}$ lie on this plane and therefore must intersect in the projective plane, which is the plane defined above plus points at infinity. Since these lines are also contained in $I$ and $I'$, the intersection $P$ must also be on $l$. The analogous argument implies $Q$ and $R$ are also on $l$.

The statement of the theorem in the Euclidean plane can be summed up by figure 16. A proof of the two dimensional case can be found in [3].

One interesting geometrical application is that Desargues' theorem can be used to construct lines that intersect at distant points. For example, if a company laying down straight train tracks encounters a large hill but wants to continue the tracks on the other side of the hill before waiting for a tunnel to be completed, Desargues' theorem could theoretically be a way to find points on the other side of the hill that lie on the line determined by the existing tracks. Possible constructions of the necessary triangles are presented in [3] and [13].

One neat aspect of Desargues' Theorem is that its dual statement is its converse. However, the really unusual feature is that it's only a theorem in three dimensions or higher. It is sometimes true and sometimes false in projective planes. Fortunately, it holds for $P\mathbb{R}^2$. An example where it fails is the projective plane $P\mathbb{O}^2$ defined over the octonians [6]. Baez notes a fascinating connection between Desargues' theorem and the usual method of constructing projective spaces over a field $K$ by taking sets of lines through the origin. This construction
also works when $K$ is a skew field, which is a ring in which every nonzero element has a left and right inverse, and projective planes defined over skew fields are exactly the ones that satisfy Desargues' theorem.

The cross ratio is the simplest and most important projective invariant.

**Definition 3.3. (Cross Ratio on a Euclidean Line)**

If $A, B, C, D$ are four numbers on a Euclidean line, then their cross ratio $[A, B, C, D]$ is defined to be

$$[A, B, C, D] = \frac{AC}{AD} \cdot \frac{BD}{BC}.$$

**Theorem 3.2.** If $A', B', C', D'$ is the projection of $A, B, C, D$ onto another line as in figure 17, then $[A, B, C, D] = [A', B', C', D']$.

**Proof.** [3] The cross ratio can be written entirely in terms of angles at the origin which don’t change under projection from the origin. Specifically,

$$[A, B, C, D] = \frac{\sin \angle AOC \sin \angle BOD}{\sin \angle AOD \sin \angle BOC}.$$

The cross ratio provides another method for tackling the case of Kermit’s kidnapper and determining real world measurements based on image plane measurements. Referring back to figure 7, take the ground as the reference plane.
and the vertical line on which the person is standing as the reference line, which in this case is perpendicular to the plane. Let \( vv \) be the vanishing point of the vertical line, which doesn’t appear in the image because it is a point at infinity, but it can be thought of as lying far below \( b \). The points \( b \) and \( t \) are already defined. Take \( i \) to be the intersection in the image with the vertical line and the vanishing line of the plane, ie: the horizon. These four points define a cross ratio \([i, t, b, vv] = \frac{(b-i)(vv-t)}{(vv-i)(b-t)}\). [5] But since \( vv \) is a point at infinity, this ratio can be rewritten as \( \frac{k-i}{k-t} \). By taking measurements on the image, we find this cross ratio to equal 2.5. Now consider the corresponding points on the vertical reference line of the person in the real world. The difference \( t - b \) is the height of the person, which we’d like to know. On the other hand, \( i - b \) is the height of the origin, namely the distance the onlooker’s eye is from the ground plane. Since in this picture, the front of the house is parallel to the image plane, we immediately see that the observer’s eye is at a height of \( 2h \), exactly twice as high as the roof of the house. Now \( (t - b) = \frac{2}{5}(i - b) = \frac{2}{5}2h = \frac{4h}{5} \), which is exactly
the height already calculated.

In general it is also possible to define the cross ratio of four points on an abstract projective line defined by two points in a projective space of arbitrary dimension.

**Definition 3.4.** Let $A, B$ be two points in $\mathbb{P} \mathbb{K}^n$. This defines a line through $A$ and $B$ defined by $\lambda A + \mu B$ where at least one of $\lambda, \mu$ is non-zero. Let $A_i$ where $i = 1, 2, 3, 4$ be 4 points on the line. In terms of the parameterization, $A_4$ can be thought of as the point $[\lambda, \mu]$ on a projective line. Thus the cross ratio is

$$[A_1, A_2, A_3, A_4] = \frac{\lambda_1 - \lambda_4}{\mu_4} - \frac{\lambda_2 - \lambda_3}{\mu_3} = \frac{\lambda_1 - \lambda_4}{\mu_4} - \frac{\lambda_2 - \lambda_3}{\mu_3}.$$ 

This cross ratio is invariant under all projective transformations, and a proof of this will be sketched in section 4.7.
4 Algebraic Curve Preliminaries

4.1 Lines and Curves

Lines are the easiest example of curves in the projective plane \( \mathbb{P} \mathbb{K}^2 \). As mentioned before, projective lines are defined by planes through the origin in \( \mathbb{K}^3 \), necessarily equations of the form \( ax + by + cz = 0 \). Since two points in \( \mathbb{P} \mathbb{K}^2 \) define vectors that span a plane in \( \mathbb{K}^3 \), there is an easy algebraic way to find the equation for that plane and hence the unique projective line through two points. Let the two points be \((x_1, y_1, z_1)\) and \((x_2, y_2, z_2)\). Any other point on the same line must be a linear combination of those two representative points, so the equation is given by the following determinant

\[
\det \begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x & y & z \end{bmatrix} = 0
\]

