Spring 2018

Affine and Projective Planes

Abraham Pascoe
Missouri State University, Abraham2@live.missouristate.edu

AFFINE AND PROJECTIVE PLANES

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

Abraham Pascoe

May 2018

AFFINE AND PROJECTIVE PROJECTIVE PLANES

Mathematics

Missouri State University, May 2018

Master of Science

Abraham Pascoe

ABSTRACT

In this thesis, we investigate affine and projective geometries. An affine geometry is an incidence geometry where for every line and every point not incident to it, there is a unique line parallel to the given line. Affine geometry is a generalization of the Euclidean geometry studied in high school. A projective geometry is an incidence geometry where every pair of lines meet. We study basic properties of affine and projective planes and a number of methods of constructing them. We end by proving the Bruck-Ryser Theorem on the non-existence of projective planes of certain orders.

KEYWORDS: Affine Geometry, Projective Geometry, Latin Square, Ternary Ring, Perfect Difference Set, Bruck-Ryser Theorem

This abstract is approved as to form and content

Dr. Les Reid
Chairperson, Advisory Committee
Missouri State University

AFFINE AND PROJECTIVE PLANES

By

Abraham Pascoe

A Masters Thesis
Submitted to The Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Mathematics

May 2018

Approved:

Dr. Les Reid, Chairperson

Dr. Mark Rogers, Member

Dr. Cameron Wickham, Member

Dr. Julie J. Masterson, Graduate College Dean

ACKNOWLEDGEMENTS

I want to first thank the faculty, staff, and students of Missouri State University who have pushed me in my education and made my experiences here enjoyable. I want to thank Dr. Mark Rogers and Dr. Cameron Wickham for not only being mentors in a classroom setting but outside of class as well.

I would like to thank Dr. Les Reid for his patience and wisdom over the last year. It has been a wonderful experience to be able to work closely with him. He is always willing to put aside what he is doing to answer any questions and handle any concerns that I had in this process.

Lastly, I owe a great debt of gratitude to my wife, Elisabeth, for her continued support and encouragement during the course of my graduate studies. She is and always will be a constant in my life who keeps me grounded. I cannot thank her enough for the love, hope, and motivation that she provides every day.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

In order to study projective planes, one must first understand the reasoning behind studying the field and the history of it. In most high schools, students learn about what is called Euclidean geometry. Around 300 B.C., the Greek geometer Euclid formalized roughly everything known about geometry up to that point in his book *Euclid's Elements* [2]. The ideas in this book are still widely used today and have inspired other fields of geometry.

Around the nineteenth century, mathematicians started to pull ideas from *Euclid's Elements* and apply them to other areas of our world that do not necessarily fit in with distance and angles [2]. The idea of how to develop other ideas was to take an axiomatic approach. This is the case in most branches of mathematics in today's times, but this process was first applied to projective geometry [6]. Mathematicians such as Pappus of Alexandria, Girard Desargues, Johannes Kepler, Blaise Pascal, J. V. Poncelet, and Karl von Staudt made large strides in this field and developed many of the foundations and terminology [9]. Desargues and Pascal's work hinted at projective geometry, but Poncelet gave a systematic development in the early nineteenth century [1].

When beginning to study projective geometry, the questions were "How do we see things?" and "Do we ever see a thing exactly as it is?" [6]. Consider paintings or drawings of train tracks continuing into the distance of the picture. We know intuitively that the rails remain parallel and will never cross. However, in paintings or in real life, our perception is that they do meet at some point. James M. Smart states that "this concept includes the principle that parallel lines seem to converge as they recede from the viewer" [8]. Thus, the study of projective geometry came about by considering these parallel lines meeting an some infinite point. This is often referred to in art as one-point perspective. Desargues was the first to consider

these points and Poncelet coined the term "points at infinity" when referring to these points [1]. The term "line at infinity" refers to the collection of these points at infinity (the line containing all of these points). Now consider a chair. Depending on the angle at which we look at the chair, the object looks totally different. We could view it from the bottom, side, or top and we might see different objects. One can use these perspectives to create a projective plane consisting of points and lines.

The study of projective geometry is important because we can use this field to develop many different non-Euclidean geometries. These geometries are necessary for ideas in sciences and technology such as relativistic cosmology [2]. While this is the historical background behind the field, the primary purpose of this particular study is to generalize the Euclidean and projective geometries in a more abstract and axiomatic framework. We will then look at general properties of affine and projective planes as well as to determine the possible orders of finite projective planes. We will use other abstract models such as Latin Squares, Perfect Difference Sets, Ternary Rings, and Near-Fields in order to construct affine and projective planes.

x

INCIDENCE GEOMETRY

DEFINITION 1: An Incidence Geometry is a set of elements we will call points $\mathbb{P}$ and a set of elements we will call lines $\mathbb{L}$ where $\mathbb{P} \cap \mathbb{L} = \emptyset$ and an incidence set $\mathbb{I} \subseteq \mathbb{P} \times \mathbb{L}$. If $(p, L) \in \mathbb{I}$, where $p \in \mathbb{P}$ and $L \in \mathbb{L}$, then p is said to be incident to L. The geometry must also satisfy the following axioms:

A1. For every $p, q \in \mathbb{P}$ where $p \neq q$, there exists a unique $L \in \mathbb{L}$ such that $(p, L), (q, L) \in \mathbb{I}$. This line is denoted $\overleftrightarrow{pq}$.

A2. Given $L \in \mathbb{L}$, there exists a $p, q \in \mathbb{P}$ such that $(p, L), (q, L) \in \mathbb{I}$.

A3. There exists $p, q, r \in \mathbb{P}$ such that there does not exist an $L \in \mathbb{L}$ where (p, L), $(q, L), (r, L) \in \mathbb{I}$.

Informally, what all of this means is that for an incidence geometry, there are a set of points $\mathbb{P}$ and a set of lines $\mathbb{L}$ such that a point can never be a line. But there are incidence relations among the points and lines and each of the relations are contained in the set $\mathbb{I}$. Used throughout this paper are other common phrases instead of explicitly saying that a point is incident to a line. For example, a point lies on a line, a line passes through a point, two lines meet at a point, or a line contains a certain point.

Continuing to examine the definition, **A1** informally states that two distinct points determine a unique line. **A2** states that every line contains at least two points. **A3** states that there exists three non-collinear points.

Note that throughout this paper, we will use the terms "geometry" and "plane" interchangeably.

DEFINITION 2: For a given line L, the set of points incident to L will be denoted L_{pt}, i.e. $L_{pt} = \{p \mid (p, L) \in \mathbb{I}\}$.

We will need the following definition.

DEFINITION 3: Two distinct lines L and M are said to be parallel if there are no points incident to both, i.e. there does not exist a p such that $(p, L), (p, M) \in \mathbb{I}$. This is denoted $L \parallel M$.

As terminology used throughout this paper, if two lines L and M are parallel, we will say that they are in the same family and the set of all parallel lines to L including L will be called a family of parallel lines.

An incidence geometry is one of the most basic types of geometries and most geometries studied are incidence geometries. For example, Euclidean geometry, which is studied in most secondary education programs, is an incidence geometry. When considering other geometries, the following parallel properties are sometimes included in their definition:

P1. The Euclidean Property states that for every line L and every point p not incident to L, there exists a unique line M through p such that $L \parallel M$.

P2. The Elliptic Property states that for every line L and every point p not incident to L, there does not exist a line M through p such that $L \parallel M$, i.e. there are no parallel lines.

P3. The Hyperbolic Property states that for every line L and every point p not incident to L, there exists more than one line through p that is parallel to L.

The following figures are given as examples of the three parallel properties. Figure 1 shows a geometry satisfying **P1**. If you choose any line and a point not lying on that line, there is only one line through that point parallel to the line. The only set of parallel lines difficult to see is the diagonal lines which happen to be parallel.

Figure 2 shows a geometry satisfying **P2**. If you choose any line and a point not lying on that line, there are no lines through that point that is not incident to the

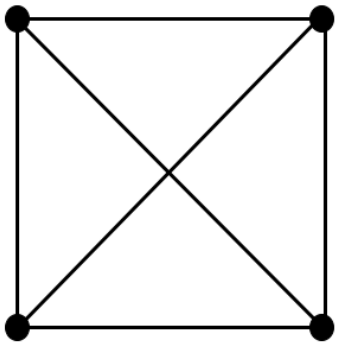

Figure 1: Geometry with the Euclidean Parallel Property

original line.

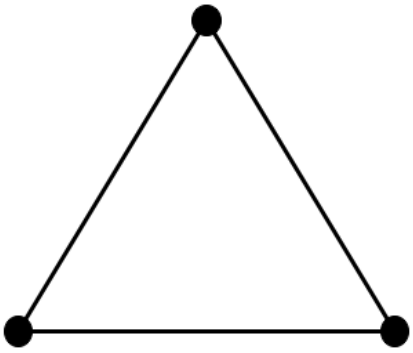

Figure 2: Geometry with the Elliptic Parallel Property

Figure 3 shows a geometry satisfying **P3**. For example, consider line $\overleftrightarrow{RS}$ and the point Q. The lines $\overleftrightarrow{QT}$ and $\overleftrightarrow{QP}$ are both parallel to $\overleftrightarrow{RS}$.

However, these three properties are mutually exclusive, i.e. every pair of point and line in a certain geometry must satisfy the same parallel property. For example, consider Figure 4. The point P has only one line through it parallel to the line L. Thus, this geometry cannot be elliptic nor hyperbolic. Likewise, the point P has two lines through it parallel to the line L'. Thus, this geometry cannot be euclidean nor elliptic. Therefore, this geometry does not have a parallel property.

Corollary 1: In an incidence geometry, if two distinct lines meet, they meet at a

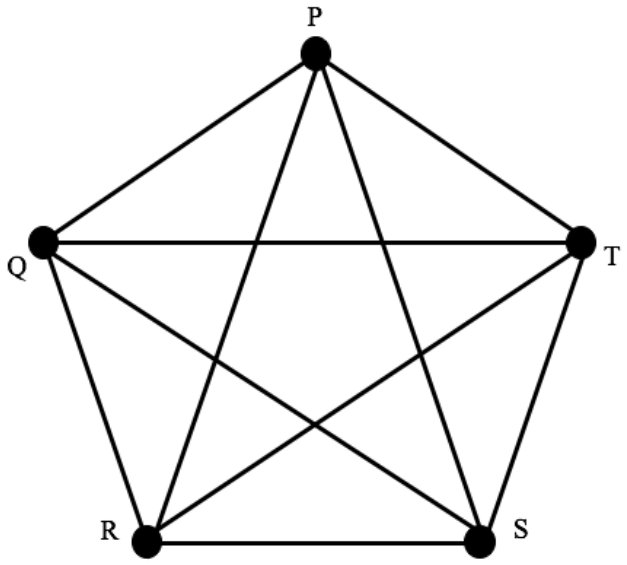

Figure 3: Geometry with the Hyperbolic Parallel Property

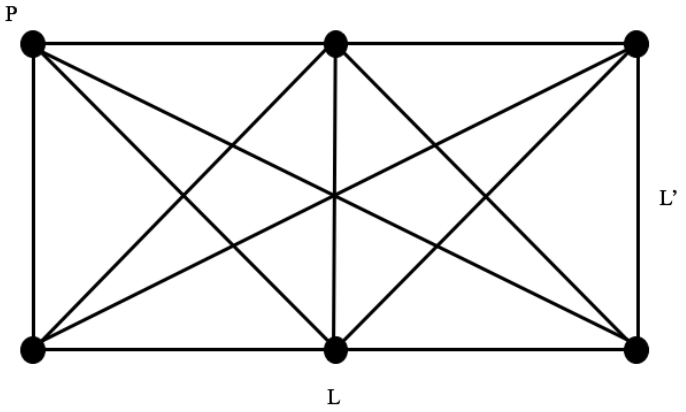

Figure 4: Geometry with no Parallel Property

unique point.

Proof. By contradiction, assume two distinct lines L and M do not meet at a unique point, i.e. they meet at points p and q ($p \neq q$). By **A1**, two distinct points determine a unique line and L and M both pass through p and q. Hence, $L = M$. Since this contradicts the assumption that L and M were different lines, then they cannot meet at more than one point. □

LEMMA 1: In an incidence geometry, given any point p, there exists a line L such that $(p, L) \notin \mathbb{I}$, i.e. p is not incident to L.

Proof. Let p be a point contained in the plane. By **A3**, there exists three distinct non-collinear points a, b, and c. By **A1**, each pair of points determine a unique line. In contradiction, assume that p lies on each of the three lines $\overleftrightarrow{ab}$, $\overleftrightarrow{ac}$, and $\overleftrightarrow{bc}$. Since p is on $\overleftrightarrow{ab}$ and $\overleftrightarrow{ac}$, because of Corollary 1, $p = a$ since a is also on both. Likewise, since p is on $\overleftrightarrow{ac}$ and $\overleftrightarrow{bc}$, then $p = c$. Therefore, $a = c$. This contradicts the initial statement that they were distinct. Thus, p can't be on all three lines. Even if p was on two of the three lines, there still exists one line that does not go through p. □

THEOREM 1: Given an incidence geometry, let L and M be two distinct lines and let p be a point not incident to either line. The cardinality of $L_{pt} - \{t \in L_{pt} \mid \overleftrightarrow{pt} \parallel M\}$ is equal to the cardinality of $M_{pt} - \{u \in M_{pt} \mid \overleftrightarrow{pu} \parallel L\}$. In other words, if we remove the number of points x in each line such that $\overleftrightarrow{xp}$ is parallel to the other line, then the remaining number of points on each line are equal.

Proof. Given two distinct lines L and M, the claim is that there is a bijection between the points on "punctured" L and the points on "punctured" M. Given a point x lying on L, consider $\overleftrightarrow{xp}$, which exists by **A1**. By Corollary 1, if $\overleftrightarrow{xp}$ meets M at a unique point y. Define $f : L_{pt} - \{t \in L_{pt} \mid \overleftrightarrow{pt} \parallel M\} \to M_{pt} - \{u \in M_{pt} \mid \overleftrightarrow{pu} \parallel L\}$ by $f(x) = y$.

First, is the function injective? Consider $f(x_1) = f(x_2)$ where $x_1, x_2 \in L_{pt} - \{t \in L_{pt} \mid \overleftrightarrow{pt} \parallel M\}$. This means that $\overleftrightarrow{x_1p}$ and $\overleftrightarrow{x_2p}$ are incident to M at the same point y, i.e. $\overleftrightarrow{x_1p} = \overleftrightarrow{yp} = \overleftrightarrow{x_2p}$ by **A1**. But $\overleftrightarrow{x_1p}$ meets L at x_1 and $\overleftrightarrow{x_2p}$ meets L at x_2. Since $\overleftrightarrow{x_1p} = \overleftrightarrow{x_2p}$ and p is not incident to L, then $x_1 = x_2$ by Corollary 1. Thus, the function is injective.

