Finite Projective Planes

1 Introduction

The following axioms are among Euclid's axioms for traditional plane geometry.

Axiom 0. *Given any two lines, there is* at most *one point incident to both of them.*

Axiom 1. *Given any two points, there is a unique line incident to both of them.*

The phrase "at most" in Axiom 0 allows for parallel lines. That is, there may be two lines that don't intersect. If we forbid parallel lines, we get projective planes. That is, projective geometries satisfy Axiom 1 and

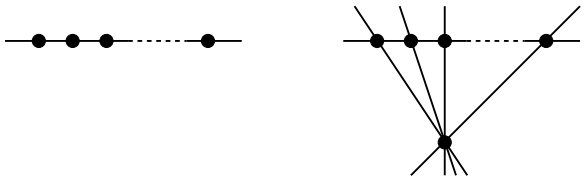
Axiom 2. *Given any two lines, there is* exactly *one point incident to both of them.*

We can modify the real plane so that it does satisfy Axiom 2. One way to do this is to add a point "at infinity" in every direction. That is, for every possible slope $m \in \mathbb{R} \cup \{\infty\}$, add a point ∞_m so that a line is incident to ∞_m if and only if its slope is m. Vertical lines are considered to have slope infinity. We also add one line which is incident to all of the points ∞_m and nothing else. Then, indeed, parallel lines meet at exactly one point, whichever ∞_m corresponds to their common slope m.

Formally, a plane is just a collection of points $\mathcal{P}$, lines $\mathcal{L}$, and an incidence relation $\mathcal{I}$. The plane we constructed above is called the real projective plane. These notes address *finite* projective planes. That is, planes where $\mathcal{P}$ and $\mathcal{L}$ are finite sets.

2 Examples

Consider the following examples.

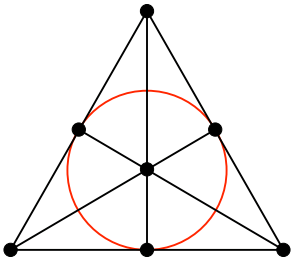


Both of these are, in some sense, degenerate. In the first, we place any number of points on a single line. Formally, there are no "points" other than the ones indicated. Drawing lines as continuous curves is just for convenience.

In the second, we simply add another point outside the first line and then draw as many connecting lines as necessary. There are also other degenerate examples with lines which don't even contain two points!

But there are nontrivial examples as well. Consider the Fano plane, pictured below. This finite projective plane consists of 7 lines and 7 points. (Note that one of these lines is drawn

as a red circle. The places where two lines cross only form a point if it is indicated by a black dot.)



3 A New Axiom

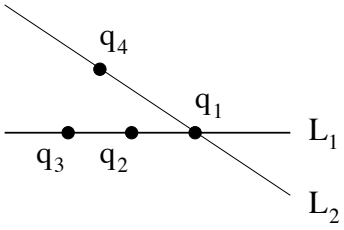
To rule out the degenerate examples from the previous section, we add a new axiom.

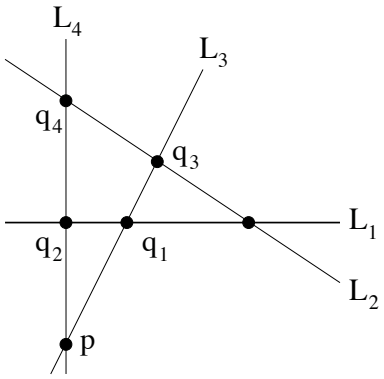
Axiom 3. *There exist four points so that no three of them are collinear.*

We see that Axiom 3 rules out the degenerate examples by proving the following useful lemma about geometries satisfying Axioms 1, 2 and 3.

Lemma 1. *No two lines can cover all points.*

Proof. Suppose that lines L_1 and L_2 cover all points. Let $Q = \{q_1, q_2, q_3, q_4\}$ be points so that no three are collinear. Q is guaranteed to exist by Axiom 3. By Axiom 2, there is a unique point incident to both L_1 and L_2.
Case 1: Suppose that this point is an element of Q. Then the other three points of Q lie on either L_1 or L_2. By the pidgeon-hole principle, at least two of these three points lie on the same line. But then the "intersection point" of L_1 and L_2 are collinear with these two points. Contradiction.





Case 2: Suppose that the intersection point is not an element of Q. Then all four elements of Q lie on exactly one of L_1, L_2. By assumption, no three lie on the same line. Hence two

are incident to L_1 and two are incident to L_2. Without loss of generality, suppose that q_1 and q_2 are incident to L_1, and q_3 and q_4 are incident to L_2.