There is also a simple algebraic method for finding the unique intersection point of two distinct lines \( a_1 x + b_1 y + c_1 z = 0 \) and \( a_2 x + b_2 y + c_2 z = 0 \) in \( \mathbb{P} \mathbb{K}^2 \). (This is the line of intersection of two planes in \( \mathbb{K}^3 \).) By dividing through by one of the variables and using Cramer’s rule the intersection of the two lines is \((X : Y : Z)\) where

\[
X = \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix}, \quad Y = \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}, \quad Z = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}
\]

All lines can be also rationally parameterized as was done in the general definition of the cross ratio, a fact that will come up again in the definition of intersection numbers.

**Definition 4.1.** A projective variety in \( \mathbb{P} \mathbb{K}^2 \) is the set of points \((X : Y : Z)\) in \( \mathbb{P} \mathbb{K}^2 \) satisfying \( P(X, Y, Z) = 0 \), where \( P \) is a homogeneous polynomial in \( \mathbb{K}^3 \). \( P \) is also known as a form.

An affine variety for comparison is the zero set of a polynomial that isn’t necessarily homogeneous. The projective variety is possibly larger since it includes points at infinity.

**Definition 4.2.** A projective algebraic curve of degree \( d \) in \( \mathbb{P} \mathbb{K}^2 \) is a non-zero homogeneous polynomial \( F(x, y, z) \) of degree \( d \) in \( \mathbb{K}^3 \).

Any non-zero multiple of \( F \) in the above equation is equivalent. The set associated to the curve \( F \) is the projective variety defined by \( F(x, y, z) = 0 \).

This is a useful definition because it only makes sense to say points in the projective plane satisfy a polynomial equation if the equation is homogeneous. Since \( P(\lambda X, \lambda Y, \lambda Z) = \lambda^n P(X, Y, Z) \), both polynomials define the same zero set regardless of \( \lambda \).

We’ve already seen that projective lines are homogeneous polynomials of degree one. Similarly, projective conics and cubics are forms of degrees two and three respectively.
Definition 4.3. If \( p(x, y) \) is a polynomial of degree \( n \), then the corresponding homogeneous polynomial is \( P[X : Y : Z] = Z^n p\left(\frac{X}{Z}, \frac{Y}{Z}\right) \).

The homogeneous polynomial of degree \( n \) of course has the property that \( P(\lambda X, \lambda Y, \lambda Z) = \lambda^n P(X, Y, Z) \). For example, the homogenization of the general affine conic \( f(x, y) = ax^2 + by^2 + cxy + dx + ey + f \) is \( F(x, y, z) = az^2 + by^2 + cxy + dxz + eyz + fz^2 \). Dephomenizing is the process of going from a projective curve \( F \) to an affine view. The three principal affine views are obtained by taking \( x = 1 \), \( y = 1 \) or \( z = 1 \), but any plane will work. Affine views don’t have to be affine equivalent. For example, different affine views of a projective conic can yield all the different conic sections.

4.2 Points at Infinity

In the affine view \( z = 1 \), the points at infinity on a curve are the points where the curve meets the line at infinity defined by \( z = 0 \). For example, the parabola \( yz - x^2 = 0 \) in \( \mathbb{P}^2 \) has only one point at infinity, namely \( (0 : 1 : 0) \). In \( \mathbb{P}^2 \) in general, a parabola only has one point at infinity. As a more interesting example consider the conic \( F(x, y, z) = (x - az)^2 + (y - bz)^2 - rz^2 \). In \( \mathbb{P}^2 \) there are no points at infinity because there are no non-zero solutions to \( x^2 + y^2 = 0 \). In \( \mathbb{P}^2 \), however, there are exactly two points at infinity, namely \( (1 : 1 : 0) \) and \( (1 : -1 : 0) \).

4.3 Intersections

The intersection number at a point where a line intersects a curve in \( \mathbb{P}^2 \) gives a way to count the multiplicity of the intersection. Let a line in \( \mathbb{P}^2 \) be parameterized by \( x_1(s, t) = sa_1 + tb_1, x_2(s, t) = sa_2 + tb_2, x_3(s, t) = sa_3 + tb_3 \) where points \( A = (a_1 : a_2 : a_3) \) and \( B = (b_1 : b_2 : b_3) \) determine the line.

Definition 4.4. [2] For a curve \( F \) of degree \( d \) and a line \( L \), the intersection form is defined by

\[
\Phi(s, t) = F(sa_1 + tb_1, sa_2 + tb_2, sa_3 + tb_3).
\]

\( \Phi \) is homogeneous of degree \( d \) and zero whenever \( F \) and \( L \) intersect, (possibly at infinitely many points if \( L \) is a component of \( F \)).

Definition 4.5. [2] The intersection number \( I(P, F, L) \) in \( \mathbb{P}^2 \) of a line \( L \) with a curve \( F \) at a point \( P \) corresponding to the ratio \( (s_0 : t_0) \) is defined to be the multiplicity of \( (s_0 : t_0) \) as a root of \( \Phi(s, t) = 0 \).