Second, is the function surjective? Let $y \in M_{pt} - \{u \in M_{pt} \mid \overleftrightarrow{pu} \parallel L\}$. Consider $\overleftrightarrow{py}$. This line meets L at a unique point x since p is not incident to L and by Corollary 1. Therefore, by construction, y is on $\overleftrightarrow{xp}$. So $\overleftrightarrow{xp}$ and M meet at y by Corollary 1 and because p is not incident to M. So $f(x) = y$ and thus the function is surjective.

Since f is both injective and surjective, then it is a bijective function which means that there is a one-to-one correspondence between the points on one "punctured" line with another. $\square$

3.1 Definitions

DEFINITION 4: An Affine Plane is an Incidence Geometry that also satisfies **P1**.

An example of an Affine Plane is given in Figure 1 above.

LEMMA 2: In an affine geometry, given two intersecting lines, there exists a point not on either of those lines.

Proof. Given two lines, L and M, and an intersection point x, **A2** states there are at least two points on each line, so consider y on L and z on M. By **P1**, there is a unique line through z parallel to L. By **A2**, there is another point on this line, w. If w was incident to L, then $\overleftrightarrow{zw}$ would not be parallel to L. If w was incident to M, then $z = w$ by **A1**. Thus, there exists a point w not incident to L and M when L and M intersect. □

LEMMA 3: In an affine plane, every line has the same number of points.

Proof. Consider the same set-up given by Theorem 1. There are two cases that must be considered. Either L and M are parallel or they are not.

If they are not parallel, then by Lemma 2 there will always exist a point p not incident to L or M. So, consider the set $\{t \in L_{pt} \mid \overleftrightarrow{pt} \parallel M\}$. By **P1**, there is a unique line through p that is parallel to M. Thus, there is only one $t \in L_{pt}$ such that $\overleftrightarrow{pt} \parallel M$. Likewise, consider the set $\{u \in M_{pt} \mid \overleftrightarrow{pu} \parallel L\}$. There is a unique line through p that is parallel to L. Thus, there is only one $u \in M_{pt}$ such that $\overleftrightarrow{pu} \parallel L$. Since $|L_{pt}| - 1 = |M_{pt}| - 1$, then $|L_{pt}| = |M_{pt}|$.

If $L \parallel M$, then consider a slightly different set-up that does not require the extra point p. Consider the line $\overleftrightarrow{xy}$ where x lies on L and y lies on M, which exists by **A1**. Since L intersects with $\overleftrightarrow{xy}$, then as previously shown $|L_{pt}| = |\overleftrightarrow{xy}_{pt}|$. Likewise, since M intersects with $\overleftrightarrow{xy}$, then $|M_{pt}| = |\overleftrightarrow{xy}_{pt}|$. Therefore, $|L_{pt}| = |M_{pt}|$. □

DEFINITION 5: Define the order of an affine plane to be the number of points on a line.

For the remainder of this section, n will denote the order of an affine plane.

LEMMA 4: The total number of points in an affine plane is n^2.

Proof. Consider a line L. By the definition of n, there are n points on L. By Lemma 1, there exists a p that is not incident to L. Given a point x on L, by **A1** and since p is not incident to L, the line $\overleftrightarrow{xp} \neq L$. By definition, there are n points on $\overleftrightarrow{xp}$ as well. By **P1**, there is a unique line through each of the $n-1$ points on $\overleftrightarrow{xp}$ that is parallel to L.

Consider all of the points in the plane. We are claiming that every point is either on L or on one of the $n-1$ lines parallel to L. If the point is incident to L, then the claim holds true. If the point y is not incident to L, then there exists a unique line N through y parallel to L. If N and $\overleftrightarrow{xp}$ do not meet at any point, then $N \parallel \overleftrightarrow{xp}$. But $N \parallel L$ and therefore L would be parallel to $\overleftrightarrow{xp}$ which we know that it cannot be because x is incident to L and $\overleftrightarrow{xp}$. Thus, $N \nparallel \overleftrightarrow{xp}$ and so they meet at z. Since z is on $\overleftrightarrow{xp}$, then this line was already considered in our $n-1$ parallel lines to L. Therefore, every point in the plane is either on L or on the $n-1$ parallel lines to L. In other words, a family of parallel lines partitions the number of points in the plane.

So there are n parallel lines each with n points on them in which no other points exist in the plane. Hence, there are $n \cdot n = n^2$ points in the plane. □

Note that in this paper we are mainly concerned with finite projective planes, but if n were infinity, this idea still makes sense due to cardinal arithmetic. As well, note the result that a family of parallel lines partitions the number of points in the plane will be used throughout this paper.

LEMMA 5: In an affine plane, the number of lines in a family of parallel lines is n.

Proof. Given a line L, consider L and all of the lines parallel to L. As seen in the proof for Lemma 4, this family of parallel lines partitions the points in the plane. If there existed a point x incident to two lines in this family M and N, then $M \nparallel N$ and therefore $M = N$ by definition of the family. Since every line has n points and since the lines in a family of parallel lines partition the n^2 points in a plane, then there are $\frac{n^2}{n} = n$ lines in each family of parallel lines. □

LEMMA 6: The number of lines through a point in an affine plane is $n + 1$.

Proof. Let p be a point contained in a plane of order n. By Lemma 1, there exists a line L not incident to p. Since there are n points on L and every pair of distinct points determine a unique line, there are n lines through p. By **P1**, there is also a unique line through p that is parallel to L. Thus, there are $n + 1$ lines through the point p. □

LEMMA 7: The total number of lines in an affine plane is $n^2 + n$.

Proof. Given a line L, there are n points incident to L. By Lemma 6, each of the points have $n + 1$ lines through it. If you do not count L, then there are n lines through each of the points on L. Thus, there are n lines through each of the n points and L, i.e. $n(n) + 1 = n^2 + 1$ lines considered so far. But, by Lemma 5, there are $n - 1$ lines parallel to L. Therefore, there are $n^2 + 1 + n - 1 = n^2 + n$ lines in a plane of order n. □

LEMMA 8: In an affine plane, there are $n + 1$ families of parallel lines.

Proof. By Lemma 7, there are $n^2 + n$ lines in an affine plane. By Lemma 5, there are n lines in each family of parallel lines. Thus, there are $\frac{n^2+n}{n} = \frac{n(n+1)}{n} = n + 1$ families of parallel lines. □

3.2 Affine Plane From A Field

Definition 6: A field is a commutative ring with multiplicative identity in which all nonzero elements are units. Furthermore, the multiplicative identity 1 is not equal to the additive identity 0.

Definition 7 (Affine Plane over a Field): Given a field $\mathbb{F}$, the affine plane over $\mathbb{F}$, denoted $\mathbb{A}^2_{\mathbb{F}}$ has points $\mathbb{P} = \mathbb{F}^2 = \{(x, y) \mid x, y \in \mathbb{F}\}$ and lines $\mathbb{L} = \{\langle m, b\rangle \mid m, b \in \mathbb{F}\} \cup \{\langle c\rangle \mid c \in \mathbb{F}\}$ where

1. (x, y) is incident to $\langle m, b\rangle$ if and only if $y = mx + b$
2. (x, y) is incident to $\langle c\rangle$ if and only if $x = c$

Note that $\mathbb{A}^2_{\mathbb{R}}$ is the usual coordinatized Euclidean Plane.

Lemma 9: For an affine plane, $\mathbb{A}^2_{\mathbb{F}}$,

(1) Two lines $\langle m, b\rangle$ and $\langle n, c\rangle$ are parallel if and only if $m = n$ and $b \neq c$.

(2) The lines $\langle c\rangle$ and $\langle d\rangle$ are parallel if and only if $c \neq d$.

(3) Moreover, $\langle m, b\rangle$ is never parallel to $\langle c\rangle$.

Proof. (1) First, we want to show that if $\langle m, b\rangle$ and $\langle n, c\rangle$ are parallel, then $m = n$ and $b \neq c$. We can show this using the contrapositive which states that if $m \neq n$ or $b = c$, then $\langle m, b\rangle$ and $\langle n, c\rangle$ are not parallel. So if $m \neq n$, then the intersection point is at $x = \frac{c-b}{m-n}$. Thus $\langle m, b\rangle$ and $\langle n, c\rangle$ are not parallel. If $b = c$, then $(0, b)$ is on both lines and therefore $\langle m, b\rangle$ and $\langle n, c\rangle$ are not parallel.

Next, we want to show that if $m = n$ and $b \neq c$, then $\langle m, b\rangle$ and $\langle n, c\rangle$ are parallel. By way of contradiction, suppose there exists an (x, y) such that (x, y) is on both lines. Therefore, $y = mx+b$ and $y = nx+c$. By elimination, $0 = b-c$ which means that $b = c$. Thus, there cannot exist an (x, y) where the two lines intersect. This means $\langle m, b\rangle$ and $\langle n, c\rangle$ are parallel.

(2) Now we want to show that if $\langle c \rangle$ and $\langle d \rangle$ are parallel, then $c \neq d$. We can show this using the contrapositive that states if $c = d$, then $\langle c \rangle$ and $\langle d \rangle$ are not parallel. So if $c = d$, then (c, a) is on both lines are therefore are not parallel for all $a \in \mathbb{F}$. Next, we want to show that if $c \neq d$, then $\langle c \rangle$ and $\langle d \rangle$ are parallel. By way of contradiction, assume there exists a point (x, y) incident to both lines. This means $x = c$ and $x = d$ which means that $c = d$. Thus, there cannot exist an (x, y) where the two lines intersect. This means $\langle c \rangle$ and $\langle d \rangle$ are parallel.

(3) Lastly, $\langle m, b \rangle$ and $\langle c \rangle$ meet at the point $(c, mc + b)$ regardless of the values. Therefore, they can never be parallel. □

THEOREM 2: $\mathbb{A}^2_{\mathbb{F}}$ is an affine plane.

Proof. To prove that $\mathbb{A}^2_{\mathbb{F}}$ is an affine plane, it must satisfy the four axioms of an affine plane.

A1. Do two distinct points determine a unique line?

Given two points (x_1, y_1) and (x_2, y_2), first assume $x_1 \neq x_2$. Note that both of these points cannot be on a $\langle c \rangle$ because if they were, then $c = x_1$ and $c = x_2$ which would imply that $x_1 = x_2$ which is a contradiction. To find a line between these two points, let $m = \frac{y_1 - y_2}{x_1 - x_2}$ and $b = \frac{y_2 x_1 - y_1 x_2}{x_1 - x_2}$. To verify that these points are on the line,

$$\begin{aligned} mx_1 + b &= \frac{y_1 - y_2}{x_1 - x_2} x_1 + \frac{y_2 x_1 - y_1 x_2}{x_1 - x_2} \\ &= \frac{(y_1 - y_2)x_1 + y_2 x_1 - y_1 x_2}{x_1 - x_2} \\ &= \frac{y_1 x_1 - y_2 x_1 + y_2 x_1 - y_1 x_2}{x_1 - x_2} \\ &= \frac{y_1 x_1 - y_1 x_2}{x_1 - x_2} \\ &= \frac{y_1 (x_1 - x_2)}{x_1 - x_2} \end{aligned}$$

$$
\begin{aligned}
&= y_1 \\
mx_2 + b &= \frac{y_1 - y_2}{x_1 - x_2} x_2 + \frac{y_2 x_1 - y_1 x_2}{x_1 - x_2} \\
&= \frac{(y_1 - y_2)x_2 + y_2 x_1 - y_1 x_2}{x_1 - x_2} \\
&= \frac{y_1 x_2 - y_2 x_2 + y_2 x_1 - y_1 x_2}{x_1 - x_2} \\
&= \frac{-y_2 x_2 + y_2 x_1}{x_1 - x_2} \\
&= \frac{y_2(x_1 - x_2)}{x_1 - x_2} \\
&= y_2
\end{aligned}
$$

Thus, there is a line between (x_1, y_1) and (x_2, y_2). To show that this line is unique, assume that $\langle m, b\rangle$ and $\langle n, c\rangle$ are two lines that go through (x_1, y_1) and (x_2, y_2). Thus we get the following four equations,

$$y_1 = mx_1 + b \qquad\qquad y_1 = nx_1 + c$$

$$y_2 = mx_2 + b \qquad\qquad y_2 = nx_2 + c$$

Just looking at corresponding equations and using the transitive property,

$$mx_1 + b = nx_1 + c \qquad\qquad mx_2 + b = nx_2 + c$$

Using elimination by subtracting the right hand equation from the left hand equation,

$$mx_1 - mx_2 + b - b = nx_1 - nx_2 + c - c$$

$$mx_1 - mx_2 = nx_1 - nx_2$$

Therefore, $m(x_1 - x_2) = n(x_1 - x_2)$. Since $x_1 \neq x_2$ and they are both elements of a field, $m = n$. Thus, since $m = n$, $mx_1 + b = mx_1 + c$ reduces to $b = c$.

Hence, since $m = n$ and $b = c$, $\langle m, b\rangle = \langle n, c\rangle$. Therefore the line between these two points is unique.

Now assume $x_1 = x_2 = c$. Note that these lines can't be on an $\langle m, b\rangle$ line. Indeed, if they were, then $y_1 = mc + b$ and $y_2 = mc + b$ which would imply that $y_1 = y_2$ which means that the points are not distinct. Thus, the line would be $\langle c\rangle$. To show that this line is unique by way of contradiction, let's assume that two lines $\langle c_1\rangle$ and $\langle c_2\rangle$ go through these two points. Then by construction, $c = c_1$ and $c = c_2$. Thus, $c_1 = c_2$ and therefore $\langle c_1\rangle = \langle c_2\rangle$. Therefore the line between these two points is unique.

A2. Does every line contain at least 2 points?

Regardless of the field, there always exists 0, the additive identity and 1, the multiplicative identity where $0 \neq 1$. Therefore, given the line $\langle m, b\rangle$, the points $(0, b)$ and $(1, m + b)$ are on that line. Likewise, given the line $\langle c\rangle$, the points $(c, 0)$ and $(c, 1)$ are on that line. Thus, every line contains at least 2 points.

A3. Do there exist three non-collinear points?

We have three points $(0, 0)$, $(0, 1)$, and $(1, 0)$. The line through the first two is $\langle 0\rangle$. The point $(1, 0)$ is not incident to $\langle 0\rangle$ because then $1 = 0$ which is certainly not true. Thus, there are 3 non-collinear points.

P1. Does it satisfy the euclidean property?

Given the line $\langle m, b\rangle$ and the point (x_1, y_1) which is not incident to $\langle m, b\rangle$, the parallel line would be $\langle m, y_1 - mx_1\rangle$. This line is parallel because of Lemma 9 (1). To show this line is unique, assume there is another line through (x_1, y_1), $\langle m, b'\rangle$. Since (x_1, y_1) is incident to both lines,

$$y_1 = mx_1 + y_1 - mx_1 \qquad \text{and} \qquad y_1 = mx_1 + b'$$

Thus,

$$mx_1 + y_1 - mx_1 = mx_1 + b'$$

$$y_1 - mx_1 = b'$$

Since $y_1 - mx_1 = b'$, then these two lines are the same line. Thus, this line is a unique line.

Now consider the line $\langle c \rangle$ and the point (x_1, y_1) which is not incident to $\langle c \rangle$. The parallel line would be $\langle x_1 \rangle$. This line is parallel because of Lemma 9 (2). To show this line is unique, assume there is another line through (x_1, y_1), $\langle d \rangle$. By construction, then $d = x_1$ which would mean that the two lines are the same. Thus, this line is a unique line.