Axiom 1 guarantees the existence of a (unique) line L_3 which is incident to q_1 and q_3. Similarly, there must be a unique line L_4 which is incident to q_2 and q_4. But by Axiom 2, there is a unique point p which is incident to both L_3 and L_4. The point p cannot be an element of Q, as this would give a set of three collinear elements in Q. Furthermore, it cannot be on L_1 or L_2 - Axiom 2 says that the elements of Q form the *unique* intersection points between L_1 or L_2 with L_3 or L_4. Therefore p is not covered by L_1 and L_2. Contradiction. □

4 Duality

The Fano plane is not the only non-degenerate finite projective plane. In fact, there are infinitely many (as we will see in later sections). All of them are very symmetric. One type of symmetry they exhibit is a *duality* between points and lines. The images we've seen above are just an illustration of a plane. Technically, each plane is just a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$, and a relation called *incidence* $\mathcal{I}$ which consists of pairs of points and lines. Axioms 1, 2 and 3 are restrictions on $\mathcal{I}$. We claim here that the plane consisting of points $\mathcal{L}$, lines $\mathcal{P}$ and incidence $\mathcal{I}$ also satisfies Axioms 1, 2 and 3. To see this, it is enough to show that the "dual" of Axiom 3 is true. Axioms 1 and 2 are already dual to one another.

Exercise 1. *Show that the dual of Axiom 3 is true. That is, that in any finite projective plane, there are four lines so that no three of them are incident to a single point.*

Then we can apply duality to get a second version of every theorem we prove. In particular,

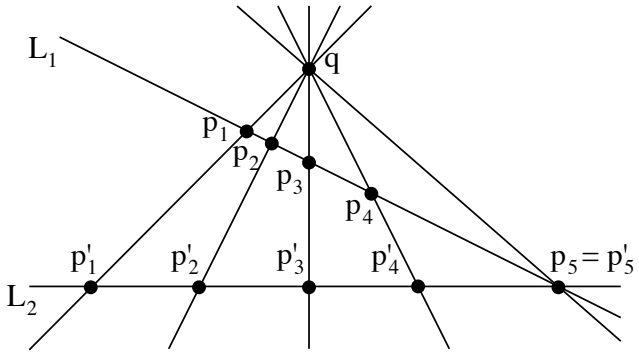
Corollary 1. *No two points cover all lines.*

Proof. We do not claim that every finite projective plane is the same as the one obtained by swapping points and lines. However, any particular finite projective plane has a dual in which no two lines cover all points. Then applying duality again to the dual gives back the original plane. So, in the original plane, no two points cover all lines. □

5 Classifying finite projective geometries

Theorem 1. *Any two lines have the same number of points. We write $n+1$ for this number.*

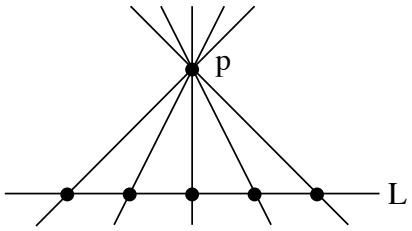
Proof. Let L_1 and L_2 be any two lines. (In this class, "two lines" means two *distinct* lines.) By Lemma 1, there is a point q which is not incident to L_1 nor to L_2. Suppose L_1 is incident to $n+1$ points called p_1, p_2, …, p_{n+1}. Then Axiom 1 gives $n+1$ lines incident to q and each p_i. Call them $L(q, p_i)$. Then for each $1 \leq i \leq n+1$, Axiom 2 gives a point p_i' which is incident to both L_2 and $L(q, p_i)$.



By Axiom 1, all of the lines $L(q, p_i)$ are distinct. (For any $i \neq j$, the unique line containing p_i and p_j is L_1, which does not contain q.) By Axiom 2, all of the points p'_i are all distinct. (For any $i \neq j$, the unique point incident to both $L(q, p_i)$ and $L(q, p_j)$, is q.) Furthermore, by Axioms 1 and 2, these are all of the points incident to L_2. (Another such point would form a new line with q, and this line would have to intersect L_1 somewhere.) Hence L_2 is incident to exactly $n + 1$ points. □