For example, if \( \Phi \) has a factor \( (t_0s - s_0t)^m \), then \( I(P, F, L) = m \). It can be shown that \( I(P, F, L) \) is independent of parameterization of \( L \). Moreover, the intersection number doesn’t change if we dehomogenize with respect to one variable and look at the resulting curve and line in an affine plane. The definition of the intersection number changes only slightly.
**Definition 4.6.** [2] In an affine view, the intersection number \( I(p, f, l) \) of a line \( l \) with a curve \( f \) at a point \( p \), is defined in terms of the intersection polynomial \( \phi(t) = f(x(t), y(t)) \), where \( (x(t), y(t)) \) parameterizes the line. Let \( p = (x(t_0), y(t_0)) \). Then \( I(p, f, l) \) is defined to be the multiplicity of \( t_0 \) as a root of the polynomial equation \( \phi(t) = 0 \).

This can be as simple as in figure 18 which shows \( y = 0 \) and \( y - (x-1)^2 = 0 \) intersecting with multiplicity 2 at \((1,0)\) because \( x = 1 \) is a double root of the parabola.

![Graph](#)

**Figure 18:** \( I(p, f, l) = 2 \)

A fundamental but technical result that can be found in [2] is that the intersection number is invariant under projective changes of coordinates.

### 4.4 Multiplicities and Singular Points

**Definition 4.7.** The multiplicity of a point \( P \) on a curve \( F \) in \( PC^2 \) is the minimum value \( m \) of the intersection number \( I(P, F, L) \) for all lines \( L \) through \( P \).

Points with multiplicity one, two, three and so on are respectively called simple, double and triple points. For example a double point, ie: a point where \( I(P, F, L) = 2 \), might look like the point in figure 19 where a curve crosses itself. \( I \) doesn’t have to equal 2 for all lines \( L \). For example, if \( L \) is one of the possible tangents at that point, then \( I \) will be greater than 2 for those lines.

**Definition 4.8.** A point \( P \) on a curve \( F \) is singular if it has multiplicity greater than or equal to 2.

**Definition 4.9.** A non-singular curve is a curve with no singular points.

**Lemma 4.1.** A point \( P \) is a singular point on \( F \) iff \( F(P) = 0 \) and \( F_x(P) = F_y(P) = F_z(P) = 0 \).

The proof is a good example of how to use the intersection form.
Proof. [2] Suppose \( F \) has degree \( m \) and let \( Q \) be any point on an arbitrary line through \( P \). The intersection form \( \Phi(s,t) \) is homogeneous of degree \( m \) and therefore looks like
\[
\Phi(s, t) = s^m F_0 + s^{m-1} t F_1 + \ldots + t^m F_m
\]
where the \( F_i \) are polynomials in the entries of \( P \) and \( Q \). \( P \) is represented by \( (s : t) = (1 : 0) \). For \( I(P,F,L) \geq 2 \), \( (1 : 0) \) must be a root of at least multiplicity 2 for \( \Phi(s,t) = 0 \). This implies \( (0s - t)^2 \), i.e. \( t^2 \), is a factor of \( \Phi \), which means \( F_0 = F_1 = 0 \). \( F_0 = 0 \) follows from \( P \) being on \( F \). Gibson uses the following trick to interpret \( F_1 \). Let \( \phi(t) = F(P + tQ) = tF_1 + \ldots + t^m F_m \). Differentiating with respect to \( t \) and setting \( t = 0 \) implies
\[
\phi'(0) = F_1 = q_1 F_x(P) + q_2 F_y(P) + q_3 F_z(P)
\]
where \( Q = (q_1 : q_2 : q_3) \). Since this is true for all \( Q \), \( \Phi = 0 \) if and only if the partials of \( F \) are zero.

Euler's Lemma gives a handy way to find singular points on a projective curve.

**Lemma 4.2.** If \( F \) is a homogeneous polynomial of degree \( m \) then
\[
mF = \sum_k x_k F_{x_k}
\]
The proof is just a quick application of the chain rule. Let \( F \) be a curve in \( \mathbb{P}^2 \) for concreteness. Since \( F \) is homogeneous of degree \( m \), then
\[
F(tx, ty, tz) = t^m F(x, y, z).
\]
Differentiating with respect to \( t \) gives
\[
x F_x + y F_y + z F_z = m t^{m-1} F(x, y, z).
\]
Setting \( t = 1 \) then gives the result. This is useful here because it implies that if the partials of \( F \) vanish at \( P \), then so does \( F \). Thus solving \( 0 = F_x = F_y = F_z \) yields the singular points of \( F \).
4.5 Tangents

**Lemma 4.3.** If \( P \) is a simple point on a curve \( F \) of degree \( m \) in \( \mathbb{P}^2 \), then the unique tangent to \( F \) at \( P \) is given by

\[
x F_x(P) = y F_y(P) + z F_z(P) = 0.
\]

The proof [2] is another neat application of Euler’s lemma.

