Finite Projective Geometry

2^{nd} year group project.

B. Doyle, B. Voce, W.C Lim, C.H Lo

Mathematics Department - Imperial College London

Supervisor: Ambrus Pál

June 7, 2015

Abstract

The Fano plane has a strong claim on being the simplest symmetrical object with inbuilt mathematical structure in the universe. This is due to the fact that it is the smallest possible projective plane; a set of points with a subsets of lines satisfying just three axioms. We will begin by developing some theory direct from the axioms and uncovering some of the hidden (and not so hidden) symmetries of the Fano plane. Alternatively, some projective planes can be derived from vector space theory and we shall also explore this and the associated linear maps on these spaces.

Finally, with the help of some theory of quadratic forms we will give a proof of the surprising Bruck-Ryser theorem, which shows that if a projective plane has order n congruent to 1 or 2 mod 4, then n is the sum of two squares. Thus we will have demonstrated fascinating links between pure mathematical disciplines by incorporating the use of linear algebra, group theory and number theory to explain the geometric world of projective planes.

Contents

1 Introduction

Projective planes are geometrical objects that consist of a set of elements called points and subsets of these elements called lines constructed following three basic axioms which give the resulting object a remarkable level of symmetry. In this paper we will introduce projective planes both axiomatically and in the form of vector spaces, study properties of the simplest projective plane and end with a proof of the Bruck-Ryser theorem which fundamentally links number theory with projective geometry.

To begin thinking about projective geometry let us imagine the standard Euclidean plane with the addition of points at infinity which are defined as the intersection of parallel lines and a line at infinity connecting the points at infinity. The relation of lines being parallel to each other is an equivalence relation and so to each equivalence class of parallel lines there is assigned a unique point at infinity. This effectively closes the Euclidean plane and is called the completion of the plane, and it is easy to show that this new collection of points and lines satisfies the projective plane axioms. This is an example of the general relationship between affine planes and projective planes, where an affine plane can be completed to form a projective plane by the inclusion of the points and a line at infinity and any projective plane can be turned into an affine plane by removing any line and all points on it.

This inclusion of points at infinity creates a fundamental difference between affine and projective planes when invariants under transformation are considered. In Euclidean geometry the transformations of rotation or translation give invariants such as angle or distance however in projective geometry these are not invariant. Instead, projective transformations maintain the structure of the plane as the information of points being on a particular line and lines intersecting at a point are preserved, with a quantity called the cross ratio invariant. These concepts are not mentioned in our paper but would provide useful further reading, as projective geometry can also be described using coordinate systems and the cross ratio used to prove results like the Fundamental Theorem of Projective Geometry. Once you have this theory established, projective geometry can then be used to analyse objects and spaces projected onto one another, as well as the geometry of optics and distortion of images whilst still retaining the original.

The biggest result considered in this paper is the Bruck-Ryser theorem about orders of pro-

jective planes. The order of a projective plane is related to the number of points (and equivalently the number of lines) in the plane and there are interesting number theoretical results describing whether a projective plane of a certain order exists or not. We will show using vector spaces over finite fields that for all integers n there exists a projective plane of order p^n for p prime and indeed all known finite projective planes have prime power order. However, the existence of projective planes for other orders is still researched, the smallest order currently without an answer being 12. Bruck-Ryser goes some way to restricting the possible orders, for example ruling out the possibility of a plane of order 6, and hence we will present a proof of it here.
For a basic introduction to projective geometry see [2].

2 Basic Defintions and results

Let's start with the definition of a projective plane.

Definition 2.1. A Projective plane P is an ordered pair of sets $(p(P), l(P))$, whose elements are called points and lines, respectively, and a relation between these sets, called incidence, satisfying the following axioms:

(I) Given any two distinct points, there is exactly one line incident with both of them.

(II) Given any two distinct lines, there is exactly one point incident with both of them.

(III) There are four points such that no line is incident with more than two of them.

We say that a projective plane is finite if the number of points of the plane is finite.

From now on, when it is convenient, $A, B, ..$ will be points and l_i will be lines, also AB will denoted the unique line incident to both A and B. A incident to l will be denoted $A \in l$ and similarly, A not incident to l is denoted by $A \notin l$. Finally the unique point incident to both l_1 and l_2 is $l_1 \cap l_2$.
The first thing that we will show about projective planes is that there are at least four distinct lines.