Theorem 2. *Every point is incident to exactly $n + 1$ lines.*

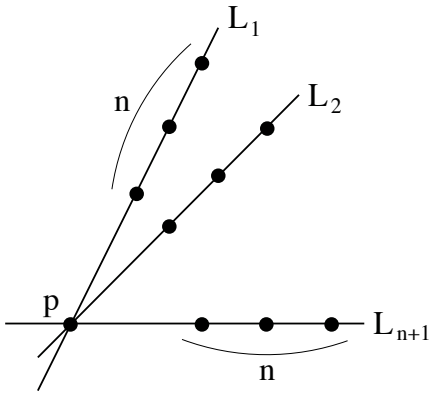
Proof. Let p be any point. By Lemma 1, there is a line L which is not incident to p. We claim that the points incident to L correspond to all the lines incident to p. The details of this proof are analogous to those of Theorem 1. We provide the illustration and leave the rest to the reader.



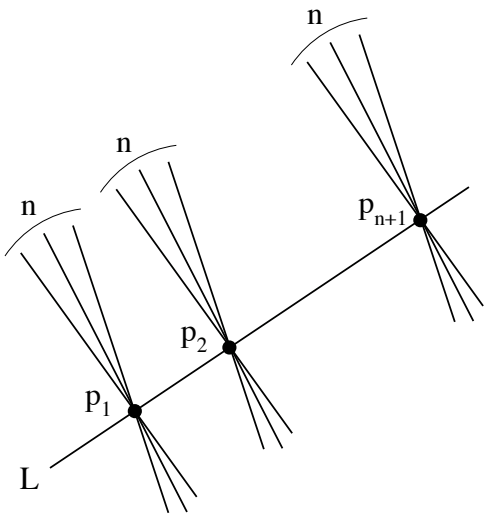
□

Theorem 3. *There are exactly $n^2 + n + 1$ points. There are exactly $n^2 + n + 1$ lines.*

Proof. Let p be any point. There are $n+1$ lines incident to p and each contains an additional n points. This gives $n(n + 1) + 1$ points in total. We leave it to the reader to see that these points are distinct and that they're *all* of the points.



The second result can be obtained by a similar argument (see below), or by applying duality.



□

6 Finite fields

Recall from last week that a field $\mathbb{F}$ as a set with operations "+" and "$*$" so that you can add, subtract, multiply and divide (by non-zero elements) just as you do for numbers. The most natural fields, $\mathbb{Q}$ and $\mathbb{R}$, can be *extended* by adding new elements like $\sqrt{2}$ or $i = \sqrt{-1}$. But you can also get new fields by changing the operations.

One important field is obtained through *modular arithmetic*. Pick a prime p and add, subtract, and multiply the numbers $\{0, 1, \ldots, p-1\}$ normally. However, when your calculations result in a number outside $\{0, 1, \ldots, p-1\}$, add or subtract p as many times needed to get back into this set. For clarity, we will write equality under this system as $\equiv_p$. For

example, $5 \times 3 = 15$ but for $p = 7$

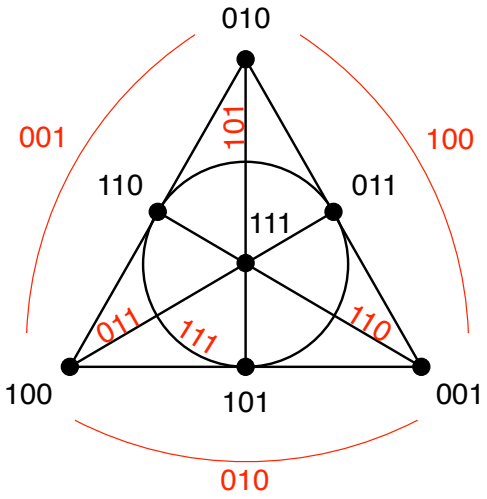
$$5 \times 3 \equiv_p 1 \quad \text{since } 15 - 7 - 7 = 1$$

This example shows that we can divide by 5 (modulo 7) and still get an integer - the same integer we would get if we multiplied by 3 instead.

We claim (but don't prove here) that, for any prime p, the numbers $\{1, 2, \ldots, p-1\}$ are invertible *modulo* p. In other words, we can divide by anything other than 0. Therefore $\{0, 1, \ldots, p-1\}$ is a field with finitely many elements. This field is denoted $\mathbb{F}_p$. It is possible to construct fields with q elements if and only if $q = p^k$ for some prime p and some $k \in \mathbb{N}$.

7 The Fano plane and finite fields

Let's look at the Fano plane again, but now with labels. In the figure below, black labels correspond to points and red labels correspond to lines.