Since $\mathbb{A}^2_{\mathbb{F}}$ satisfies all four axioms of an affine plane, then it is an affine plane. $\square$

Figure 5 shows an example of an affine plane other than $\mathbb{A}^2_{\mathbb{R}}$. This happens to be the affine plane over the field $\mathbb{F}_2 = \{0, 1\}$. The set of points in $\mathbb{F}_2^2$ are $\mathbb{P} = \{(0,0), (0,1), (1,0), (1,1)\}$ and the set of lines are $\mathbb{L} = \{\langle 0,0 \rangle, \langle 0,1 \rangle, \langle 1,0 \rangle, \langle 1,1 \rangle, \langle 0 \rangle, \langle 1 \rangle\}$. Most of the lines are similar to what you would see in $\mathbb{A}^2_{\mathbb{R}}$ except the line $\langle 1,1 \rangle$. Recall from the construction that this line corresponds to the equation $x + 1 = y$. Therefore $(0,1)$ is incident to this line because $0 + 1 = 1$. As well, $(1,0)$ is incident to this line because $1 + 1 = 2 \equiv 0 \pmod 2$. Note that this geometry is the same one seen earlier in Figure 1.

Even though this plane came from an intuition of the normal xy-plane, the points and lines do not have to be in that specific order. For example, Figure 6 is isomorphic to Figure 5.

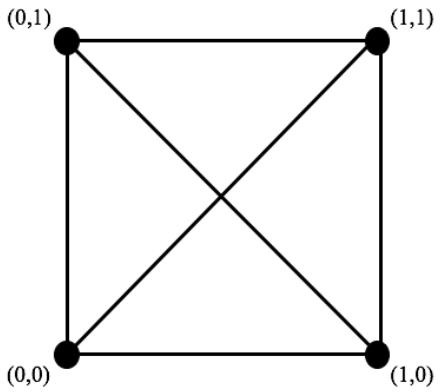

Figure 5: Affine Plane over $\mathbb{F}_2^2$

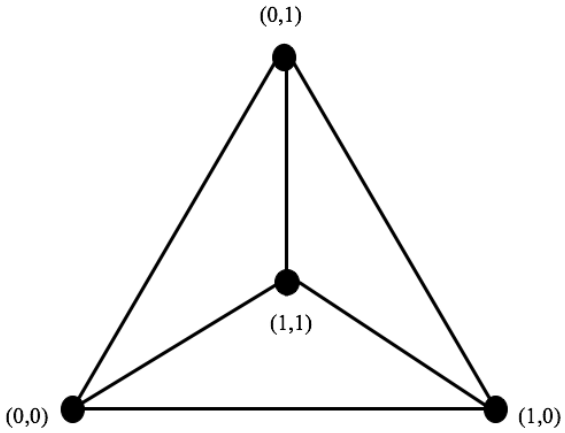

Figure 6: A Graph Isomorphic to Figure 5

4.1 Definitions

Definition 8: A Projective Plane is an Incidence Geometry that satisfies **P2** as well as

A2$^+$. Given $L \in \mathbb{L}$, there exists distinct $p, q, r \in \mathbb{P}$ such that $(p, L), (q, L), (r, L) \in \mathbb{I}$.

The axiom **A2**$^+$ informally states that each line now must contain at least three points instead of two.

The smallest plane is called the Fano Plane seen in Figure 7. The Fano Plane has 7 points and 7 lines: the six normal lines and the one in the center that looks like a circle. One can go through each of the axioms to verify that the Fano Plane is a projective plane.

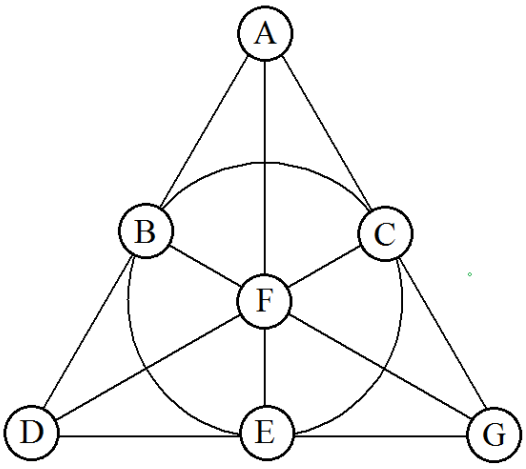

Figure 7: Fano Plane

Corollary 2: In a projective plane, each pair of lines meet at a unique point.

Proof. By Corollary 1, every pair of lines either meet at one unique point or they don't meet at all. But by **P2**, every pair of lines meet at some point, therefore they can't not meet. Thus, every pair of lines meet at a unique point. □

LEMMA 10: Given two lines in a projective plane, there exists a point not on either of those lines.

Proof. By Corollary 2, given two distinct lines, L and M, they meet at a unique point, p. By $\mathbf{A2}^+$, these lines have another point on them, q on L and r on M. Since these lines only meet at one point, q is not on M and r is not on L. Therefore, $q \neq r$. Then by **A1**, there exists a unique line $\overleftrightarrow{qr}$ through q and r. $\mathbf{A2}^+$ states there exists another point s on $\overleftrightarrow{qr}$. Using Corollary 2, s does not lie on L nor M. Thus, given two lines, there exists a point not on either of these. □

THEOREM 3: In a given projective plane, every line contains the same number of points.

Proof. Let L and M be two distinct lines in the same set-up given by Theorem 1. By Lemma 10, there exists a point p not incident to either line. Since there are no parallel lines in a projective plane, $|\{t \in L_{pt} \mid \overleftrightarrow{pt} \parallel M\}| = |\{u \in M_{pt} \mid \overleftrightarrow{pu} \parallel L\}| = 0$. Thus, the function would just map L_{pt} to M_{pt}, i.e. $f : L_{pt} \to M_{pt}$.

Since f is both injective and surjective, then it is a bijective function which means that there is a one-to-one correspondence between the points on one line with another. Thus, every line contains the same number of points. □

DEFINITION 9: For a given projective plane, define the order of the plane to be the number of points on a given line minus 1.

Thus, there are $n + 1$ points on each line. Note that a projective plane cannot have order 1, i.e. $n \geq 2$. If it was possible, then this would violate $\mathbf{A2}^+$ because there would be $1 + 1 = 2$ points on each line.

In the Fano Plane, as mentioned earlier, the order is $n = 2$. There are 3 points on each line, which is $n + 1$. As an example for the following lemmas and theorems, the Fano Plane is a good way to see what is going on. So by Theorem 4, there are

$n+1 = 3$ lines through each point. By Theorem 5, there are $n^2+n+1 = 2^2+2+1 = 7$ total points and 7 total lines in the plane.

THEOREM 4: In a projective plane of order n, every point has $n + 1$ lines through it.

Proof. Let p be a point contained in a plane of order n. By Lemma 1, there exists a line L that does not go through p. Since there are $n + 1$ points on L and every pair of distinct points determine a unique line, there are $n + 1$ lines through p. Because of **P2**, there cannot be any other lines through p. If there were another line through p, then that line would also have to cross L at some point. Since every point on L was already considered, then this line was already considered. Therefore, there are $n + 1$ points through any given point. □

THEOREM 5: The total number of points in a projective plane of order n is given by $n^2 + n + 1$. The number of lines is also $n^2 + n + 1$.

Proof. Let p be a point contained in a plane of order n. From Theorems 3 and 4, there are $n + 1$ lines that go through p and each of those lines have $n + 1$ points on them. Since each line has $n + 1$ points on it, there are n points remaining on each line because p is already defined as being on each of those lines. Thus, there are n points on $n + 1$ lines and p. Therefore, there are $n(n + 1) + 1 = n^2 + n + 1$ points total in the plane.

Let L be a line contained in a plane of order n. From Theorems 3 and 4, there are $n + 1$ points on L and each of those points have $n + 1$ lines through them them. Since each point has $n+1$ lines through it, there are n lines remaining through each line because L is already defined as going through those points. Thus, there are n lines going through $n+1$ points and L. Therefore, there are $n(n+1)+1 = n^2+n+1$ lines total in the plane. □

4.2 Duality

In projective geometry, every dual statement in which the lines and points swap roles is a theorem. Each of the axioms can be used to prove the dual of each axiom. The duals of each axiom are as follows:

A1. Two distinct lines determine (intersect at) a unique point.

Proof. This is precisely Corollary 2. □

A2$^+$. There are at least three lines through each point.

Proof. By **A2**$^+$, there are at least three points on each line. Thus, the order is at least 2. By Theorem 4, there are $n + 1$ lines through each point. Thus, there are at least $2 + 1 = 3$ lines through every point. □

A3. There exist three non-concurrent lines.

Proof. By **A3**, there exist three non-collinear points p, q, and r. Consider the lines $\overleftrightarrow{pq}$, $\overleftrightarrow{qr}$ and $\overleftrightarrow{pr}$. Since each pair of these lines meet at one of the three named points, then they cannot meet elsewhere by **A1**. Therefore, $\overleftrightarrow{pq}$, $\overleftrightarrow{qr}$ and $\overleftrightarrow{pr}$ do not all three go through the same point and thus they are non-concurrent. □

P2. Given a point p and all lines L that don't pass through p, consider a point q on L. There will always exist a line M through both p and q.

Proof. By **A1**, two points determine a unique line, thus M will always exist.

□

Given any projective plane, you can get a "new" plane by taking it's dual (by switching the role of the lines and points).

4.3 Projective Plane From An Affine Plane

Given an affine plane, define a relation on the lines of an affine plane by

$$l \sim m \iff l \parallel m \text{ or } l = m$$

PROPOSITION 1: This relation is an equivalence relation.

Proof. To prove this is an equivalence relation, it must be reflexive, symmetric, and transitive.

1. Is the relation reflexive? Does $l \sim l$? Because $l = l$, then $l \sim l$. Thus, it is reflexive.

2. Is the relation symmetric? Is $l \sim m$ imply $m \sim l$? Since $l \sim m$, then either $l \parallel m$ or $l = m$. If $l \parallel m$, then because parallelism is symmetric, then $m \parallel l$. Otherwise, if $l = m$, then because equality is symmetric, then $m = l$. Regardless of the case, $m \sim l$ and thus the relation is symmetric.

3. Is the relation transitive? If $l \sim m$ and $m \sim n$, does this imply that $l \sim n$? This must be split into several different cases,

   (i) If $l = m$, then $l \sim n$ because $m \sim n$.

   (ii) If $l \parallel m$ and $m = n$, then $l \parallel n$ and thus $l \sim n$.

   (iii) If $l \parallel m$ and $m \parallel n$, then either $l = n$ or $l \neq n$. If $l = n$, then $l \sim n$. Otherwise, if $l \neq n$, we claim that $l \parallel n$. This is because if $l \nparallel n$, then there would exist a point p on both l and n. Because they are parallel to m, p is not incident to m. Thus, by the euclidean property, there must be a unique line through p parallel to m. But since l and n are distinct lines through p and we assumed $l \neq n$, then there can't exist a point p and thus they are parallel. Therefore $l \parallel n$, hence $l \sim n$.

Regardless of the case, we have $l \sim n$ making the equivalence relation transitive.

□

The equivalence class $[l]$ is the set of lines that are equivalent to l. As described in the introduction, Poncelet had these points that he called "points at infinity." In this construction, we are going to consider every equivalence class $[l]$ as a point at infinity. So given any affine plane $\mathbb{A}$, we want to construct the projective plane from $\mathbb{A}$ such that the set of points are the points of $\mathbb{A}$ and the points at infinity, i.e., there are more points in the projective plane than in $\mathbb{A}$. The set of lines in the projective plane are the lines of $\mathbb{A}$ and the line at infinity. This new line is the line that is incident to all of the points at infinity and none of the originial points of $\mathbb{A}$.

Definition 10: More formally, given an affine plane $\mathbb{A}$, a projective plane constructed from $\mathbb{A}$ denoted Proj($\mathbb{A}$) is formed from points being $\mathbb{P} = \{p \mid p \in \mathbb{A}\} \cup \{[l] \mid l \in \mathbb{A}\}$ and lines $\mathbb{L} = \{l \mid l \in \mathbb{A}\} \cup \{l_\infty\}$ where

1. p is incident to l if and only if p is incident to l in $\mathbb{A}$
2. p is never incident to l_∞
3. $[l]$ is incident to m where $m \in [l]$ in $\mathbb{A}$
4. $[l]$ is always incident to l_∞

Theorem 6: Proj($\mathbb{A}$) is a projective plane.

Proof. The four axioms of a projective plane:

A1. Do two distinct points determine a unique line?

If given two distinct points p and q, then by **A1**, they would determine a unique line because the points are also in $\mathbb{A}$. If given two distinct points $[l]$ and $[m]$, then by definition they are both on l_∞. They cannot be on another

line n because if $[l]$ and $[m]$ were incident to n, then $n \in [l]$ and $n \in [m]$ which would mean that $[l] = [m]$ since equivalence classes are always a disjoint partition of a set. If given two distinct points p and $[l]$, the line through them cannot be l_∞ by definition, therefore they must be on a line m. Therefore, $m \in [l]$ and p is incident to m in $\mathbb{A}$. Because $m \in [l]$, then either $m = l$ or $m \parallel l$. If p is incident to l, then $m = l$. If p is not incident to l, then by the euclidean property, there is a unique line through p parallel to l, which is m in this case.

A2$^+$. Does each line contain at least three points?

Since this plane comes from an affine plane, every line l contains at least two points. In this construction, we are adding a point at infinity, $[l]$ to each l. Thus, each line from $\mathbb{A}$ has three points incident to it. Are there three points on l_∞? Since there are three non-collinear points $a, b, c \in \mathbb{A}$, then there are three distinct lines $\overleftrightarrow{ab}, \overleftrightarrow{ac}, \overleftrightarrow{bc} \in \mathbb{A}$. Thus, $[\overleftrightarrow{ab}]$, $[\overleftrightarrow{ac}]$, and $[\overleftrightarrow{bc}]$ are all incident to l_∞.

A3. Do there exist three non-collinear points?

By **A3**, there exists three points in $\mathbb{A}$ that are non-collinear. Since all of those points are still in Proj($\mathbb{A}$), then they are still non-collinear.

P2. Does every pair of lines meet at some point?

Given two distinct lines, l and m, then either they do meet in $\mathbb{A}$ or they don't meet. If they do meet in $\mathbb{A}$, then they would still meet in Proj($\mathbb{A}$). If they did not meet in $\mathbb{A}$, then they are in the same equivalence class (they were parallel). By part 3 of Definition 10, these lines meet at $[l]$ in Proj($\mathbb{A}$). If given the distinct lines l and l_∞, then by definition, $[l]$ is incident to l and l_∞.