Lemma 2.2. *A Projective plane has at least four distinct lines such that no three are incident at the same point.*

Proof. By axiom (III) there are four points A, B, C, D and then by (I) there is a line AB, BC, CD, and DA, incident to each pair $(A, B), (B, C), (C, D), (D, A)$ and each line is unique, otherwise there would be three points incident to one line, contradicting (III). □

Definition 2.3. Let F be a statement about points and lines in a projective plane. The *dual statement* F' of F is the statement where the words *points* and *lines* are swapped.

Given this definition, we have the following dual axioms:

(a) Given any two distinct lines, there is exactly one point incident on both of them.

(b) Given any two distinct points, there is exactly one line incident with both of them.

(c) There are four lines such that no point is incident with more than two of them.

Theorem 2.4. *These two sets of axioms are equivalent.*

Proof. We see that $(I) = (b)$ and $(II) = (a)$. Let us assume the first set of axioms holds. Then by lemma 2.2 we have that the dual axioms hold. Now let's assume the dual axioms hold. By (c) there exist four lines such that their points of intersection are all distinct. Suppose for contradiction that three of these points are collinear on a new line. Then this contradicts (I), as there are two distinct lines through two of the points. (based on ideas from [3, page 4]). □

Hence for any statement about projective planes, the dual statement is also true. This greatly simplifies later proofs and is also one of the beautiful symmetric properties of projective planes.

Theorem 2.5. *Let P be a finite projective plane, then there exists an integer $t \geq 2$ such that,*

(i) Given any point of P there are exactly $t + 1$ lines incident.

(ii) Given any line of P there are exactly $t + 1$ points incident.

We say that t is the order of the projective plane P.

Proof. Consider a point A and a line l with $A \notin l$, we can always do this by (III). Then by (I) there are the same number of points incident with l as lines incident with A. Now pick another point $B \notin l$, again can always do this by (III). The number of lines incident with B is the same as the number of points incident with l, which is the number of lines incident with A. Now A and B were arbitrary therefore this holds for every point of P. □

The other half of the proof holds by duality, or a very similar argument.

Corollary 2.6. *Let P be a finite projective plane of order n, then the number of points (and lines) of P is $n^2 + n + 1$.*

Proof. Pick any point of P, by 2.5 there are $n + 1$ lines incident to it, each line has another n points incident to it, which are all unique by (I). Therefore the total number of points is $(n + 1)n + 1 = n^2 + n + 1$. □

The proofs of 2.5 and 2.6 are influenced by [1, page 9] .

Definition 2.7. Let P be a finite projective plane of order n, then P has $n^2 + n + 1 = N$ points and lines. Let $P_1, P_2, \ldots, P_N$ be the points, and $l_1, l_2, \ldots, l_N$ be the lines. Then we define the incidence matrix A of P to be the N by N matrix such that $a_{ij} = 1$ if and only if the line l_i is incident to the point P_j and 0 otherwise; here the rows represent the lines and the columns the points. This matrix represents the incidence relation between the points and the lines of the plane.(This definition comes from [3, pages 7-8] - note, sometimes the transpose of A is called the incidence matrix, this makes no difference, because of duality).

An incidence matrix is another way to represent finite projective planes, it is very useful for computers. We will use this form of representation later on when proving a result first shown by R. H. Bruck and H. J. Ryser (from now on known as the Bruck-Ryser theorem). But first,we present a proposition that we will use later on.

Proposition 2.8. *Let $B = AA^T$ with A an N×N incidence matrix. Then $b_{ij} = 1$ and $b_{ii} = n+1, i \neq j$.*

Proof. Consider the ij-entry of B, this is $\sum_{k=1}^{N} a_{ik}a_{kj}^T = \sum_{k=1}^{N} a_{ik}a_{jk}$. Since A is an incidence matrix, there are 2 cases to consider, if $i = j$ and if $i \neq j$. When $i \neq j$ then the rows (representing the lines) are different and so have one point in common, giving the sum to be 1. If they are the same line, then as each line has $n + 1$ points on it,the sum will also be $n + 1$. □

3 The Fano Plane

In this section we look at the smallest possible projective plane, as well as introducing some more definitions.