**Proof.** WLOG assume \( P = (a : b : 1) \) so that it is safe to dehomogenize with respect to \( z \) to get an affine curve \( f(x, y) \). The tangent to \( f \) at \((a, b)\) is defined by

\[
(x - a)f_x(p) + (y - b)f_y(p) = 0
\]

Homogenizing this implies the projective tangent is given by

\[
(x - az)F_x(P) + (y - bz)F_y(P) = 0
\]

Euler’s lemma implies

\[
a F_x(P) + b F_y(P) + F_z(P) = 0
\]

which when substituted in the above equation gives the desired formula for a projective tangent. \(\square\)

One interesting result is a simple formula for finding tangents to projective conics at simple points. If \( P = (p_1 : p_2 : p_3) \) is a simple point on a conic \( V \), then the tangent to \( V \) at \( P \) is just

\[
p_1 V_x + p_2 V_y + p_3 V_z = 0.
\]

To see this, write the conic in its general form

\[
V = ax^2 + by^2 + cxy + d z^2 + eyz + f z^2.
\]

The tangent formula implies that

\[
x(2ap_1 + cp_2 + dp_3) + y(2bp_2 + cp_1 + cp_3) + z(dp_1 + cp_2 + 2fp_3) = 0.
\]

Regrouping terms shows that

\[
p_1(2ax + cy + dz) + p_2(2by + cx + ez) + p_3(2fz + ey + dz) = 0,
\]

which is exactly the desired formula.

It’s also possible to find tangents at singular points, although tangents at such points are no longer unique as figure 19 indicates. The strategy for finding such tangents is to dehomogenize the curve \( F \) and set the lower order terms equal to zero.

26
4.6 Flexes

Definition 4.10. A simple point $P$ on a curve $F$ is a flex, or point of inflection, if the tangent $T$ at $P$ intersects $F$ with multiplicity greater than or equal to 3, i.e: $I(P, T, F) \geq 3$.

Flexes will be important to the definition of the group structure on a cubic because flexes are chosen to be the base points $O$ in the definition of addition of two points on a cubic, as was briefly discussed earlier.

Lemma 4.4. If $P$ is a simple point on $F$, a homogeneous polynomial of degree 2 or more, then $P$ is a flex iff it satisfies the Hessian equation

$$H(X, Y, Z) = \det \begin{bmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{bmatrix} = 0$$

The proof can be found in [2] or [7].

4.7 Projective Transformations and Equivalence

Since an invertible linear transformation $\Phi$ in $\mathbb{K}^3$ maps lines through the origin to other lines through the origin, it defines a bijective projective mapping $\Phi$ of $\mathbb{P}\mathbb{K}^2$.

Definition 4.11. A projective mapping $\Phi$ in $\mathbb{P}\mathbb{K}^2$ is defined by

$$\tilde{\Phi}(x : y : z) = (X : Y : Z)$$

where

$$\Phi \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}$$

If $\Phi'$ is a scalar multiple of $\Phi$, then they define the same projective transformation. A projective map is an invertible linear transformation in $\mathbb{K}^3$ up to non-zero scalar multiplication. In fact, it can be shown that projective transformations form a group called the projective linear group $PGL(2)$, which is a quotient of the general linear group $GL(3)$ of invertible linear maps of $\mathbb{K}^3$ by the subgroup of non-zero scalar multiples of the identity.

Equivalent projective maps actually must come from invertible linear maps that differ by at most a scalar multiple. A related lemma to this effect is the four point lemma.

Lemma 4.5. Let $E_1 = (1 : 0 : 0), E_2 = (0 : 1 : 0), E_3 = (0 : 0 : 1), U = (1 : 1 : 1)$. Then if $P_1, P_2, P_3, P_4$ are four points in $\mathbb{P}\mathbb{K}^2$ in general position, which means any three of them are linearly independent, then there exists a unique projective map $\tilde{\Phi}$ taking $P_1, P_2, P_3, P_4$ to $E_1, E_2, E_3, U$ in that order.
As an example of how this can be done, choose the four points to be \( P_1 = (3 : -2 : 1) \), \( P_2 = (-4 : 2 : -1) \), \( P_3 = (2 : -1 : 1) \) and \( P_4 = (3 : 0 : 1) \). Let \( \Phi_0 \) be the inverse of
\[
\begin{bmatrix}
3 & -4 & 2 \\
-2 & 2 & -1 \\
1 & -1 & 1
\end{bmatrix}
\]
which equals
\[
\begin{bmatrix}
-1 & -2 & 0 \\
-1 & -1 & 1 \\
0 & 1 & 2
\end{bmatrix}
\]
Note that
\[
\Phi_0 P_4 = \begin{bmatrix}
-3 \\
-2 \\
2
\end{bmatrix}
\]
but we want that to be \( U \), which suggests that \( \Phi \) should be a scaled version of \( \Phi_0 \) defined by
\[
\Phi = \begin{bmatrix}
-\frac{1}{3} & 0 & 0 \\
0 & -\frac{1}{2} & 0 \\
0 & 0 & \frac{1}{2}
\end{bmatrix} \Phi_0
\]
A related result is the four line lemma that says there is a unique projective transformation taking four lines in general position to four other lines in general position, where general position in this sense just means no three lines are concurrent. The proof follows from the four point lemma and the dual nature of the projective plane. A point in \( PK^2 \) is a line through the origin in \( K^3 \), which defines a unique plane through the origin in \( K^3 \) which is a line in \( PK^2 \). It remains only to be shown that four lines in general position correspond in this manner to four points in general position.