Since Proj($\mathbb{A}$) satisfies all four axioms of a projective plane, then it is a projective

plane. □

Looking back at the example from above in Figures 5 and 6 with the affine plane $\mathbb{F}_2^2$, we can construct a projective plane using this. First, we need the equivalence classes from $\mathbb{F}_2^2$. Thus, which lines never cross at a point? The following equivalence classes are obtained:

$$E = [\langle 0,0\rangle] = \{\langle 0,0\rangle, \langle 0,1\rangle\}$$
$$C = [\langle 1,0\rangle] = \{\langle 1,0\rangle, \langle 1,1\rangle\}$$
$$B = [\langle 0\rangle] = \{\langle 0\rangle, \langle 1\rangle\}$$

Therefore, in constructing $\text{Proj}(\mathbb{F}_2^2)$, the set of points are $\mathbb{P} = \{p \mid p \in \mathbb{F}_2^2\} \cup \{E, C, B\}$ and the set of lines are $\mathbb{L} = \{l \mid l \in \mathbb{F}_2^2\} \cup \{l_\infty\}$. The plane would look roughly like Figure 8.

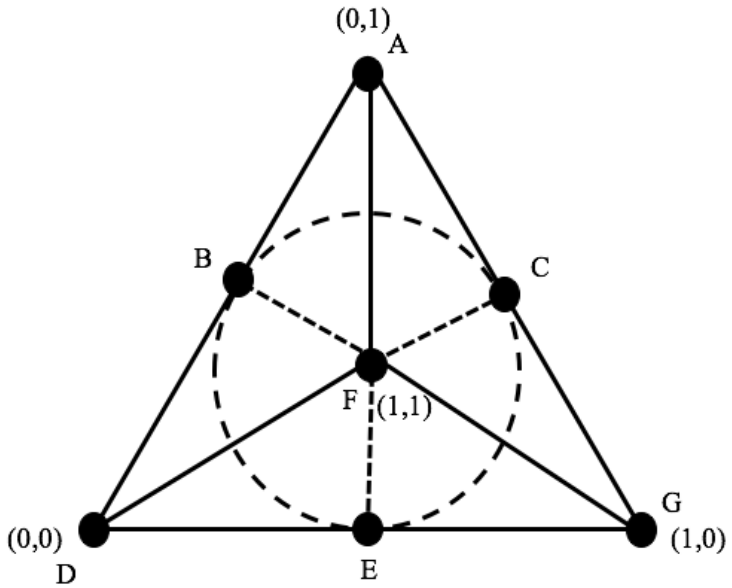

Figure 8: Projective Plane from the Affine Plane over $\mathbb{F}_2^2$

The dotted lines indicate the extensions of previous lines from Figure 6 and the

line at infinity (the circle). Note that this plane is isomorphic to the Fano Plane first discussed where the original four points are D, G, A, and F, respectively and E, C, and B from this example correspond to those points in Figure 7.

4.4 Affine Plane From A Projective Plane

One thing that needs to be considered is if we are given a projective plane, can we return back to an affine plane? In other words, can we take out one line as well as the points on it and result in an affine plane? So given a projective plane, P, let's take out the line at infinity containing the points at infinity and check the axioms of an affine plane to see if we get an affine plane.

DEFINITION 11: More formally, given a projective plane P, an affine plane constructed from P denoted Aff(P) is formed from removing one line from the set of lines in P and all of the points incident to that line.

LEMMA 11: Given a line l in a projective plane P, there exists three non-collinear points that are not incident to l.

Proof. Given a line l, there exists two points incident to l, a and b. Because of **P3**, since there are three non-collinear points in P, there exists a point c not incident to l. By **A1**, $\overleftrightarrow{ac}$ and $\overleftrightarrow{bc}$ are two distinct lines. $\mathbf{A2}^+$ states that there are three points on each line. So there exists a point d incident to $\overleftrightarrow{ac}$ and a point e incident to $\overleftrightarrow{bc}$. Because these two lines are distinct, c, d, and e are non-collinear and are not incident to l. If they were the same line, then they would be incident to l at a and at b. Therefore, the two lines are distinct. □

THEOREM 7: Aff(P) is an affine plane.

Proof. The four axioms of an affine plane:

A1. Do two distinct points determine a unique line?

Given two distinct points not on the removed line, p and q, they determined a unique line in P. Therefore, since we are removing one line and those points incident to the line, then p and q still determine that one unique line.

A2. Does every line contain at least 2 points?

Recall from projective planes, each line had at least 3 points. So accounting for each line losing one point (those points at infinity), each line still has at least two points.

A3. Do there exist 3 non-collinear points?

From Lemma 11, if you remove one line, there are still three non-collinear points not incident to that line.

P1. Does it satisfy the euclidean property?

Given two lines l and m with intersection at q and a point p not incident to either of the lines, let n be the unique line through p and q by **A1**. If l is the line removed, then q is also removed. Therefore, m and n have no intersection point. In other words, m and n are parallel to each other. Thus, given a line m and a point p, there exists a line parallel to m through p. Is this line unique? Assume there exists another line n' through p that is also parallel to m. Through the original construction with **P2**, n' and m intersect at a point r. If $r \neq q$, then r would still be left in the plane once l is removed. Thus, m and n' would still intersect. Therefore, $r = q$. Since $r = q$, then $n = n'$ and thus the line is unique.

Since Aff(P) satisfies all four axioms of an affine plane, then it is an affine plane.

□

It should be noted that if you begin with an affine plane $\mathbb{A}$ of order n and constructed $P = \text{Proj}(\mathbb{A})$, you would not necessarily end up with $\mathbb{A}$ when constructing $\text{Aff}(P)$. If you took out the same line at infinity that you added to the affine plane, then you would get the same plane back. But if you take another line out, it is conceivable that this plane might not be isomorphic to the original affine plane.

4.5 Projective Plane Directly From A Field

The plan under this construction from a field is to use equations to obtain our incidence relations and use three-tuples from elements in our field as points and lines. We can think about the following construction using Euclidean three-space for geometric intuition. Consider the plane $z = 1$ and all of the lines through the origin. Since $z = 1$ is the xy-plane shifted up one unit, the points in $z = 1$ make up an affine plane because of Theorem 2. There is a one-to-one correspondence between the points in this plane and some of the lines through the origin in $\mathbb{R}^3$. This correspondence is given by taking the line through the point in the plane $z = 1$ and the origin. Note that horizontal lines do not arise in this way. We will identify the points in the affine plane with non-horizontal lines through the origin in $\mathbb{R}^3$. Similarly, every line in $z = 1$ corresponds to a plane through the origin in $\mathbb{R}^3$ (except for the xy-plane).

Recalling our construction of a projective plane from an affine plane, we need to add points at infinity and a line at infinity. Given a line in the plane $z = 1$ and a sequence of points going toward infinity, the corresponding lines in $\mathbb{R}^3$ become more and more horizontal and the limit will lie in the xy-plane. These will be our points at infinity and the xy-plane will be the line at infinity.

The equation of a line parametrically in three-space is given by $x = \alpha t$, $y = \beta t$, and $z = \gamma t$; so we can represent lines by (α, β, γ). However, noting that multiply-

ing this triple by a scalar to results in the same line which motivates the need for Proposition 2.

The equation of a plane in three-space is given by $ax + by + cz = d$. Since we want the planes to go through the origin, we instead use $ax + by + cz = 0$; so we can represent these planes as $\langle a, b, c\rangle$. Likewise, noting that multiplying this triple by a scalar results in the same plane which motivates the need for Proposition 3.

We know that a line is incident to a plane whenever there is equality through the equation of our plane, i.e. when $ax + by + cz = 0$. Since we know the equations of our lines parametrically, $ax + by + cz = a(\alpha t) + b(\beta t) + c(\gamma t) = 0$. Since we want this to be true for all t, then we need to consider $t \neq 0$ and thus a line is incident to a plane whenever $a\alpha + b\beta + c\gamma = 0$.

For a given field, $\mathbb{F}$, define a relation for the points on triples $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ where $(\alpha, \beta, \gamma) \in \mathbb{F}^3$ such that, for some $\lambda \neq 0$,

$$(\alpha, \beta, \gamma) \quad \sim \quad (\alpha', \beta', \gamma') \quad \iff \quad (\alpha, \beta, \gamma) = \lambda(\alpha', \beta', \gamma')$$

Proposition 2: This relation is an equivalence relation.

Proof. To prove this is an equivalence relation, it must be reflexive, symmetric, and transitive.

1. Is the relation reflexive? Does $(\alpha, \beta, \gamma) \quad \sim \quad (\alpha, \beta, \gamma)$? Taking $\lambda = 1$, then $(\alpha, \beta, \gamma) = 1(\alpha, \beta, \gamma)$. Thus, the relation is reflexive.

2. Is the relation symmetric? Does $(\alpha, \beta, \gamma) \quad \sim \quad (\alpha', \beta', \gamma')$ imply $(\alpha', \beta', \gamma') \quad \sim \quad (\alpha, \beta, \gamma)$? If $(\alpha, \beta, \gamma) \quad \sim \quad (\alpha', \beta', \gamma')$, then there exists a nonzero λ in the field such that $(\alpha, \beta, \gamma) = \lambda(\alpha', \beta', \gamma')$. Since $\mathbb{F}$ is a field, then $\lambda^{-1} \in \mathbb{F}$ and thus by multiplying both sides of the equation by λ^{-1}, $\lambda^{-1}(\alpha, \beta, \gamma) = (\alpha', \beta', \gamma')$. Therefore, $(\alpha', \beta', \gamma') \quad \sim \quad (\alpha, \beta, \gamma)$.

3. Is the relation transitive? If $(\alpha, \beta, \gamma) \sim (\alpha', \beta', \gamma')$ and $(\alpha', \beta', \gamma') \sim (\alpha'', \beta'', \gamma'')$, does this imply that $(\alpha, \beta, \gamma) \sim (\alpha'', \beta'', \gamma'')$? If $(\alpha, \beta, \gamma) \sim (\alpha', \beta', \gamma')$, then there exists a nonzero λ in the field such that $(\alpha, \beta, \gamma) = \lambda(\alpha', \beta', \gamma')$. Likewise, if $(\alpha', \beta', \gamma') \sim (\alpha'', \beta'', \gamma'')$, then there exists a nonzero ϵ in the field such that $(\alpha', \beta', \gamma') = \epsilon(\alpha', \beta', \gamma'')$. Therefore,

$$(\alpha, \beta, \gamma) = \lambda(\alpha', \beta', \gamma')$$

$$(\alpha, \beta, \gamma) = \lambda\Big(\epsilon(\alpha'', \beta'', \gamma'')\Big)$$

Because we are doing multiplication in a field, then we can re-associate through scalar multiplication,

$$(\alpha, \beta, \gamma) = (\lambda\epsilon)(\alpha'', \beta'', \gamma'')$$

Since $\lambda, \epsilon \in \mathbb{F}$, then $\Lambda = \lambda\epsilon \in \mathbb{F}$ because of closure. Since $\lambda \neq 0$ and $\epsilon \neq 0$, then because these are elements in a field, $\Lambda \neq 0$. Thus $(\alpha, \beta, \gamma) = \Lambda(\alpha'', \beta'', \gamma'')$ and therefore $(\alpha, \beta, \gamma) \sim (\alpha'', \beta'', \gamma'')$.

□

Likewise, define a relation for the lines on triples $\langle a, b, c\rangle \neq \langle 0, 0, 0\rangle$ where $\langle a, b, c\rangle \in \mathbb{F}^3$ such that, for some $\lambda \neq 0$,

$$\langle a, b, c\rangle \sim \langle a', b', c'\rangle \iff \langle a, b, c\rangle = \lambda\langle a', b', c'\rangle$$

Proposition 3: This relation is an equivalence relation.

Proof. This proof is identical to the proof for Proposition 2. The only difference is the grouping symbols around the entries. □

Through these two relations, we can construct a projective plane from the field where the points are lines in the affine three-space through the origin and the lines

are the planes in affine three-space through the origin.

DEFINITION 12: Given a field, $\mathbb{F}$, the projective plane over $\mathbb{F}$ denoted Proj($\mathbb{F}$) has points being $\mathbb{P} = \{[(\alpha, \beta, \gamma)] \mid [(\alpha, \beta, \gamma)] \neq [(0, 0, 0)]\}$ and lines being $\mathbb{L} = \{[\langle a, b, c\rangle] \mid [\langle a, b, c\rangle] \neq [\langle 0, 0, 0\rangle]\}$ where a point is incident to a line if $a\alpha + b\beta + c\gamma = 0$.

To list all of the equivalence classes of points (or lines) in this set-up, we used the following procedure.

1. If $\gamma \neq 0$, then $(\alpha, \beta, \gamma) \sim \gamma^{-1}(\alpha, \beta, \gamma) = (\alpha\gamma^{-1}, \beta\gamma^{-1}, 1) = (x, y, 1)$. Thus, we can list every triple using every pairing of x and y following a similar set-up.

2. If $\gamma = 0$ and $\beta \neq 0$, then $(\alpha, \beta, 0) \sim \beta^{-1}(\alpha, \beta, 0) = (\alpha\beta^{-1}, 1, 0) = (x, 1, 0)$. Thus, we can list every triple using every value of x.

3. If $\gamma = \beta = 0$ and $\alpha \neq 0$, then $(\alpha, 0, 0) \sim \alpha^{-1}(\alpha, 0, 0) = (1, 0, 0)$.

Note that in this procedure, if the field had n elements, Step 1 would result in n^2 different equivalence classes because there are n choices for x and n choices for y. Step 2 would result in n different equivalence classes because there are n choices for x. Lastly, Step 3 would only have one equivalence class. Thus, there are $n^2 + n + 1$ equivalence classes. Recall from Theorem 5 that there are $n^2 + n + 1$ lines and $n^2 + n + 1$ points in a projective plane of order n.

Figure 9 is a table of the field $\mathbb{F}_2^3$ and the points on each line. An "$\times$" implies it lies on the line. One can quickly check and see that each line (denoted with $\langle a, b, c\rangle$) has 3 points on it (satisfying $\mathbf{A2}^+$). As well, it is easy to see that there exists 3 non-collinear points (**A3**) by looking at the first two points listed and the last point. Likewise, all lines meet together at some point (**P2**). Two points determine a unique line (i.e. two points are not on another line together), satisfying **A1**. Thus, this set-up is a projective geometry. We can check the theorems as well and see that every line contains the same number of points (3 for this case).

	$[\langle 0,0,1\rangle]$	$[\langle 0,1,1\rangle]$	$[\langle 1,0,1\rangle]$	$[\langle 1,1,1\rangle]$	$[\langle 0,1,0\rangle]$	$[\langle 1,1,0\rangle]$	$[\langle 1,0,0\rangle]$
[(0,0,1)]					×	×	×
[(0,1,1)]		×		×			×
[(1,0,1)]			×	×	×		
[(1,1,1)]		×	×			×	
[(0,1,0)]	×		×				×
[(1,1,0)]	×			×		×	
[(1,0,0)]	×	×			×		

Figure 9: Incidence Table for $\mathbb{F}_2^3$

Using this incidence table, we can construct an incidence matrix taking each of the blank spaces as zeros and the × as ones, as seen below:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Figure 10 is a table of the field $\mathbb{F}_3^3$ and the points on each line. An "×" implies it lies on the line. Just as before, one can check to make sure that it satisfies the four axioms.