We see that the smallest projective plane is of order two and has seven lines and points. Each line has three points incident to it, and each point is incident to three lines. In fact there is only one projective plane of order two up to isomorphism, called the Fano plane. It is usually represented as in Figure 1. The dots are the points, and the straight lines, plus the circle, are the lines.

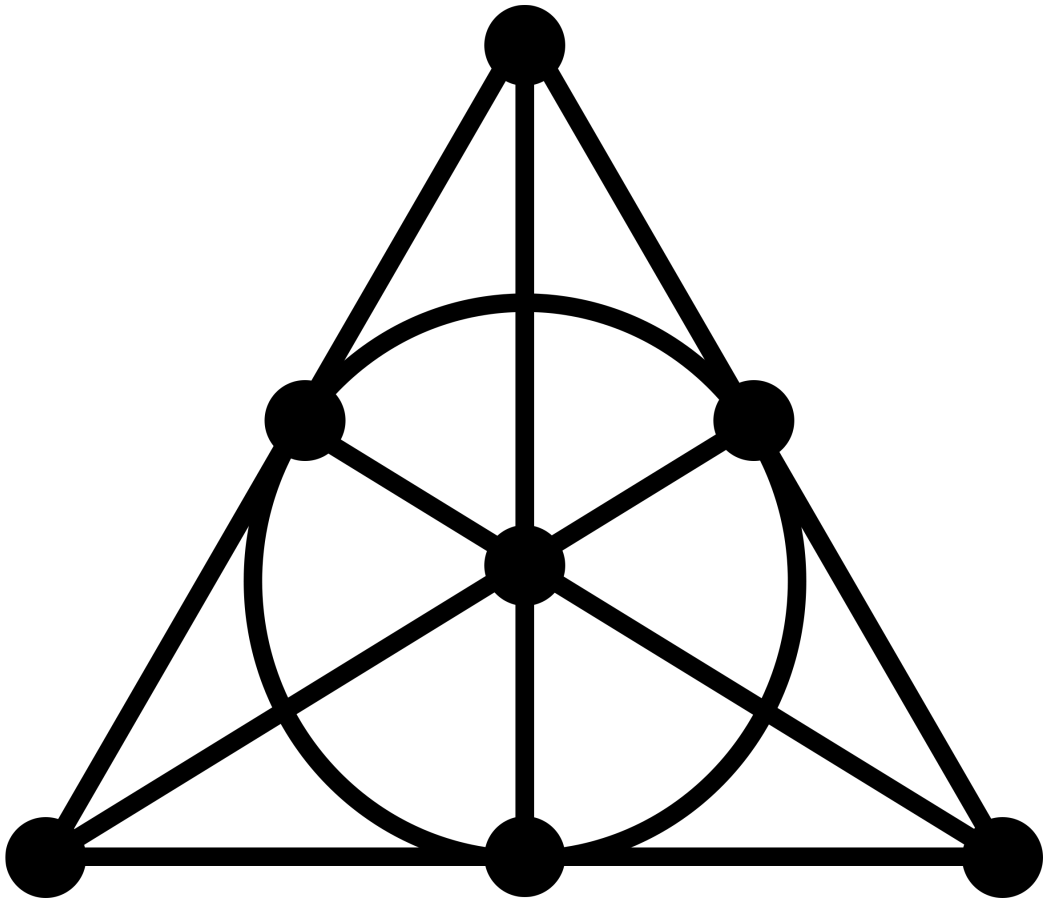

Figure 1: The Fano plane.

3.1 Isomorphism and Automorphism

Definition 3.1. Let $P_1 = (p(P_1), l(P_1))$ and $P_2 = (p(P_2), l(P_2))$ be two projective planes. An isomorphism from P_1 to P_2 is a pair of bijections $\pi : p(P_1) \to p(P_2)$ and $\lambda : l(P_1) \to l(P_2)$ which respect the incidence relation. Clearly the inverses π^{-1}, λ^{-1} form an isomorphism from P_2 to P_1.