Returning to the discussion of projective equivalence, we can define what it means for two curves to be equivalent.

**Definition 4.12.** Two curves \( F \) and \( G \) are projectively equivalent if \( G(x, y, z) = \lambda F(X, Y, Z) \) where once again
\[
\begin{bmatrix}
X \\
Y \\
Z
\end{bmatrix} = \Phi \begin{bmatrix}
x \\
y \\
z
\end{bmatrix},
\]
and \( \Phi \) is an invertible linear transformation.

This idea of projective equivalence can be used to classify curves up to projective equivalence. This is briefly mentioned in the next section for projective lines, conics and cubics.

Projective maps can also be seen to be equivalent to affine transformations. An affine map is just translation composed with an invertible linear map in an affine plane such as \( z = 1 \).
Lemma 4.6. [2] An affine map $\phi$ in $\mathbb{R}^2$ extends to a projective map $\Phi$ in $P\mathbb{R}^2$ mapping $z = 0$ to itself. Conversely, a projective map $\Phi$ mapping $z = 0$ to itself is an affine map when restricted to $\mathbb{R}^2$.

Proof. Given an affine map $\phi$, since $\phi$ is degree 1 a projective map $\Phi$ can be defined to be

$$\Phi(x, y, z) = z\phi\left(\frac{x}{z}, \frac{y}{z}\right).$$

Conversely, if $\Phi$ maps $z = 0$ to itself, then since $\Phi$ is also invertible $\Phi(x, y, z) = (X, Y, Z)$ has the property that $Z = kZ$ for $k \neq 0$. Thus the restriction to the affine plane is achieved by dehomogenizing with respect to $z$. \qed

This correspondence is what manifested itself in the discussion of projection transformations in $P\mathbb{R}^3$ in computer graphics as an equivalent way of expressing affine transformations in $\mathbb{R}^3$.

This concept of projective equivalence also helps prove the invariance of the cross ratio as defined in Definition 3.4. A sketch of the proof follows. We already have the general ratio defined in terms of points $(s : t)$ on a projective line. An invertible linear transformation in the larger space descends to an invertible linear transformation on the projective line. For the cross ratio to be invariant, it only needs to be shown that if

$$\begin{bmatrix} s' \\ t' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix}$$

then the cross ratio is the same in $(s' : t')$ coordinates as it is in $(s : t)$ coordinates. If we dehomogenize with respect to $t$ and let $u = \frac{s}{t}$, we see that the map is really a linear fractional transformation on the affine line.

$$\begin{bmatrix} u \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} au + b \\ c + d \end{bmatrix}$$

So the problem again reduces to showing the cross ratio is invariant under linear fractional transformations of the line. Since three points uniquely determine a linear fractional transformation [21], let $L(u) = w$ be the unique linear fractional transformation that takes $u_1$, $u_2$ and $u_3$ to $w_1$, $w_2$ and $w_3$ respectively. Define $A(u) = \frac{w - u_1}{w - u_3}$. Define $B(w) = \frac{w - u_3}{w - u_1}$ where $w = L(u)$. Now $A(u) = B(L(u))$ at three points. Specifically, $u_1$, $u_2$ and $u_3$ map to 0, 1 and infinity respectively. Thus $A(u) = B(L(u))$. Substituting $u$ with $u_4$ now implies the invariance of the cross ratio, namely

$$\frac{w_4 - w_1}{w_4 - w_3} = \frac{u_4 - u_1}{u_4 - u_3}$$

One final transformation of interest is that is it possible to define a projection from one projective space onto another of lower dimension. In fact, it is sometimes useful to think of central projection as a 3 by 4 matrix that projects $P\mathbb{R}^3$ to $P\mathbb{R}^2$. This is done in [5] to produce a general algebraic method for
making measurements of distances and ratios in a 3D scene from a 2D image. Criminisi uses such a projection matrix to define general methods for determining camera position, relating measurements on parallel planes and for measuring distances between planes. This gives a third way to tackle the Kermit kidnapper problem and determine the height of the abscending criminal seen in Figure 7. Referring back to this figure, we know from previous arguments that the world origin is perpendicular to the image plane at the vanishing point \( v_y \), so we take that to be the origin for our measurements on the image plane. Define affine coordinates \((X, Y, Z)\) as indicated in figure 7 with the affine origin as yet undetermined. The projection matrix \( P \) can then be defined in terms of where the lines \((1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0)\) and \((0 : 0 : 0 : 1)\) project to. This defines the first three columns of \( P \) as the vanishing points of the \(X\), \(Y\) and \(Z\) directions in affine coordinates. Since these are only determined up to scalar factors \( \alpha, \beta \) and \( \gamma \) as columns in \( P \), there is lots of freedom in placing the affine origin and hence determining the fourth columns of \( P \). The only placement that would be bad would be if the line connecting the two origins in world coordinates were parallel to the reference plane, which is the ground in this case. In this case we’d lose information about depth in the picture. This only happens if the fourth column is a linear combination of the first two, both of which lie on the vanishing line of the reference plane in \( \mathbb{RP}^2 \). Since there is so much freedom in choosing the fourth column, the easy solution is to define it by normalizing the coordinates of the vanishing line. Thus if the vanishing line is \( ax + by + cz = 0 \), then the fourth column is \( \frac{1}{\sqrt{a^2 + b^2 + c^2}} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \). For the situation in figure 7, the projection matrix is defined as

\[
\begin{bmatrix}
\alpha & 0 & 0 & 0 \\
0 & 0 & \gamma & 1 \\
0 & \beta & 0 & 0
\end{bmatrix}
\]