Likewise, an incidence matrix can be made from this set as well. Figure 10 represents the projective plane of order 3 which is displayed below in Figure 11.

	$[\langle 0,0,1\rangle]$	$[\langle 0,1,1\rangle]$	$[\langle 0,2,1\rangle]$	$[\langle 1,0,1\rangle]$	$[\langle 1,1,1\rangle]$	$[\langle 1,2,1\rangle]$	$[\langle 2,0,1\rangle]$	$[\langle 2,1,1\rangle]$	$[\langle 2,2,1\rangle]$	$[\langle 0,1,0\rangle]$	$[\langle 1,1,0\rangle]$	$[\langle 2,1,0\rangle]$	$[\langle 1,0,0\rangle]$
[(0,0,1)]										×	×	×	×
[(0,1,1)]			×			×			×				×
[(0,2,1)]		×			×			×					×
[(1,0,1)]							×	×	×	×			
[(1,1,1)]			×		×		×					×	
[(1,2,1)]		×				×	×				×		
[(2,0,1)]				×	×	×				×			
[(2,1,1)]			×	×				×			×		
[(2,2,1)]		×		×					×			×	
[(0,1,0)]	×			×			×						×
[(1,1,0)]	×					×		×				×	
[(2,1,0)]	×				×				×		×		
[(1,0,0)]	×	×	×							×			

Figure 10: Incidence Table for $\mathbb{F}_3^3$

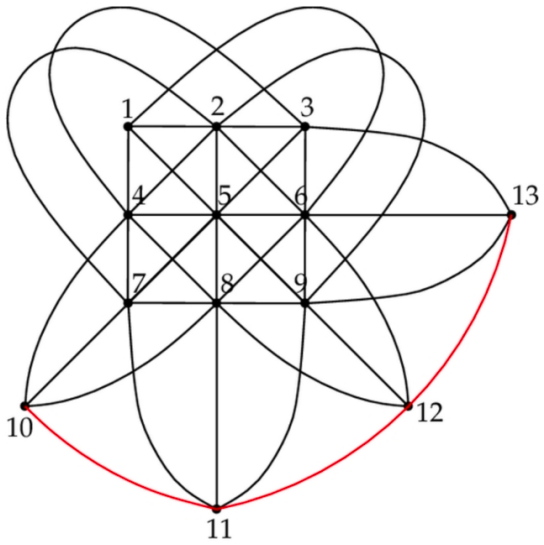

Figure 11: Projective Plane of Order 3

5.1 Affine Plane From Latin Squares

DEFINITION 13: A Latin Square of order n is an n by n table whose entries come from a set of elements $[n] = \{1, 2, \ldots, n\}$ and no column or row has any repeated entries.

An example of a Latin Square for [5] can be seen below.

4	3	2	1	5
3	2	1	5	4
2	1	5	4	3
1	5	4	3	2
5	4	3	2	1

DEFINITION 14: Two Latin Squares,

$$\mathrm{A} = \begin{array}{|c|c|c|c|} \hline a_{11} & a_{12} & \cdots & a_{1n} \\ \hline a_{21} & a_{22} & \cdots & a_{2n} \\ \hline & & \cdots & \\ \hline a_{n1} & a_{n2} & \cdots & a_{nn} \\ \hline \end{array} \text{ and } \mathrm{B} = \begin{array}{|c|c|c|c|} \hline b_{11} & b_{12} & \cdots & b_{1n} \\ \hline b_{21} & b_{22} & \cdots & b_{2n} \\ \hline & & \cdots & \\ \hline b_{n1} & b_{n2} & \cdots & b_{nn} \\ \hline \end{array}$$

are orthogonal if the product

$$\mathrm{A} \times \mathrm{B} = \begin{array}{|c|c|c|c|} \hline (a_{11}, b_{11}) & (a_{12}, b_{12}) & \cdots & (a_{1n}, b_{1n}) \\ \hline (a_{21}, b_{21}) & (a_{22}, b_{22}) & \cdots & (a_{2n}, b_{2n}) \\ \hline & & \cdots & \\ \hline (a_{n1}, b_{n1}) & (a_{n2}, b_{n2}) & \cdots & (a_{nn}, b_{nn}) \\ \hline \end{array}$$

contains every ordered pair in $[n]^2$.

For example, these 2 Latin Squares for [5] are orthogonal.

A =

4	3	2	1	5
3	2	1	5	4
2	1	5	4	3
1	5	4	3	2
5	4	3	2	1

and B =

5	4	3	2	1
1	5	4	3	2
2	1	5	4	3
3	2	1	5	4
4	3	2	1	5

A × B =

(4,5)	(3,4)	(2,3)	(1,2)	(5,1)
(3,1)	(2,5)	(1,4)	(5,3)	(4,2)
(2,2)	(1,1)	(5,5)	(4,4)	(3,3)
(1,3)	(5,2)	(4,1)	(3,5)	(2,4)
(5,4)	(4,3)	(3,2)	(2,1)	(1,5)

Note that every solution of the popular number placement puzzle, Sudoku, is a 9 by 9 Latin Square. Sudoku, however, places an extra restriction on the number placement where each of the nine 3 by 3 grids must contain the numbers 1 through 9.

THEOREM 8: There is an affine plane of order n ($n \geq 2$) if and only if there are $n-1$ orthogonal n by n Latin Squares.

Proof. ($\Rightarrow$) Given an affine plane of order n, we want to show that there are $n-1$ orthogonal Latin Squares. As shown in Lemmas 5 and 8, there are n lines in each of the $n+1$ families of parallel lines.

Consider two of the families of parallel lines $[L]$ and $[M]$. In each of these families, there are n lines each with n points on them. We can number each of these lines as L_1, L_2, ..., L_n and M_1, M_2, ..., M_n. The idea is to make a coordinate system out of these. Given a point x, x is associated with (i, j) if x is incident to L_i and x is incident to M_j. The point x will be denoted $p_{(i,j)}$.

Consider another family $[N]$. We can number these lines as $1, 2, \ldots, n$. In the n by n Latin Square we are constructing, we will put k in entry (i, j) when $p_{(i,j)}$ lies

on N_k. These are n by n because there are n lines in $[L]$ and n lines in $[M]$ which would correspond to n rows and n columns. Since there are a total of $n+1$ families of parallel lines and two are used to make the coordinate system, then there are $n-1$ Latin Squares we can construct using this method.

Why are these Latin Squares? In order to be a Latin Square, there must be no repeated entries in any row or in any column. Let $[N]$ be one the remaining $n-1$ families. Assume k appeared in two entries of the ith row, (i,j) and (i,j') of the Latin Square associated with $[N]$. Thus, $p_{(i,j)}$ lies on N_k and $p_{(i,j')}$ lies on N_k. As well, $p_{(i,j)}$ lies on L_i and M_j and $p_{(i,j')}$ lies on L_i and $M_{j'}$. Then $L_i = N_k$ by **A1**. Since N_k came from $[N]$ and not $[L]$, then this a contradiction. Thus, there are no repeated entries in any row. A similar argument can be shown that there are no repeated entries in any column. Hence, each of these $n-1$ tables are Latin Squares.

Are these Latin Squares pairwise orthogonal? Let $[N]$ and $[N']$ ($[N] \neq [N']$) be associated with two of the Latin Squares. Assume that the ordered pair (k,k') appeared in two of the entries (i,j) and (i',j') in the product of the two Latin Squares. Then $p_{(i,j)}$ and $p_{(i',j')}$ lie on N_k and $p_{(i,j)}$ and $p_{(i',j')}$ lie on $N'_{k'}$. Then $N_k = N'_{k'}$ by **A1**. Since these lines come from different families, this a contradiction. Thus, since there are no repeated entries in the product, each of the $n-1$ Latin Squares are pairwise orthogonal.

($\Leftarrow$) Given $n-1$ orthogonal n by n Latin Squares and we want to construct an affine plane of order n. First, we will define a geometry and then prove that it is an affine plane. Define the points in our geometry to be as follows

$$\begin{array}{cccc} (1,1) & (1,2) & \cdots & (1,n) \\ (2,1) & (2,2) & \cdots & (2,n) \\ & & \cdots & \\ (n,1) & (n,2) & \cdots & (n,n) \end{array}$$

Number each of the Latin Squares as LS_1, LS_2, ..., and LS_{n-1}. Define the lines in our geometry to be as follows

$$L_{-1,i} = \{(p,q) \mid p = i, 1 \leq q \leq n\}$$
$$L_{0,i} = \{(p,q) \mid q = i, 1 \leq p \leq n\}$$
$$L_{h,i} = \{(p,q) \mid (p,q) \text{ is a position in } LS_h \text{ labeled } i\}$$

Note that we now have n^2 points. Likewise, we have n $L_{-1,i}$ lines, n $L_{0,i}$ lines, and n lines for each of the $n-1$ Latin Squares. Thus, we have $n + n + n(n-1) = 2n + n^2 - n = n^2 + n$ lines. In this geometry, for two lines $L_{a,b}$ and $L_{c,d}$ to be parallel means that $a = c$. The reasoning is that distinct rows are disjoint and therefore each of the $L_{-1,i}$ lines are parallel. Similarly, distinct columns are disjoint and therefore each of the $L_{0,i}$ lines are parallel. Likewise, each of the $L_{h,i}$ lines are distinct. This is because if they were not distinct, consider $L_{h,k}$ and $L_{h,k'}$. In order for them to not be parallel, then in a k would have to be in the same entry as a k' in LS_h, which can't happen. Also note that every point in the plane is on one of these lines in each family. Clearly every point is in the $L_{-1,i}$ family and likewise every point is in the $L_{0,i}$ family. Since every number is being represented in one of the $L_{h,i}$'s for a given h, then every point is in these families as well.

To show that this geometry is an affine plane, it must satisfy the four axioms of an affine plane:

A1. Do two distinct points determine a unique line?

Given two distinct points, (a,b) and (c,d), first assume $a = c$. The line $L_{-1,a}$ goes through both of these points. None of the $L_{0,i}$ lines contain this point because in order for these points to be distinct, $b \neq d$ (if $a = c$). If one of the $L_{h,i}$ lines went through both of these points, then i is represented twice in the same row of LS_h by construction. Since this can't happen because LS_h is a

Latin Square, then none of the $L_{h,i}$ lines can go through these points.

Next, assume $a \neq c$ and $b = d$. The unique line through these two points is $L_{0,b}$. A similar argument can be shown here as to why this is the only line. However, in this case, i would be represented twice in the same column of LS_h.

Next, assume $a \neq c$ and $b \neq d$. Then none of the $L_{-1,i}$ lines nor the $L_{0,i}$ lines can pass through these points. Thus, one of the $L_{h,i}$ lines passes through these points. Assume there was another line $L_{h',i'}$ that also went through (a, b) and (c, d). Then, there was an i in the (a, b)th and (c, d)th positions of LS_h and likewise an i' in the (a, b)th and (c, d)th positions of $LS_{h'}$. If this was the case, then LS_h and $LS_{h'}$ would not be orthogonal because (i, i') would appear twice in the product. Thus, $L_{h,i}$ is the unique line through the two points.

A2. Does each line contain at least two points?

Since $n \geq 2$, then each $L_{-1,i}$ and $L_{0,i}$ has at least two points. As well, each $L_{h,i}$ has at least two points because in each LS_h, i would appear n times.

A3. Do there exist three non-collinear points?

We have three points $(1, 1), (1, 2)$, and $(2, 1)$ since $n \geq 2$. The line through $(1, 1)$ and $(1, 2)$ is $L_{-1,1}$ and $(2, 1)$ is not contained in $L_{-1,1}$. Thus, there are 3 non-collinear points.

P1. Does it satisfy the euclidean property?

First, are two lines from different families parallel? If the first line was $L_{-1,a}$, then every $L_{0,b}$ intersects with $L_{-1,a}$ at (a, b). Likewise, every $L_{h,i}$ intersects with this line because i appears in the ath row of LS_h. Similarly, if the first line was $L_{0,a}$, then every $L_{-1,b}$ intersects with $L_{0,a}$ at (b, a). Likewise, every

$L_{h,i}$ intersects with this line because i appears in the ath column of LS_h. If the first line was $L_{h,a}$, as just shown, this line can't be parallel to ant $L_{-1,i}$ line nor any $L_{0,i}$ line. So consider another line $L_{h',a'}$ $(h \neq h')$. If these two lines intersected, (a, a') must be in some position (r, s) of $LS_h \times LS_{h'}$. Since LS_h and $LS_{h'}$ are orthogonal, then (a, a') appears in $LS_h \times LS_{h'}$. Hence, they are not parallel. Therefore, two lines from different families cannot be parallel.

Given a line $L_{a,b}$ and a point p not on $L_{a,b}$, this point lies on one of the lines parallel to $L_{a,b}$ since each family partitions the points. Since none of the other families have lines that are parallel to $L_{a,b}$, then there is a unique line $L_{a,b'}$ through p that is parallel to $L_{a,b}$.

Since the geometry satisfies all four axioms on an affine plane, then an affine plane can be constructed given $n - 1$ orthogonal n by n Latin Squares. □

For an example of the constructions done in the first case, consider $\mathbb{F}_3$. As seen in Figure 12, the two families chosen are $[\langle 0, 0\rangle]$ and $[\langle 0\rangle]$. Following Figure 12 are the Latin Squares in this construction using the two remaining families $[\langle 1, 0\rangle]$ and $[\langle 2, 0\rangle]$ where the number each lines is associated with is b in $\langle m, b\rangle$.

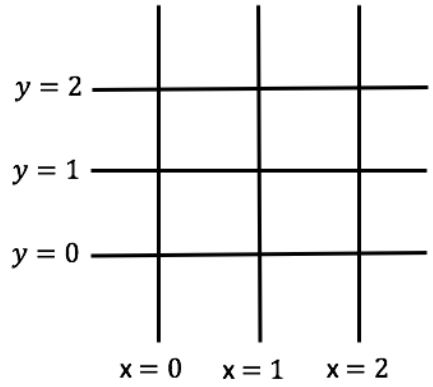

Figure 12: Construction of the Coordinate System in $\mathbb{F}_3$

$[\langle 2,0\rangle]$

0	1	2
1	2	0
2	0	1

$[\langle 1,0\rangle]$

0	2	1
1	0	2
2	1	0

As seen in the product below, these two Latin Squares are orthogonal because every element in $\mathbb{F}_3 \times \mathbb{F}_3$ is represented.

$$[\langle 2,0\rangle] \times [\langle 1,0\rangle] = \begin{array}{|c|c|c|} \hline (0,0) & (1,2) & (2,1) \\ \hline (1,1) & (2,0) & (0,2) \\ \hline (2,2) & (0,1) & (1,0) \\ \hline \end{array}$$

Likewise, to understand the $L_{h,i}$ lines in the second case, consider the Latin Square above over the family $LS_h = [\langle 2,0\rangle]$. The points incident to the lines in this family are

$$L_{h,0} = \{(1,1),(3,2),(2,3)\}$$

$$L_{h,1} = \{(1,2),(2,1),(3,3)\}$$

$$L_{h,2} = \{(3,1),(2,2),(1,3)\}$$

5.2 Projective Plane From A Perfect Difference Set

Definition 15: A perfect difference set is a set $S \subseteq \mathbb{Z}_m$ such that for $s_i, s_j \in S$, $\{s_i - s_j \mid i \neq j\} = \mathbb{Z}_m - \{0\}$. Furthermore, there differences are required to be unique in the following sense: if $s_i - s_j = s_{i'} - s_{j'}$, then $s_i = s_{i'}$ and $s_j = s_{j'}$.