Theorem 3.2. *Let P be a finite projective plane of order two, then P is isomorphic to the Fano plane.*

Proof. Let P have seven points, label them $1, 2, ..., 7$. By theorem 2.5 each line has three points incident to it and each point is incident to three lines. Without loss of generality, say the lines incident to 1 are the lines containing $\{1, 2, 3\}, \{1, 4, 6\}, \{1, 5, 7\}$. There must be two other lines on 2 and one of these must be on 4, so again without loss of generality one of them is $\{2, 4, 7\}$ and the other is $\{2, 5, 6\}$. Now 4 must be on one more line, $\{3, 4, 5\}$ and now $\{3, 6, 7\}$ is another line as no two of these points already lie on a line. Hence it is only possible to construct a projective plane of order 2 in one way up to renumbering of the points, so there is only one projective plane of order 2. □

Definition 3.3. An automorphism of a projective plane P is an isomorphism of the plane to itself. All the automorphisms of P form a group, with respect to composition, this group is denoted Aut(P).

Theorem 3.4. *Let P be the Fano plane, then $|Aut(P)| = 168$.*

Proof. Let the points of P be $\{1, 2, 3, 4, 5, 6, 7\}$, and let φ be an automorphism of P, we will consider the possible options for φ.

There are 7 possible options for $\varphi(1)$, and then 6 options for $\varphi(2)$ Without loss of generality, assume 3 is incident to the same line as 1 and 2 are incident to. Then we have 1 choice for $\varphi(3)$ seeing as it has to be incident to the same line as $\varphi(1)$ and $\varphi(2)$. Next there are 4 choices for $\varphi(4)$, and this is the final choice that needs to be made, all the other points have their mapping decided by the incidence relations. We can now see that there are $7 \times 6 \times 4 = 168$ ways of picking φ, each of these are unique and are isomorphic to the Fano plane by 3.2. Therefore $|\text{Aut}(P)| = 168$. □

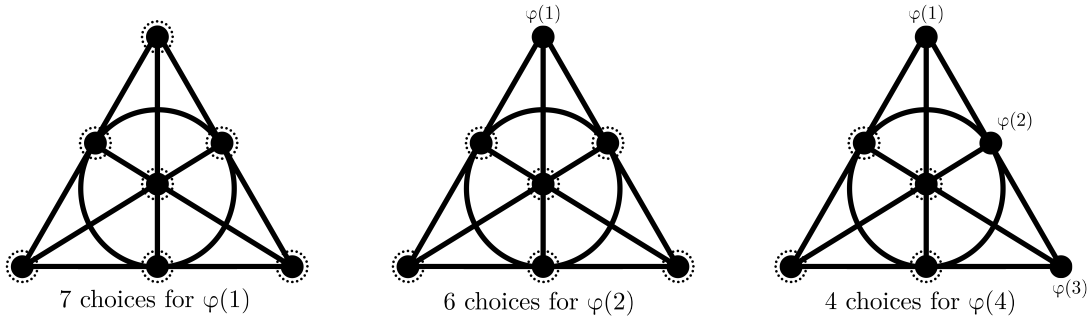

Figure 2: Automorphism options.

Proposition 3.5. *There is an automorphism of the Fano plane that doesn't leave any point fixed.*

To prove this propsition we will use the following result from group theory.

Theorem 3.6 (Cauchy's Theorem)**.** *Let G be a finite group, and let p be a prime that divides the order of G, then there is an element of order p.*

Proof. Let G be any finite group, $|G| = n$ and let p be a prime dividing n, and consider the set

$$X = \{(x_1, x_2, \ldots, x_p) | x_i \in G, x_1 x_2 \ldots x_p = e_G\}.$$

Then $|X| = n^{p-1}$ because the first $p-1$ elements can be any element from G, and $x_p = (x_1 x_2 \ldots x_{p-1})^{-1}$. Now define an equivalence relation $\sim$ on X, where $(a_1, \ldots, a_p) \sim (b_1, \ldots, b_p)$ if $(b_1, \ldots, b_p)$ is a cyclic permutation of $(a_1, \ldots, a_p)$, i.e. $a_i = b_j$ where $j + k \equiv i \pmod{p}$ for some fixed k and all i, j. Then either all the x_i are the same ($x_i^p = e_G$), and these equivalence classes are of size one, or $x_i \neq x_j$ for some $i \neq j$ and the equivalence classes are of size p. Therefore $s + tp = n^{p-1}$, where s, t are the number of equivalence classes of size 1,p respectively. Now p divides n, therefore p divides s, and $s \geq 1$ seeing as $x_i = e_G$ for all i, is an equivalence class of size one. □