To find the persons unknown height, we first need to determine \( \gamma \) from the known height of the house. The bottom right corner of the house is

\[
B = \begin{bmatrix} 15 \\ -8 \\ 1 \end{bmatrix} = \rho \begin{bmatrix} X \\ Y \\ 0 \end{bmatrix}
\]

Similarly, the top right corner of the house is

\[
T = \begin{bmatrix} 15 \\ -4 \\ 1 \end{bmatrix} = \mu \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}
\]
where $\rho$ and $\mu$ are unknown scale factors. This gives two equations:

\[
\begin{bmatrix}
15 \\
-8 \\
1 \\
\end{bmatrix}
= \rho
\begin{bmatrix}
\alpha X \\
1 \\
\beta Y \\
\end{bmatrix}
\]

and

\[
\begin{bmatrix}
15 \\
-4 \\
1 \\
\end{bmatrix}
= \mu
\begin{bmatrix}
\alpha X \\
\gamma Z + 1 \\
\beta Y \\
\end{bmatrix}
\]

There is enough information to solve for $\gamma Z$. The equations for $X$ and $Y$ are actually irrelevant for our purposes. Plugging in $Z = h$ implies $\gamma = \frac{1}{2h}$.

Now that $\gamma$ is determined, this process is repeated with the points $b = (18, -5, 1)$ and $t = (18, -3, 1)$ representing the bottom and top of the person in image coordinates.

The resulting equation for $\gamma Z$ is $\frac{-3}{5} = \gamma Z$. But since $\gamma = \frac{1}{2h}$, we can solve for $Z$, which is in this case the height of the person. $Z = \frac{4h}{5}$ as in the previous two calculations regarding this example. With the height of the kidnapper thus confirmed, Miss. Piggy can surely be removed from the list of suspects.

5 Classification by Projective Equivalence

5.1 Lines

**Theorem 5.1.** All lines are equivalent in the projective plane.

**Proof.** [2] Let an arbitrary line $L$ be defined by $ax + by + cz = 0$. Define a projective change of coordinates by

\[
\begin{bmatrix}
a \\
b \\
c \\
0 \\
1 \\
0 \\
0 \\
1 \\
\end{bmatrix}
\begin{bmatrix}
x \\
y \\
z \\
\end{bmatrix}
= \begin{bmatrix}
X \\
Y \\
Z \\
\end{bmatrix}
\]

The matrix is clearly invertible and the line in new coordinates is given by $X = 0$. Thus all lines are projectively equivalent to the line $X = 0$ and therefore to each other. \qed

5.2 Conics

There are only three projectively equivalent types of projective conic. They are conics of the form $x^2 + y^2 + z^2$, $x^2 + y^2 + z^2$. All irreducible conics are projectively equivalent.

5.3 Cubics

Gibson defines nine types of cubics, but only eight represent classes of projectively equivalent cubics. Six of these are reducible cubics. There are then three types of irreducible cubics:
1. General cubics of the form $y^2z = 4x^3 - \alpha xz^2 - \beta z^3$

2. Nodal cubics of the form $x^3 + y^3 - xyz$

3. Cuspidal cubics of the form $y^2z - x^3$

Figure 20 shows affine views of these cubics.

![Elliptic Curve (General Cubic), Cuspidal Cubic, Nodal Cubic]

Figure 20: Possible affine views of irreducible cubics

Only the nodal and cuspidal cubics are classes of projective equivalence. Each has one singular point. The general cubic is non-singular and hence an elliptic curve. It does not define a class of projective equivalence. It's just a category for all the leftover cubics, which are the most interesting ones anyway. A cuspidal cubic has only one flex, a nodal cubic has three and a general cubic has 9.

6 Bézout’s Theorem

6.1 Resultants and Main Idea

The geometric idea behind the proof of Bézout’s Theorem presented by Gibson [2] is to project the two curves $F$ and $G$ from a point $S$ onto a line $L$. The next step is to find a method for counting points on $L$ that correspond to the projections of points of intersection of $F$ and $G$. WLOG assume $S = (0 : 0 : 1)$ and $z = 0$. We can write the curves $F$ and $G$ as

$$F = F_0(x, y)z^m + \ldots + F_m(x, y)$$

$$G = G_0(x, y)z^n + \ldots + G_n(x, y)$$

where $F_i$ and $G_i$ are homogeneous polynomials of degree $i$ and $j$ respectively. $(x : y : 0)$, a point on $L$, is a projection of an intersection of $F$ and $G$ if and only if there is some $z$ such that $F(x, y, z) = G(x, y, z) = 0$. It’s possible to define what’s called a resultant $R(x, y)$, a homogeneous polynomial of degree $mn$ that is zero if and only if $F$ and $G$ have a common zero.
Definition 6.1. The resultant \( R(x, y) \) of \( F, G \) with respect to \( z \) is defined to be the determinant of the \((n + m)\) square resultant matrix below.