As an example, consider the difference set $S = \{0,1,3\}$ as a subset of $\mathbb{Z}_7$. The differences would be,

$$3-0=3 \qquad 1-0=1 \qquad 0-1=-1\equiv 6$$

$$3-1=2 \qquad 1-3=-2\equiv 5 \qquad 0-3=-3\equiv 4$$

As illustrated, every nonzero element of $\mathbb{Z}_7$ is obtained by taking a difference of every distinct element in S.

By defining the cardinality of S to be $n+1$, the number of differences can be found using the cardinality. In taking the differences, you have $n+1$ choices for the first value and then n choices for the second value. So, there are $(n+1)\cdot n$ nonzero elements in $\mathbb{Z}_m$. Thus, $m = (n+1)\cdot n + 1 = n^2 + n + 1$ because of the inclusion of zero. Hopefully this number looks familiar, because in a projective plane there are n^2+n+1 points.

Definition 16: Given a perfect difference set S, a projective plane constructed from S denoted Proj(S) is formed by points $\mathbb{P} = \{p_0, p_1, \ldots, p_{n^2+n}\}$ and lines $\mathbb{L} = \{L_0, L_1, \ldots, L_{n^2+n}\}$ where p_i is incident to L_j if and only if $(i+j) \in S$.

Using the same example from above with $\mathbb{Z}_7$, $\mathbb{P} = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6\}$ and $\mathbb{L} = \{L_0, L_1, L_2, L_3, L_4, L_5, L_6\}$. An incidence table can be formed as seen in Figure 13 using the definition above. Given p_2, it is incident to lines L_1, L_5, and L_6 because $2+1=3$, $2+5=7\equiv 0 \pmod 7$, and $2+6=8\equiv 1 \pmod 7$. We can then look throughout the table and see the four axioms of a projective plane. Each pair of lines meet at unique points; between two distinct points, there exists a line through them; there are three non-collinear points; and each line has at least three points.

	p_0	p_1	p_2	p_3	p_4	p_5	p_6
L_0	×	×		×			
L_1	×		×				×
L_2		×				×	×
L_3	×				×	×	
L_4				×	×		×
L_5			×	×		×	
L_6		×	×		×		

Figure 13: Incidence Table for $\mathbb{Z}_7$ with difference set S

Note that this plane is also isomorphic to the Fano Plane first discussed. Freder-

ick W. Stevenson [10] calls these planes cyclic planes of order n generated by S due to the cyclic nature of the points in the incidence table.

THEOREM 9: If $|S| \geq 3$, Proj(S) is a projective plane.

Proof. The four axioms of a projective plane:

A1. Do two distinct points determine a unique line?

Given two distinct points, p_i and $p_{i'}$ $(i \neq i')$, there exists a unique $s, s' \in S$ such that $s - s' = i - i'$ since $i \neq i'$. Let $j = s - i$. Are these points incident to L_j? They are incident because $i + j = i + s - i = s$ which is an element of S and $i' + j = i' + s - i = s - (i - i') = s - (s - s') = s'$ which is an element of S.

To show this line is unique, assume there exists a line $L_{j'}$ such that p_i and $p_{i'}$ are incident to it. We know that $i + j \in S$ and $i' + j \in S$, but now $i + j' \in S$ and $i' + j' \in S$. Because S is a perfect difference set, differences of elements of S are unique. So, $(i + j') - (i' + j') = i - i'$ and $(i + j) - (i' + j) = i - i'$ implies that $i + j' = i + j$. Using subtraction, $j = j'$. Therefore the line between p_i and $p_{i'}$ is unique.

A2$^+$. Does each line contain at least three points?

$|S|$ is the same as the number of points on each line. So, since $|S| \geq 3$, there are at least three points on each line.

A3. Do there exist three non-collinear points?

Given three points p_0, p_1, and p_2, assume that there exists a line L_j such that all three points are incident to it. Thus, $0 + j \in S$, $1 + j \in S$, and $2 + j \in S$. Thus, since each of these elements are in S, their differences should result in a unique nonzero element of $\mathbb{Z}_{n^2+n+1}$. Hence, $(1 + j) - (0 + j) = 1$ and $(2 + j) - (1 + j) = 1$. This is a contradiction because the differences should be

distinct. Thus, there cannot exist a line L_j such that these three points are on it. Therefore, p_0, p_1, and p_2 are non-collinear.

P2. Does every pair of lines meet at some point?

Given two distinct lines, L_j and $L_{j'}$ ($j \neq j'$), there exists a unique $s, s' \in S$ such that $s - s' = j - j'$ since $j \neq j'$. Let $i = s - j$. Is p_i incident to these lines? It is incident because $i + j = s - j + j = s$ which is an element of S and $i + j' = s - j + j' = s - (j - j') = s - (s - s') = s'$ which is an element of S. Thus every pair of lines meet at some point.

Since Proj(S) satisfies all four axioms of a projective plane when $|S| \geq 3$, then it is a projective plane □

5.3 Affine Plane From Ternary Rings

DEFINITION 17: A ternary ring is a set of elements R and a mapping $t : R \times R \times R \to R$ satisfying the following properties:

T1. There exists $0, 1 \in R$ where $0 \neq 1$ and for all elements $a, b \in R$,

$$t(0, a, b) = t(a, 0, b) = b \qquad t(1, a, 0) = t(a, 1, 0) = a$$

T2. For all $a, b, c, d \in R$ ($a \neq c$), there exists a unique $x \in R$ such that $t(x, a, b) = t(x, c, d)$.

T3. For all $a, b, c \in R$, there exists a unique $x \in R$ such that $t(a, b, x) = c$.

T4. For all $a, b, c, d \in R$ ($a \neq c$), there exists a unique $(x, y) \in R \times R$ such that $t(a, x, y) = b$ and $t(c, x, y) = d$.

An example of a ternary ring is if R is a field under the function $t(p,q,r) = pq + r$. One can verify the four axioms to check that this is a ternary ring.

T1. If $1 \neq 0$, $t(0,q,r) = 0 \cdot q + r = r = q \cdot 0 + r = t(q,0,r)$
and $t(1,q,0) = 1 \cdot q + 0 = q = q \cdot 1 + 0 = t(q,1,0)$

T2. If $t(x,a,b) = xa + b \qquad t(x,c,d) = xc + d \qquad \Rightarrow \qquad x = (d-b)(a-c)^{-1}$ since this ring contains inverse elements.

T3. If $t(a,b,x) = ab + x = c \qquad \Rightarrow \qquad x = c - ab$

T4. If $t(a,x,y) = ax + y = b$ and $t(c,x,y) = cx + y = d$
$\Rightarrow \qquad x = (a-c)^{-1}(b-d) \qquad y = (a-c)^{-1}(da - cb)$

Definition 18 (Affine Plane over a Ternary Ring): Given a ternary ring R, the affine plane over R, denoted Aff(R) has points $\mathbb{P} = \{[x,y] | x, y \in R\}$ and lines $\mathbb{L} = \{\langle m,k\rangle \mid m,k \in R\} \cup \{\langle m\rangle \mid m \in R\}$ where

1. $[x,y]$ is incident to $\langle m,b\rangle$ if and only if $t(x,m,k) = y$
2. $[x,y]$ is incident to $\langle m\rangle$ if and only if $x = m$

Theorem 10: Aff(R) is an affine plane.

Proof. The four axioms of an affine plane:

A1. Do two distinct points determine a unique line?

Given two distinct points $[a,b]$ and $[c,d]$, first consider $a = c$. Hence, $b \neq d$ and both of these points are incident to $\langle a\rangle$. There can't be another line $\langle e\rangle$ ($a \neq e$) incident to both of these by construction. There cannot be a line $\langle m,k\rangle$ through these points because $t(a,m,k) = b$ and $t(a,m,k) = d$ yet $b \neq d$.

Next, assume $a \neq c$. Therefore, none of the $\langle m \rangle$ lines go through the two points. By **T4**, there exists a unique $(m, k) \in R \times R$ such that $t(a, m, k) = b$ and $t(c, m, k) = d$. Thus, the unique line through these points is $\langle m, k \rangle$.

A2. Does every line contain at least 2 points?

Given the line $\langle m, k \rangle$, the points $[0, k]$ and $[1, t(1, m, k)]$ are on this line. The former is because $t(0, m, k) = k$ by **T1**.

Given the line $\langle m \rangle$, the points $[m, 0]$ and $[m, 1]$ are on this line.

A3. Do there exist 3 non-collinear points?

There exists three points $[0, 0]$, $[1, 0]$, and $[0, 1]$. The line $\langle 0, 0 \rangle$ contains the points $[0, 0]$ and $[1, 0]$ because $t(0, 0, 0) = 0$ and $t(1, 0, 0) = 0$ by **T1**. However, $[0, 1]$ is not incident to $\langle 0, 0 \rangle$ because $t(0, 0, 0) \neq 1$ by **T1**. Thus, these three points are non-collinear.

P1. Does it satisfy the euclidean property?

Note that one can do a similar proof for Lemma 9 for ternary rings. The intersection points are different, however, but using the incidence relation for these ternary rings, one can find the intersection points.

Given a line $\langle m, k \rangle$ and a point $[x, y]$ not incident to $\langle m, k \rangle$. By Lemma 9, there is not a line $\langle m \rangle$ that is parallel to this line. So any line parallel to $\langle m, k \rangle$ must have the same m and a different k. Consider the line $\langle m, z \rangle$ $(z \neq k)$. By **T3**, there exists a unique $z \in R$ such that $t(x, m, z) = y$. Therefore, this line is the only line through $[x, y]$ and parallel to $\langle m, k \rangle$.

Given a line $\langle m \rangle$ and a point $[x, y]$ not incident to $\langle m \rangle$, i.e., $m \neq x$. By Lemma 9, there is not a line $\langle m, k \rangle$ that is parallel to this line. Consider the line $\langle x \rangle$. The point $[x, y]$ is incident to this line and since $m \neq x$, then it is parallel to $\langle m \rangle$.

Since Aff(R) satisfies all four axioms of an affine plane, then it is an affine plane.

□

Using the field considered above, an affine plane can be made using this construction. This is a result we would hope would happen given that we have already shown that an affine plane can be constructed using a field.

5.4 Projective Plane Not Constructed From A Field

DEFINITION 19: A near-field is a set N with two binary operations $\oplus$ and $*$ satisfying the following axioms:

Q1. $(N, \oplus)$ is an abelian group.

Q2. For all $a, b, c \in N$, $(a * b) * c = a * (b * c)$.

Q3. For all $a, b, c \in N$, the operation is right distributive, i.e. $(a \oplus b) * c = a * c \oplus b * c$.

Q4. There exists a multiplicative identity $1 \in N$ such that for all $a \in N$, $a * 1 = 1 * a = a$.

Q5. For all nonzero elements a of N, there exists a multiplicative inverse $a^{-1} \in N$ such that $a * a^{-1} = a^{-1} * a = 1$.

Note that every field is a near field but not every near field is a field.

G. Pilz [5] gives an example of a near-field that is not a field. Consider a field of order p^2 where p is an odd prime under the normal addition $+$ and multiplication $*$. Let Q be the field of order p^2, $\mathbb{F}_{p^2}$, where addition is the same as in the field but multiplication $\otimes$ is defined as

$$a \otimes b = a * b \text{ if } b \in (\mathbb{F}_{p^2})^2 \qquad \text{and} \qquad a \otimes b = a^p * b \text{ if } b \notin (\mathbb{F}_{p^2})^2$$

where $a, b \in Q$ (i.e., b is either a square or not a square).

LEMMA 12: In a finite field F, (1) A square times a square is a square. (2) A square times a non-square is a non-square. (3) A non-square times a non-square is a square.

Proof. Recall that in a finite field F, the nonzero elements form a cyclic group, i.e. for all $f \in F$ ($f \neq 0$), $f = x^{\alpha}$ for some element $x \in F$ and integer power α.

First, we claim that if x^k is a square, then k is even and if x^k is a non-square, then k is odd. If $a = x^k$ is a square, then $a = y^2$ for some $y \in F$. Since F is cyclic, $y^2 = (x^m)^2 = x^{2m}$. Therefore, $k = 2m$ and thus k is even. Next, through the contrapositive of the second statement, we want to show that if k is even, then x^k is a square. Note that for any element $t \in F$, $t^{2w} = (t^w)^2$ is always a square. Therefore, if x^k is a non-square, then k is odd.

(1) Given two squares $a = p^2$ and $b = q^2$, the product $ab = p^2q^2 = (pq)^2$ is also a square. (2) Given a square $a = x^m$ and a non-square $b = x^n$, then m is even and n is odd. Thus, the product, $ab = x^m x^n = x^m + n$ is a non-square since $m + n$ is odd. (3) Given two non-squares, $a = x^m$ and $b = x^n$, then m and n are both odd. Thus, the product $ab = x^m x^n = x^m + n$ is a square since $m + n$ is even. □

THEOREM 11: Q is a near-field.

Proof. In order for Q to be a near-field, it must satisfy the five axioms.

Q1. $(Q, +)$ is an abelian group since addition did not change and the set of elements are from a field.

Q2. Is $\otimes$ associative?

Let $a, b, c \in Q$. Since the first element is not affected by our new multiplication, it does not matter whether or not a is a square. Hence, first assume that b and c are both squares,

$$a \otimes (b \otimes c) = a \otimes (b * c) = a * (b * c)$$

This used Lemma 12 since $b * c$ is a square. Now, since $*$ is associative,

$$a * (b * c) = (a * b) * c = (a * b) \otimes c = (a \otimes b) \otimes c$$

since c is a square.

Next, assume that b is a square and c is not,

$$a \otimes (b \otimes c) = a \otimes (b^p * c)$$

Since b is a square, b^p is also a square and thus by Lemma 12, $b^p * c$ is not a square. Therefore,

$$a \otimes (b^p * c) = a^p * (b^p \times c) = (a^p * b^p) \times c = (a * b)^p * c$$

We can do this since $*$ is an operation under a field, which means that it is commutative. Now since c is not a square and b is,

$$(a * b)^p * c = (a * b) \otimes c = (a \otimes b) \otimes c$$

Third, assume that c is a square and b is not,

$$a \otimes (b \otimes c) = a \otimes (b * c) = a^p * (b * c)$$

since $b * c$ is not a square by Lemma 12. Now by the associativity of $*$,

$$a^p * (b * c) = (a^p * b) * c = (a^p * b) \otimes c = (a \otimes b) \otimes c$$

Finally, assume that both b and c are not squares. Recall that in a finite group of order n, for all nonzero elements x, $x^n = x$. Beginning with the other side

first in this case,

$$(a \otimes b) \otimes c = (a^p * b) \otimes c = (a^p * b)^p * c = (a^{p^2} * b^p) * c$$

Using the fact above, since $a^{p^2} = a$,

$$(a^{p^2} * b^p) * c = (a * b^p) * c = a * (b^p * c)$$

Since $b^p * c$ is a square by Lemma 12,

$$a * (b^p * c) = a \otimes (b^p * c) = a \otimes (b \otimes c)$$

By looking at the extremes in all cases, $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ and thus $\otimes$ is associative.