Each label consists of three 0's and 1's. In fact *all* triples of 0's and 1's are used except 000. These labels reflect an underlying rule for incidence: A point xyz is incident to the line abc if and only if

$$ax + by + cz \equiv_2 0.$$

A simple consequence of this rule is the fact that any two points on the same line add up (coordinate-wise, modulo 2) to the third point on that line. For example, the points 010, 111, and 101 all lie on the central vertical line. Remember that $1 + 1 \equiv_2 0$. Therefore the (coordinate-wise, modulo 2) sum of 010 and 111 is 101.

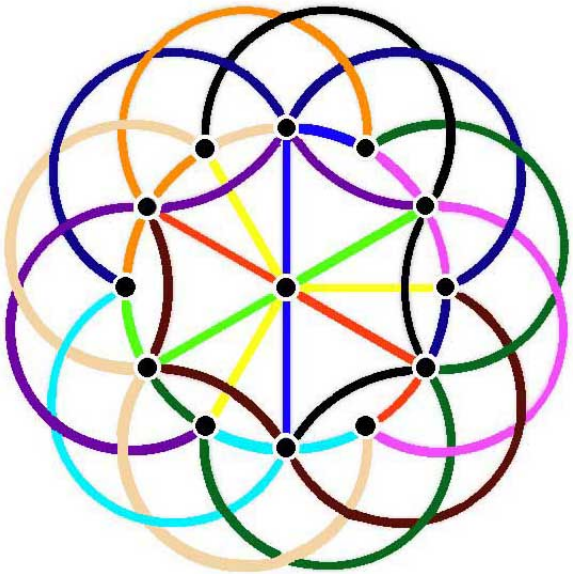
This observation is actually a recipe for building the Fano plane using $\mathbb{F}_2$. Step 1: Make a point and a line for each nonzero triple of integers in $\mathbb{F}_2$. Step 2: Say point xyz is incident to line abc iff $ax + by + cz \equiv_2 0$. The drawing above is just a representation of this rule.

We can do the same for $\mathbb{F}_p$ for any prime p with a small tweak. Underlying everything here is a deep result about linear algebra over finite fields. Points and lines correspond to subspaces of $\mathbb{F}_p^3$. A subspace of dimension 1 (a point here) consists of all scalar multiples of a single vector. In simpler terms, points aren't really vectors, they're *directions*. This is similar to the "points at infinity" we discussed for the real projective plane - we add one in each direction. A subspace of dimension 2 (a line here) consists of all linear combinations of two vectors. This is why labels of points on a line are closed under addition.

The bottom line: we need to ignore scalar multiples. We didn't need this idea for $\mathbb{F}_2$ because the only scalar multiples in this field are 0 and 1. In $\mathbb{F}_3$ we have a nontrivial scalar. Since $2 \times 2 \equiv_3 1$, the vectors 120 and 210 represent the same direction. In fact there are 13 distinct, nonzero directions:

001=002	010=020	100=200
011=022	101=202	110=220
012=021	102=201	120=210
	111=222	

In general, for $\mathbb{F}_p$, there are $(p^3-1)/(p-1)$ directions. This is because there are p^3-1 nonzero vectors and $p-1$ scalar multiples (times $1, 2, \ldots, p-1$) of each vector that "point in the same direction." Take a point p and a line L. Pick some vectors xyz and abc representing their respective directions. Then we define p to be incident to L exactly when $ax + by + cz \equiv_p 0$. The figure below represents the resulting plane for $\mathbb{F}_3$.



Each such plane satisfies Axioms 1, 2, and 3. This is a nontrivial fact but it can be proven using elementary facts about numbers. For example, it is easy to see that no three of the points 001, 010, 100, and 111 can lie on a single line. You can also show that each

point is incident to $p+1$ lines, and each line is incident to $p+1$ points. Finally, the number of points (and lines) is $(p^3-1)/(p-1)$. But simple polynomial division shows us that

$$\frac{p^3-1}{p-1} = p^2 + p + 1.$$

So we have a concrete model for at least one finite projective plane for $n = p$ for a prime in Theorems 1, 2, and 3. You can extend this to $n = p^k$ by using the (more involved) finite fields of prime power order. It is unknown whether other finite projective geometries exist. Using number theory and computer simulations, researchers have shown that such geometries do not exist for $n = 6$ and $n = 10$. Already the case $n = 12$ is open.