\[
\begin{bmatrix}
F_m & F_{m-1} & F_{m-2} & \cdots & F_0 & 0 & 0 & \cdots \\
0 & F_m & F_{m-1} & F_{m-2} & \cdots & F_0 & 0 & \cdots \\
0 & 0 & F_m & F_{m-1} & F_{m-2} & \cdots & F_0 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
G_n & G_{n-1} & G_{n-2} & \cdots & G_0 & 0 & 0 & \cdots \\
0 & G_n & G_{n-1} & G_{n-2} & \cdots & G_0 & 0 & \cdots \\
0 & 0 & G_n & G_{n-1} & G_{n-2} & \cdots & G_0 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots 
\end{bmatrix}
\]

It can be shown [2] that \( R(x, y) \) is identically zero if and only if \( F \) and \( G \) have a common non-constant factor.

It can also be shown [2] that \( R(x, y) \) as defined above is a homogeneous polynomial of degree \( mn \). The only exception is if \( F \) and \( G \) have a common component, in which case \( R(x, y) \) becomes identically zero.

6.2 Sketch of Proof

The full statement of Bézout's theorem is essentially the same as already stated.

Theorem 6.1. (Bézout's Theorem)

Let \( F, G \) be curves in \( \mathbb{P}^2 \) of degrees \( m \) and \( n \) with no common component. Then the sum of the intersection numbers \( I(P, F, G) \) at the points of intersection \( P \) is exactly \( mn \).

Proof. Given \( F \) and \( G \), choose a point \( S \) not on \( F \) or \( G \) and project the plane from \( S \) onto a line \( L \) that doesn't pass through \( S \). Since \( F \) and \( G \) have no common factor, \( R(x, y) \) is not identically zero, and any line through \( S \) contains only finitely many intersection points of \( F \) and \( G \). By the four point lemma, it's possible to choose \( S = (0 : 0 : 1) \) and define \( L \) to be the line \( z = 0 \). Write \( F \) and \( G \) as above. Then \( (x : y : 0) \) is the projection of an intersection if and only if \( R(x, y) = 0 \). To ensure that \( (x : y) \) does not correspond to multiple intersection points of \( F \) and \( G \), ensure \( S \) doesn't lie on any line defined by a pair of intersection points. This is possible because there are only finitely many intersections. This gives a one to one correspondence between ratios \( (x : y) \) that satisfy \( R(x, y) = 0 \) and intersections \( (x : y : z) \) of the two curves. Since \( C \) is an algebraically closed field, \( R(x, y) \) has exactly \( mn \) roots, counted with multiplicity, which is precisely the sum of the intersection numbers at the points of intersection. \( \square \)

One interesting application of Bézout's theorem is that it limits the number of points with high multiplicity on curves. For example, a curve of degree 4 can't have 2 points of multiplicity 2 and 3 respectively because a line through those two points would then intersect a quartic 5 times, which violates the theorem.
7 Group Structure on a Cubic

7.1 Definition of $\ast$ Operation

In the following discussion, consider $F$ to be an irreducible cubic and $P$ and $Q$ to be simple points on $F$. (Since elliptic curves are defined to be non-singular cubics they consist only of simple points by definition.) The $\ast$ operation is the first step to defining addition of a cubic.

**Definition 7.1.** If $P$ and $Q$ are distinct and $L$ through $P$ and $Q$ is not tangent to either point, then $P \ast Q$ is the third point on the intersection of $L$ and $F$. If $L$ is tangent to, say, $P$, then define $P \ast Q = P$. If $P$ and $Q$ coincide and $P$ is not a flex, then $P \ast Q$ is again the third point on the intersection of $L$ with $F$. Finally, if they coincide and $P$ is a flex define $P \ast Q = P$.

Note $P \ast Q$ is always a simple point. Otherwise, $L$ would intersect $F$ more than 4 times, which is impossible.

7.2 Definition and Properties of Addition

**Definition 7.2.** Choose a base point $O$ to be a flex. Then addition on the set of simple points of a cubic is defined by

$$P + Q = (P \ast Q) \ast O$$

**Theorem 7.1.** The set of simple points on a general cubic with addition defined as above constitutes an abelian group.

**Proof.** $O$ is the additive identity. Note that $O \ast O = O$ and $O + P = (O \ast P) \ast O = P$.

The additive inverse $-P$ of $P$ can be defined by $-P = P \ast O$. To verify this, note that

$$P + -P = (P \ast -P) \ast O = (P \ast (P \ast O)) \ast O = O \ast O = O.$$ 

Since $\ast$ is commutative, $+$ is also commutative.

It can also be shown that $+$ is associative, which is needed to complete the proof. See [2] for details. 