Proof of 3.5. $|\text{Aut}(P)| = 168 = 7 \times 24$, therefore by 3.6 there is an element of order seven, and an automorphism of order seven can't fix any points. □

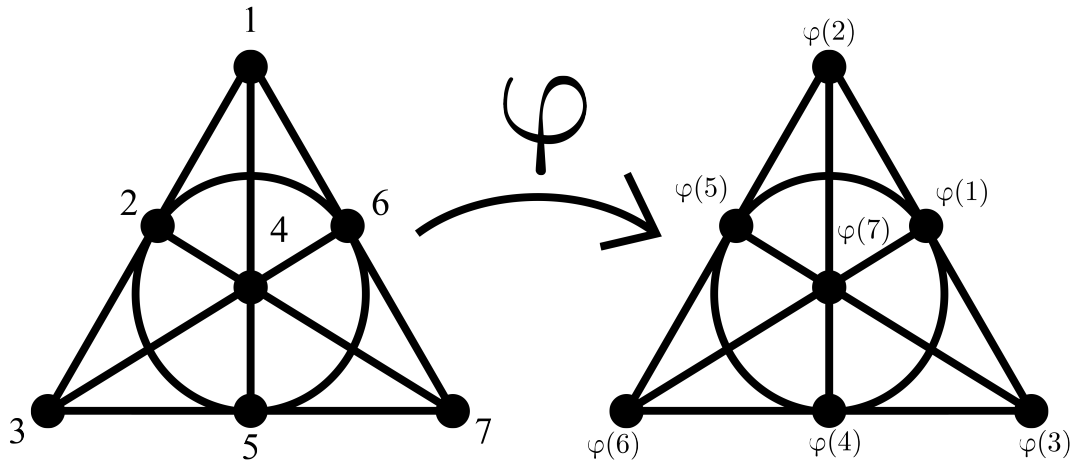

Figure 3: An automorphism that leaves no point fixed.

3.2 Ovals

The natural object of study after objects defined by linear equations, or lines, in the Euclidean space are quadratic sets. In the Euclidean plane, theses correspond to the well-known conic sections. In the projective plane, the non-degenerate quadratic sets correspond to ovals (see - [6, page 144]). Here we will look at ovals in the Fano plane.

Definition 3.7. An oval (also called a super-oval or hyper-oval) on the Fano plane is a set of four points such that no line is incident with more then two of them, denoted O.

Proposition 3.8. *There are 7 ovals in the Fano Plane.*

Proof. We will show this by counting all the possible ovals, each oval has four points, so all we need to do is find the number of ways to pick each point. Label the points of the oval $\{1, 2, 3, 4\}$. We see that there are seven ways to pick 1, six ways to pick 2, and now even though there are five remaining points, one of them is incident to the line incident to both 1 and 2, so there are only four ways to pick 3. Once the first three points have been picked, the fourth point is decided, there is only one place for it to go. The reason for this is, we have four remaining points, but three of these are collinear with one of the pairs $\{1, 2\}, \{1, 3\}, \{2, 3\}$ (if two of those pairs met at the same point, there would be two lines incident to two points, contradicting (I)).

So we see that there are $7 \times 6 \times 4 \times 1$ ways of picking the points to create an oval, however some of these will create the same oval, seeing as $\{1, 2, 3, 4\}$ is the same oval as {4,2,1,3} for example. There are $4!$ ways of ordering four items, so

$$\frac{7 \times 6 \times 4 \times 1}{4 \times 3 \times 2 \times 1} = 7$$

different ovals in the Fano plane. □

After finding some examples of ovals, and the fact that we have seven ovals, and seven lines, we wondered if there was a relationship between lines and ovals. In fact there is, every oval is related to a line in a certain way, and the reverse also holds.