Q3. Is the operation right distributive?

Let $a, b, c \in Q$. First, assume that c is a square. Recall that $\times$ is already right distributive.

$$(a + b) \otimes c = (a + b) * c = a * c + b * c = a \otimes c + b \otimes c$$

Next, assume that c is not a square. Recall the "Freshman's Dream" which states that in a finite field of order n, $(x + y)^n = x^n + y^n$.

$$(a + b) \otimes c = (a + b)^p * c = (a^p + b^p) * c = a^p * c + b^p * c = a \otimes c + b \otimes c$$

Thus the operation is right distributive.

Q4. Does there exist a multiplicative identity?

Since the elements of Q come from elements in a field, then $1 \in Q$. Is 1 a multiplicative identity?

$$1 \otimes a = 1 * a = a \text{ (if } a \text{ is a square)}$$
$$1 \otimes a = 1^p * a = 1 * a = 1 \text{ (if } a \text{ is not a square)}$$
$$a \otimes 1 = a \otimes 1 = a$$

Therefore, 1 is a multiplicative identity.

Q5. For each element, does there exist a multiplicative inverse?

Given a nonzero element $a \in Q$, first assume that a is a square. Then, the multiplicative inverse is $a^{-1} = \frac{1}{a}$ (which exists since a is an element of a field). Since a is a square, then so is $\frac{1}{a}$. Thus,

$$a \otimes \frac{1}{a} = a * \frac{1}{a} = 1$$
$$\frac{1}{a} \otimes a = \frac{1}{a} * a = 1$$

Next, assume a is not a square. Then, the multiplicative inverse is $a^{-1} = \frac{1}{a^p}$.

$$a \otimes \frac{1}{a^p} = a^p * \frac{1}{a^p} = 1$$
$$\frac{1}{a^p} \otimes a = \left(\frac{1}{a^p}\right)^p * a = \frac{1}{a^{p^2}} * a = \frac{1}{a} * a = 1$$

This recalls the fact that $a^{p^2} = a$. Thus, there is a multiplicative inverse for each nonzero element in Q.

Since Q satisfies all five axioms of a near-field, then Q is a near-field. □

LEMMA 13: Q is a ternary ring under the operation $t(a, b, c) = a \otimes b + c$.

Proof. In order for Q to be a ternary ring, it must satisfy the four axioms of a ternary

ring.

T1. Are there elements 0 and 1 such that $0 \neq 1$ and satisfy the equations?

There are elements 0 and 1 in Q such that $0 \neq 1$ and, if a is a non-square, then

$$\begin{aligned} t(0,a,b) =& 0 \otimes a + b = 0 * a + b = 0 + b = b \\ t(a,0,b) =& a \otimes 0 + b = a * 0 + b = 0 + b = b \\ t(1,a,0) =& 1 \otimes a + 0 = 1 * a + 0 = a + 0 = a \\ t(a,1,0) =& a \otimes 1 + 0 = a * 1 + 0 = a + 0 = a \end{aligned}$$

Likewise, if a is a non-square, then

$$\begin{aligned} t(0,a,b) =& 0 \otimes a + b = 0^p * a + b = 0 * a + b = 0 + b = b \\ t(a,0,b) =& a \otimes 0 + b = a * 0 + b = 0 + b = b \\ t(1,a,0) =& 1 \otimes a + 0 = 1^p * a + 0 = 1 * a + 0 = a + 0 = a \\ t(a,1,0) =& a \otimes 1 + 0 = a * 1 + 0 = a + 0 = a \end{aligned}$$

T2. Does there exist a unique $x \in Q$ such that $t(x,a,b) = t(x,c,d)$ for all $a,b,c,d \in Q$?

If a and c are both squares, let $x = (d-b) * (a-c)^{-1}$. Then,

$$\begin{aligned} t(x,a,b) =& x \otimes a + b = (d-b) * (a-c)^{-1} * a + b \\ =& [a * (d-b) + b * (a-c)] * (a-c)^{-1} \end{aligned}$$

$$=[a*d-a*b+b*a-c*b]*(a-c)^{-1}=[a*d+c*b]*(a-c)^{-1}$$

$$=[a*d-c*d+c*d-c*b]*(a-c)^{-1}$$

$$=[d*(a-c)+c(b-d)]*(a-c)^{-1}$$

$$=(d-b)*(a-c)^{-1}*c+d=x\otimes c+d=t(x,c,d)$$

If a and c are both non-squares, let $x=(d-b)^p*(a-c)^{-p}$. Then,

$$t(x,a,b)=x\otimes a+b=[(d-b)^p*(a-c)^{-p}]^p*a+b$$

$$=(d-b)^{p^2}*(a-c)^{-p^2}*a+b=(d^{p^2}-b^{p^2})*(a-c)^{-p^2}*a+b$$

$$=[a*(d^{p^2}-b^{p^2})+b*(a^{p^2}-c^{p^2})]*(a-c)^{-p^2}$$

$$=[a*d^{p^2}-a*^{p^2}+b*a^{p^2}-b*c^{p^2}]*(a-c)^{-p^2}$$

$$=[a*d^{p^2}-b*c^{p^2}]*(a-c)^{-p^2}$$

$$=[a*d^{p^2}-c*d^{p^2}+c*d^{p^2}-b*c^{p^2}]*(a-c)^{-p^2}$$

$$=[d^{p^2}*(a-c)+c^{p^2}*(d-b)]*(a-c)^{-p^2}$$

$$=[d^{p^2}*(a-c)^{p^2}+c^{p^2}*(d-b)]*(a-c)^{-p^2}$$

$$=d^{p^2}+c^{p^2}*(d-b)*(a-c)^{-p^2}$$

$$=d+c*(d-b)*(a-c)^{-p^2}=d+(a-c)^{-p^2}*c$$

$$=d+x\otimes c=t(x,c,d)$$

For the last case, without loss of generality assume a is a square and c is not. We can define a function $\phi:\mathbb{F}_{p^2}\to\mathbb{F}_{p^2}$ by $\phi(x)=x^p*c-x*a$. To show that ϕ is a bijection, it is enough to show that it is injective since $\mathbb{F}_{p^2}$ is finite. To

show ϕ is injective, assume $f(x) = f(y)$ for $x, y \in \mathbb{F}_{p^2}$. Therefore,

$$\begin{aligned} x^p * c - x * a &= y^p * c - y * a \\ c * (x^p - y^p) &= a(x - y) \\ c * (x - y)^p &= a * (x - y) \end{aligned}$$

If to the contrary we assume that $x \neq y$, then we conclude that

$$c * (x - y)^{p-1} = a$$

Since p is an odd prime, then $p-1$ is even so $(x-y)^{p-1}$ is a square. Therefore, since c is not a square, the product of c and $(x - y)^{p-1}$ is not a square by Lemma 12. However, a is a square. Hence, it can't be that $x \neq y$ and so $x = y$. Thus ϕ is injective. This means that there exists a unique solution where $x^p * c - x * a = b - d$ for $b - d \in \mathbb{F}_{p^2}$. Thus, there is a unique solution where $x * a + b = x^p * c + d$ which is $x \otimes a + b = x \otimes c + d$. Hence, there exists a unique $x \in Q$ such that $t(x, a, b) = t(x, c, d)$.

T3. Does there exist a unique $x \in Q$ such that $t(a, b, x) = c$ for all $a, b, c \in Q$?

Let $x = c + (-a \otimes b)$ where $-a \otimes b$ is the additive inverse of $a \otimes b$. Since addition is commutative, then $t(a, b, x) = a \otimes b + c + (-a \otimes b) = 0 + c = c$.

T4. Does there exist a unique $(x, y) \in Q \times Q$ such that $t(a, x, y) = b$ and $t(c, x, y) = d$ for all $a, b, c, d \in Q$?

Consider $(a - c)^{-1} * (b - d)$. If this is a square, then let $x = (a - c)^{-1} * (b - d)$ and $y = b - a \otimes x$. Thus,

$$
\begin{aligned}
t(a,x,y) =& a \otimes x + y = a \otimes x + b - a \otimes x \\
=& 0 + b = b \\
t(c,x,y) =& c \otimes x + y = c \otimes x + b - a \otimes x \\
=& c * (a-c)^{-1} * (b-d) + b - a * (a-c)^{-1} * (b-d) \\
=& [c * (b-d) + b * (a-c) - a * (b-d)] * (a-c)^{-1} \\
=& [c * b - c * d + b * a - b * c - a * b + a * d] * (a-c)^{-1} \\
=& [a * d - c * d] * (a-c)^{-1} \\
=& d * (a-c) * (a-c)^{-1} = d
\end{aligned}
$$

If $(a-c)^{-1} * (b-d)$ is a non-square, then let $x = (a^p - c^p)^{-1} * (b-d)$ and $y = b - a \otimes x$. Therefore by Lemma 12, $x = (a-c)^{-p} * (b-d) = (a-c)^{-(p-1)} * (a-c)^{-1} * (b-d)$ is not a square since $(a-c)^{-(p-1)}$ is a square because p is odd. Thus,

$$
\begin{aligned}
t(a,x,y) =& a \otimes x + y = a \otimes x + b - a \otimes x \\
=& 0 + b = b \\
t(c,x,y) =& c \otimes x + y = c \otimes x + b - a \otimes x \\
=& c^p * (a^p - c^p)^{-1} * (b-d) + b - a^p (a^p - c^p)^{-1} * (b-d) \\
=& [c^p * (b-d) + b(a^p - c^p) - a^p (b-d)] * (a^p - c^p)^{-1} \\
=& [c^p * b - c^p * d + b * a^p - b * c^p - a^p * b + a^p * d] * (a^p - c^p)^{-1} \\
=& [a^p * d - c^p * d] * (a^p - c^p)^{-1} \\
=& d * (a^p - c^p) * (a^p - c^p)^{-1} = d
\end{aligned}
$$

Since Q satisfies the four properties of a ternary ring, then it is a ternary ring. $\square$

Since Q is a ternary ring, then by Theorem 10, $A = \text{Aff}(Q)$ is an affine plane. As well, by Theorem 6, $\text{Proj}(A)$ is a projective plane.

BRUCK-RYSER THEOREM

To motivate Lemma 14, consider the determinant of this 2 by 2 matrix,

$$\det \begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix} = a - 1 = (a-1)^{2-1}$$

Likewise, consider the determinant of this 3 by 3 matrix. Since the determinant is preserved through row operations, subtracting the second row from the first row results,

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix} = \det \begin{pmatrix} 0 & 1-a & 0 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix}$$

Using cofactor expansion along the first row,

$$\det \begin{pmatrix} 0 & 1-a & 0 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix} = 0 \cdot \det \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix} - (1-a) \cdot \det \begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix} + 0 \cdot \det \begin{pmatrix} 1 & a \\ 1 & 1 \end{pmatrix}$$

$$= -(1-a) \det \begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix} = (a-1)(a-1) = (a-1)^{3-1}$$

LEMMA 14: For a given k by k matrix,

$$\det(A_k) = \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ 1 & 1 & a & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix} = (a-1)^{k-1}$$

Proof. We will induct on k. When $k = 1$,

$$\det(A_1) = \det(1) = 1 = (a-1)^0$$

By induction, assume this holds for any $(k-1)$ by $(k-1)$ matrix, i.e. $\det(A_{k-1}) = (a-1)^{(k-1)-1} = (a-1)^{k-2}$. Since determinants are preserved under row operations, subtracting the second row from the first row on A_k results,

$$\det(A_k) = \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ 1 & 1 & a & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix} = \det \begin{pmatrix} 0 & 1-a & 0 & \cdots & 0 \\ 1 & a & 1 & \cdots & 1 \\ 1 & 1 & a & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix}$$

Using cofactor expansion along the first row,

$$\det A_k = 0 \cdot \det(M_1) - (a-1)\det(M_2) + 0 \cdot \det(M_3) - \ldots \pm 0 \cdot \det(M_k)$$

$$= -(1-a)\det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix}$$

where each M_i is the matrix obtained from the new A_k by deleting the first row and the ith column. Therefore,

$$\det(A_k) = (a-1)\det(A_{k-1}) = (a-1)(a-1)^{k-2} = (a-1)^{k-1}$$

□

Again to motivate Lemma 15, consider the determinant of this 2 by 2 matrix,

$$\det \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix} = a^2 - 1 = (a-1)(a+1) = (a-1)^{2-1}(a+2-1)$$

Likewise, consider the determinant of this 3 by 3 matrix. Since the determinant is preserved through row operations, subtracting the second row from the first row results,

$$\det \begin{pmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix} = \det \begin{pmatrix} a-1 & 1-a & 0 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix}$$

Using cofactor expansion along the first row,

$$\det \begin{pmatrix} a-1 & 1-a & 0 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix} = (a-1)\det \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix} - (1-a)\begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix} + 0 \begin{pmatrix} 1 & a \\ 1 & 1 \end{pmatrix}$$

$$= (a-1)(a^2-1) + (a-1)(a-1) = (a-1)^2(a+1) + (a-1)^2 = (a-1)^2(a+1+1)$$

$$= (a-1)^{3-1}(a+3-1)$$

Lemma 15: For a given k by k matrix,

$$\det(B_k) = \det \begin{pmatrix} a & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ 1 & 1 & a & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix} = (a-1)^{k-1}(a+k-1)$$

Proof. We will induct on k. When $k = 1$,

$$\det(B_1) = \det(a) = a = (a-1)^0(a+1-1)$$

By induction, assume this holds for any $(k-1)$ by $(k-1)$ matrix, i.e., $\det(B_{k-1}) = (a-1)^{(k-1)-1}(a+(k-1)-1) = (a-1)^{k-2}(a+k-2)$. Since determinants are preserved under row operations, subtracting the second row from the first row on B_k results,

$$\det(B_k) = \det\begin{pmatrix} a & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ 1 & 1 & a & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix} = \det\begin{pmatrix} a-1 & 1-a & 0 & \cdots & 0 \\ 1 & a & 1 & \cdots & 1 \\ 1 & 1 & a & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix}$$

Using cofactor expansion along the first row,

$$\det(B_k) = (a-1)\det(N_1) - (1-a)\det(N_2) + 0 \cdot \det(N_3) - \ldots \pm 0 \cdot \det(N_k)$$

$$= (a-1)\det\begin{pmatrix} a & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix} + (a-1)\det\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & 1 & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & a \end{pmatrix}$$

where each N_i is the matrix obtained from the new B_k by deleting the first row and the ith column. By Lemma 14 this results,

$$\det(B_k) = (a-1)\det(B_{k-1}) + (a-1)\det(A_{k-1})$$

$$= (a-1)(a-1)^{k-2}(a+k-2) + (a-1)(a-1)^{k-2} = (a-1)^{k-1}(a+k-2) + (a-1)^{k-1}$$

$$= (a-1)^{k-1}(a+k-2+1) = (a-1)^{k-1}(a+k-1)$$

□

PROPOSITION 4: The determinant of an incidence matrix A for a projective plane of order n is $\det(A) = n^{\frac{1}{2}n(n+1)}(n+1)$.