Figure 21 adapted from [17] gives a geometric interpretation of addition on the cubic $y^2 = x^3 - x^2$. One of the nine points of inflection is a point at infinity, specifically $(0 : 1 : 0)$. The base point $O$ is chosen to be this point.

The three types of cubics - cuspidal, nodal and elliptic - have very different group structures. The group structure on a cuspidal cubic is $\mathbb{C}^+$. The group structure on a nodal cubic is $\mathbb{C}$. The group structure on an elliptic curve is that of the quotient group $\mathbb{C}/\Lambda$ where $\Lambda$ is a lattice, namely the subgroup $m\omega_1 + n\omega_2$ where $\omega_1$ and $\omega_2$ are the generators of the lattice. This group is isomorphic to the torus $S^1 \times S^1$. Thinking of $S^1$ as the unit circle in the complex plane, the isomorphism is just given by $\phi(z) = (e^{2\pi i a}, e^{2\pi i b})$ where $z = a\omega_1 + b\omega_2$ for
Figure 21: Addition defined on the cubic \( y^2 = x(x^2 - 1) \)

\( a, b \in \mathbb{R} \). [17] The set of points defined by a projective cubic is also topologically equivalent to a torus. However, these tori are actually Riemann surfaces on which the holomorphic structure actually varies depending on the lattice.

8 Parameterizations of Conics and Cubics

All conics can be rationally parameterized [20]. As an example, a rational parameterization of the circle is given by

\[
x = \frac{1 - t^2}{1 + t^2}; y = \frac{2t}{1 + t^2}
\]

Projective conics are topologically a sphere.

On the other hand, elliptic curves cannot be rationally parameterized. Elliptic functions are the simplest functions that parameterize elliptic curves. A method will be sketched below that shows how to parameterize an elliptic curve in normal form \( y^2 = x^3 + \alpha x + \beta \) using the Weierstrass \( \wp \) function. Fortunately, all elliptic curves can be written in the normal form displayed above.

8.1 Elliptic Curves and Functions

Definition 8.1. Elliptic functions are doubly periodic functions. A meromorphic function \( f \) on \( \mathbb{C} \) is an elliptic function relative to some lattice \( \Lambda \) if \( f(z + l) = f(z) \) for all \( l \in \Lambda \).
Definition 8.2. The Weierstrass $\wp$ function is an elliptic function defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \omega \neq 0} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}\right)$$

$\wp'(z)$ satisfies the following differential equation

$$(\wp'(z))^2 = f(\wp(z))$$

where $f$ is a cubic in normal form. This is usually written as

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3.$$  

Theorem 8.1. There is a bijective analytic map from $\mathbb{C}/\Lambda$ to the elliptic curve $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ in $\mathbb{C}^2$. This map is defined by

$$z \mapsto (\wp(z) : \wp'(z) : 1) \text{ for } z \neq 0$$

$$0 \mapsto (0 : 1 : 0)$$

Since $(\wp'(z))^2$ is a cubic in $\wp(z)$, every point maps onto the elliptic curve $f$. It's interesting to note that this analytic bijection is a group isomorphism from $\mathbb{C}/\Lambda$ to the group already geometrically defined on an elliptic curve.

A trick for finding the cubic that corresponds to a lattice $\Lambda$ involves finding the zeros of $\wp'(z)$. Since $\wp$ is even, $\wp(z) = \wp(w_1 - z) = -\wp'(z)$. This implies $\wp'(\frac{w_1}{2}) = \wp'(\frac{w_2}{2}) = \wp'(\frac{w_1 + w_2}{2}) = 0$. Denote the three roots of $f(\wp(z))$, a cubic in $\wp$, as

$$e_1 = \wp(\frac{w_1}{2})$$
$$e_2 = \wp(\frac{w_2}{2})$$
$$e_3 = \wp(\frac{w_1 + w_2}{2})$$

Since $(\wp'(z))^2$ factors into $4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$, then the unknown coefficients of the cubic are determined by

$$g_3 = 4e_1 e_2 e_3$$
$$g_2 = -4(e_2 e_3 + e_3 e_1 + e_1 e_2)$$

In practice this is not easy to compute because it involves sums over lattice points. An example result is that the lattice of Gaussian integers corresponds to a cubic of the form where $g_3 = 0$. [17]

Determining the lattice that corresponds to a given cubic in normal form is an even more horrendous computation because it involves elliptic integrals. In [19], the solution to the differential equation $(\wp'(z))^2 = f(\wp(z))$ is given by the following elliptic integral:

$$z - z_0 = \int_{\wp(z_0)}^{\wp(z)} \frac{dw}{\sqrt{4w^3 - g_2w - g_3}}$$
The periods of the lattice can be recovered by integrating the above integral over a path that avoids zeros and poles. For example, since $\varphi(e^{\pi i / 2}) = e_1$ and $\varphi(z)$ has a pole at $w_1$, one generator of the lattice can be recovered as below.

$$w_1 - \frac{w_1}{2} = \frac{w_1}{2} = \int_{e_1}^{\infty} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}}$$

This relationship only scratches the surface of the study of elliptic functions and curves, which have numerous applications today in number theory and cryptography. As an example, they played a strong role in Wiles’ proof of Fermat’s last theorem.
References