Proof. Define the matrix A to be an incidence matrix for a projective plane, P. Note that A is an (n^2+n+1) by (n^2+n+1) matrix. Recall that an incidence matrix has the rows (or columns) as points and the other as lines. A one indicates that a point is incident to the corresponding line and a zero indicates that the point is not incident to that line. The transpose of A is simply where the rows of A are now the columns and likewise the columns are now the rows. When computing the dot product of A and A^T,

$$AA^T = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ & \dots & & \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & \dots & a_{r1} \\ a_{12} & a_{22} & \dots & a_{r2} \\ & \dots & & \\ a_{1r} & a_{2r} & \dots & a_{rr} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{21} & \dots & b_{r1} \\ b_{12} & b_{22} & \dots & b_{r2} \\ & \dots & & \\ b_{1r} & b_{2r} & \dots & b_{rr} \end{pmatrix}$$

where each b_{ij} is computed by multiplying the ith row of A with the jth column of A^T and $r = n^2 + n + 1$. In each of the diagonal entries, b_{ii} is taking the ith row of A and doing the product of that row with itself. In terms of what A is defined as, since it is only ones and zeros, the dot product of each row multiplied by itself will simply be however many ones are in the row. For example, given the row $(1, 1, 0, 1)$, the dot product of the row with itself is

$$(1, 1, 0, 1) \cdot (1, 1, 0, 1) = (1 \cdot 1) + (1 \cdot 1) + (0 \cdot 0) + (1 \cdot 1) = 3$$

Thus, since each row in an incidence matrix is the number of points on a line (or lines through a given point), the number of ones in that row will be $n + 1$. As for the other entries, the dot product between two vectors of ones and zeros will

be the number of times that a one appears in the same entry of both vectors. For example, given the vectors $(1,1,1,0)$ and $(0,1,1,0)$, the dot product is

$$(1,1,1,0)\cdot(0,1,1,0) = (1\cdot 0)+(1\cdot 1)+(1\cdot 1)+(0\cdot 0) = 2$$

Thus, the dot product in AA^T will be taking a row in A times a column in A^T (which is basically a row in A times another row in A). So, how many times do two rows (lines) have a one in the same entry (cross through the same point) in a projective plane? Since every pair of lines meet at a unique point, there would only be one entry in each row of A that has a one in both rows. Thus,

$$AA^T = \begin{pmatrix} n+1 & 1 & 1 & \cdots & 1 \\ 1 & n+1 & 1 & \cdots & 1 \\ 1 & 1 & n+1 & \cdots & 1 \\ & & \cdots & & \\ 1 & 1 & 1 & \cdots & n+1 \end{pmatrix}$$

From Lemma 15, $\det(AA^T) = [(n+1)-1]^{r-1}[(n+1)+r-1] = n^{r-1}(n+r)$. Since r is the size of the matrix and the size correlates to the number of points (or lines) in the plane,

$$\begin{aligned} \det(AA^T) &= n^{r-1}(n+r) \\ &= n^{n^2+n+1-1}(n+n^2+n+1) \\ &= n^{n^2+n}(n^2+2n+1) \\ &= n^{n(n+1)}(n+1)^2 \end{aligned}$$

Since $\det(AA^T) = [\det(A)]^2$,

$$\det(A) = \pm n^{\frac{1}{2}n(n+1)}(n+1)$$

Hence because the determinant is either positive or negative, we can assume without loss of generality that it is positive. If it were negative, we can switch around the order of two of the rows. By transposing the rows, the sign of the determinant changes to positive. Therefore, $\det(A) = n^{\frac{1}{2}n(n+1)}(n+1)$. □

THEOREM 12: If $n = p^k$ where p is prime and k is a non-negative integer, then there exists a projective plane of order n.

Proof. Since every finite field has $n = p^k$ elements, then there we can construct an affine plane $\mathbb{A}^2_{\mathbb{F}}$ from this field. Next, construct Proj($\mathbb{A}^2_{\mathbb{F}}$). Thus, there exists a projective plane with order p^k. □

The following lemmas and theorems stated below are needed in order to prove the Bruck-Ryser Theorem. The proofs for these, however, are not included in this paper.

LEMMA 16 (The Four-Squares Identity): If $b_1, b_2, b_3, b_4, x_1, x_2, x_3, x_4 \in \mathbb{Z}$, then $(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = (y_1^2 + y_2^2 + y_3^2 + y_4^2)$ where

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = B \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \qquad \text{with} \qquad B = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ -b_2 & b_1 & -b_4 & b_3 \\ -b_3 & b_4 & b_1 & -b_2 \\ -b_4 & -b_3 & b_2 & b_1 \end{pmatrix}$$

and $\det(B) = (b_1^2 + b_2^2 + b_3^2 + b_4^2)^2$ which means that B is invertible.

THEOREM 13 (Lagrange [7]): Any positive integer can be written as the sum of four squares.

LEMMA 17 (Rational Sum of Two Squares [3]): For any integer n, if the equation $x^2 + y^2 = nz^2$ has an integer solution with x, y, z not all zero, then n is the sum of two squares.

THEOREM 14 (Bruck-Ryser Theorem [3]): If $n \equiv 1$ or 2 (mod 4) and $n \neq a^2 + b^2$, then there is no projective plane of order n.

Proof. Let A be an incidence matrix for a projective plane of order n where $n \equiv 1$ or 2 (mod 4) and $n \neq a^2 + b^2$. Let $N = n^2 + n + 1$. In our assumption, $n \equiv 1$ or 2 (mod 4) and thus, $N \equiv 3$ (mod 4).

Consider the vector $\overrightarrow{x} = (x_1, x_2, \ldots, x_N)^T \in \mathbb{Q}^N$. Define $\overrightarrow{z} = A\overrightarrow{x} = (z_1, z_2, \ldots, z_N)^T$. Therefore,

$$\overrightarrow{z}^T\overrightarrow{z} = (z_1, z_2, \ldots, z_N)\begin{pmatrix} z_1 \\ \ldots \\ z_N \end{pmatrix} = z_1^2 + z_2^2 + \ldots + z_N^2$$

As well, $\overrightarrow{z}^T\overrightarrow{z} = (A\overrightarrow{x})^T(A\overrightarrow{x}) = \overrightarrow{x}^T A^T A\overrightarrow{x}$. Now, since we know what AA^T looks like from Proposition 4, this is the same as $\overrightarrow{x}^T(J + nI)\overrightarrow{x}$ where J is the N by N matrix of all ones. So,

$$\begin{aligned}
\overrightarrow{x}^T(J + nI)\overrightarrow{x} =& \overrightarrow{x}^T J\overrightarrow{x} + \overrightarrow{x}^T nI\overrightarrow{x} \\
=& \overrightarrow{x}^T J\overrightarrow{x} + n\overrightarrow{x}^T\overrightarrow{x} \\
=& \overrightarrow{x}^T J\overrightarrow{x} + n(x_1^2 + x_2^2 + \ldots + x_N^2) \\
=& (x_1, x_2, \ldots, x_N)\begin{pmatrix} x_1 + x_2 + \ldots + x_N \\ \ldots \\ x_1 + x_2 + \ldots + x_N \end{pmatrix} + n(x_1^2 + x_2^2 + \ldots + x_N^2) \\
=& (x_1 + x_2 + \ldots + x_N)^2 + n(x_1^2 + x_2^2 + \ldots + x_N^2)
\end{aligned}$$

Let $\omega = x_1 + x_2 + \ldots + x_N$. Since we now have two results for $\overrightarrow{z}^T\overrightarrow{z}$, then the results

are equal. And therefore,

$$z_1^2 + z_2^2 + \ldots + z_N^2 = \omega^2 + n(x_1^2 + x_2^2 + \ldots + x_N^2)$$

Since $N \equiv 3 \pmod 4$, we will add an nx_{N+1}^2 term on both sides so that the number of x_i's is congruent to 0 (mod 4),

$$z_1^2 + z_2^2 + \ldots + z_N^2 + nx_{N+1}^2 = \omega^2 + n(x_1^2 + x_2^2 + \ldots + x_N^2 + x_{N+1}^2)$$

By Theorem 13, every non-negative integer can be written as the sum of four squares, i.e. $n = a^2 + b^2 + c^2 + d^2$. Now because of Lemma 16, $(a^2 + b^2 + c^2 + d^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2$. Therefore, since n can be written as the sum of four squares and we can group our x_i's into groups of four, a group of four nx_i's will now be written as a group of four y_i's. In other words,

$$z_1^2 + z_2^2 + \ldots + z_N^2 + nx_{N+1}^2 = \omega^2 + y_1^2 + y_2^2 + \ldots + y_N^2 + y_{N+1}^2 \tag{1}$$

Now, since the matrix B from Lemma 16 is invertible and has integer coefficients, we can write each of the x_i's as a rational linear combination of the y_i's and therefore each of the z_i's can be written as a linear combination of the y_i's with rational coefficients.

Now, since each z_i is a linear combination of the y_i's with rational coefficients, $z_1 = c_{11}y_1 + c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1}$ with $c_{ij} \in \mathbb{Q}$. If $c_{11} \neq 1$, then we can set $y_1 = \frac{1}{1-c_{11}}(c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1})$ which would mean that

$$z_1 = \frac{c_{11}}{1 - c_{11}}(c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1}) + c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1} = y_1$$

If $c_{11} = 1$, then we can set $y_1 = -\frac{1}{2}(c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1})$ which would mean

that

$$z_1 = -\frac{1}{2}(c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1}) + c_{12}y_2 + \ldots + c_{1(N+1)}y_{N+1} = -y_1$$

But regardless of what c_{11} is, $y_1^2 = z_1^2$ and y_1 is written in terms of the other y_i's. Thus, we can subtract y_1^2 off of each side in (1). We can continue this process on each y_i $(1 \leq i \leq N)$ such that $y_i^2 = z_i^2$ and y_i is written as a linear combination of $y_{i+1}, \ldots, y_{N+1}$. Therefore, (1) is now reduced to

$$nx_{N+1}^2 = \omega^2 + y_{N+1}^2 \tag{2}$$

Since each x_i is a linear combination of the y_i's, then x_{N+1} and ω are linear combinations of the y_i's. However, each y_i $(1 \leq i \leq N)$ was rewritten as a linear combination of $y_{i+1}, \ldots, y_N$, and y_{N+1}. Therefore, x_{N+1} and ω are a linear combination of y_{N+1}, i.e. $x_{N+1} = ky_{N+1}$ and $\omega = ly_{N+1}$ where k and l are rational coefficients. Hence, (2) is now

$$nk^2y_{N+1}^2 = l^2y_{N+1}^2 + y_{N+1}^2$$

We can choose y_{N+1} to be the least common multiple of the denominators of k and l so that each term has integer coefficients that are squares. Thus, n is a sum of two squares by Lemma 17. This is a contradiction since our initial assumption was that $n \neq a^2 + b^2$. Therefore, a projective plane of order n cannot exist. □

As an application of Bruck-Ryser, a projective plane cannot have order $n = 6$ because $6 \equiv 2 \pmod 4$ and 6 can not be written as a sum of squares. Likewise, there cannot exist a projective plane of order $n = 14$.

CONCLUSION

Throughout this paper we have examined basic properties of affine and projective geometries. We constructed a projective plane given an affine plane and made an affine plane given a projective plane. We took fields and made both affine and projective geometries. We produced affine planes using $n-1$ pairwise orthogonal Latin Squares. We constructed projective planes using Perfect Difference Sets. As well, we made affine and projective planes using ternary rings and a near-field.

In conclusion, we have shown that the order of finite projective planes n can be a power of a prime and it can't be equivalent to 1 or 2 (mod 4) while $n \neq a^2 + b^2$. For ease, Figure 14 begins a list of orders that projective planes can be or not be along with the reason why.

n	Possible Projective Plane?	Reason
1	Not possible	violates $\mathbf{A2}^+$
2	Possible	2 is prime, Fano Plane
3	Possible	3 is prime
4	Possible	Theorem 12
5	Possible	5 is prime
6	Not possible	Bruck-Ryser Theorem
7	Possible	7 is prime
8	Possible	Theorem 12
9	Possible	Theorem 12, 4 known planes up to isomorphism
10	Not possible (computer)	See next paragraph
11	Possible	11 is prime
12	?	?
13	Possible	13 is prime
14	Not possible	Bruck-Ryser Theorem

Figure 14: Possible Projective Planes of Order n

A big question in finite projective geometry is how many planes of order n are there (up to isomorphism)? There may be more than one plane up to isomorphism. For example, there are at least four non-isomorphic projective planes of order 9

[10]. There may be more but there are currently only four known. Another question is about projective planes of prime order p and whether or not there is more than one.

Another big question in finite projective geometry is what the order of a plane can be. Theorems 12 and 14 produce several questions. Can the order only be a power of a prime? If n fails to satisfy the restrictions placed by the Bruck-Ryser Theorem, will there always be a projective plane? We believe that the general consensus is that the answer is somewhere in the middle of these two extremes. In the last decades of the twentieth century, C.W. H. Lam [4] ran a computer simulation that apparently proved that a projective plane of order 10 is not possible. However, computers do make errors and an actual proof has not been given yet. The next integer which is yet to be shown whether or not it can be the order of a projective plane is $n = 12$. There is no known proof whether or not $n = 12$ can be an order of a projective plane. For this reason, using Latin Squares, Ternary Rings, and Perfect Difference Sets are an important topic in projective geometry. If we can find one of these sets has an order that is not a power of a prime, then we know that we can make a projective plane of this given order. Determining which orders are possible for projective planes is one of the great unsolved problems in combinatorics.

REFERENCES

[1] Carl B. Boyer, A History of Mathematics, John Wiley & Sons, Inc., 1968, 367-597.

[2] H. S. M. Coxeter, The Real Projective Plane Edition 2, Cambridge University Press, 1955, 1-10.

[3] Kahrstrom, Johan, On Projective Planes,
Mid Sweden University, 2002, Available at
http://kahrstrom.com/mathematics/documents/OnProjectivePlanes.pdf.

[4] C.W. H. Lam, The Search for a Finite Projective Plane of Order 10, American Mathematics Monthly 98 (1991), 305-318.

[5] G. Pilz, Near-Rings, North-Holland, Amsterdam, 1977, 257.

[6] Abraham Seidenberg, Lectures in Projective Geometry, D. Van Nostrand Company, Inc., 1962, 1-68.

[7] Sierpinski, Waclaw, Elementary Theory of Numbers, Poland, 1964, 368.

[8] James M. Smart, Modern Geometries Edition 3, Brooks/Cole Publishing Company, 1988, 219-274.

[9] D. E. Smith, History of Mathematics, vol. 2, Dover Publications, Inc., 1958, 331-338.

[10] Frederick W. Stevenson, Projective Planes, W. H. Freeman and Company, 1972.