Theorem 3.9. *Let the points of the Fano plane be labelled $\{A, B, C, D, E, F, G\}$, then $O = \{A, B, C, D\}$ is an oval if and only if $O^c = \{E, F, G\}$ is a line l.*

Proof. (if)
Assume $O = \{A, B, C, D\}$ is an oval, then by (I), between each pair of points there is a unique line, four points means six pairs and therefore six lines. By 2.6 we have that there is a seventh line l in the Fano plane. Next we show that the points incident to l are disjoint from O. Without loss of generality, consider the lines l_1, l_2, l_3 such that $A \in l_i, i = 1, 2, 3$. We have B, C, D incident to l_1, l_2, l_3 respectively, and a third unique point of each line by (I) (if it wasn't unique, there would be two lines incident to A and that point). So we have three more points E, F, G, now sufficient to show that $EF = FG$, but this clearly holds, because we have seven lines in the Fano plane by 2.6, and six of them are incident to two points of O, now both EF and FG can be incident to at most one point of O. Therefore EF and FG must both be line seven which implies $EF = FG = l$ and $l \cap O = \emptyset$.
(only if)
Let $l = \{A, B, C\}$, then by (II) each other line must be incident with one and only one of A, B, C, this implies that no three of $\{D, E, F, G\}$ can be collinear (be incident to the same line). Therefore $\{D, E, F, G\}$ is an oval. □

So we see that most questions that can be asked about ovals can be answered by looking at the complementary line. The next proposition is a clear example of this.

Proposition 3.10. *Let O_1 and O_2 be any two ovals on the Fano plane, then there exists an automorphism φ of the Fano plane such that $\varphi(O_1) = O_2$.*

Proof. Let O_1 and O_2 be any two ovals of the Fano plane, then by 3.9 there are two lines l_1 and l_2 associated with respectively O_1 and O_2. Now using a similar argument as in 3.4 we see that we can pick any two points incident to l_1 and always be able to map them to any two points incident to l_2. Therefore by 3.9 we have O_1 is mapped to O_2. □

Proposition 3.11. *The subgroup of $Aut(P)$ which maps O to itself is isomorphic to S_4*

Proof. Let O be any oval in the Fano plane, and let H be the subgroup of Aut(P) that maps O to itself. First note that if an automorphism fixes three non-collinear points it is then the identity. Therefore we see that H is isomorphic to a subgroup of S_4 (all automorphisms are just permutations of the four points of O). Now by 3.9 there is a complementary line l, and if O is mapped to itself, so is l, therefore can look at automorphisms φ that map l to itself. Pick any two points $A, B \in l$, then there are three choices for $\varphi(A)$, and two choices for $\varphi(B)$, these two points fully determine l. Finally by a similar argument to 3.4 φ is determined by a third point $C \notin l$, this point can be mapped to any of the four points of O. Therefore there are $3 \times 2 \times 4 = 24$ different automorphisms in H. We have H isomorphic to a subgroup of S_4 and $|H| = |S_4|$, which implies $H \cong S_4$. □

4 Projective Geometry with fields

4.1 Constructing Projective Planes from fields

Constructing projective planes from the axioms, while possible, is a rather difficult task. In this section, we will show that for every field, we can define a projective plane corresponding to the field. This gives many important examples of projective planes.

Definition 4.1. Let F be a (commutative) field and let V be a three-dimensional vector space over F. The projective plane $\mathbb{P}(F)_V$ over F is defined as follows. The set of points of $\mathbb{P}(F)_V$ are the one-dimensional linear subspaces of V , and the set of lines of $\mathbb{P}(F)$ are the two-dimensional linear subspaces of V. A point p of $\mathbb{P}(F)_V$ is incident to a line l of $\mathbb{P}(F)_V$ if p is contained in l.

Remark 4.2. We will show later that this definition is, in fact, independent of the vector space chosen. That is, if V and W are two different three-dimensional vector spaces over F, then $\mathbb{P}(F)_V$ and $\mathbb{P}(F)_W$ are isomorphic projective planes.

Proposition 4.3. *$\mathbb{P}(F)_V$ is a projective plane.*

Proof. Let U, W be distinct points in $\mathbb{P}(F)_V$. Since U, W are one-dimensional subspaces of V, where V is a three-dimensional vector space over F, we can write $U = \langle u \rangle$, $W = \langle w \rangle$ for some $u, w \in V$, u, w are linearly independent (otherwise $U = W$).
Let $l = \text{span}(u, w)$. Clearly, $U, W \subset l$. Suppose l' is another line containing U and W, then it must contain u, w as elements. Since l' is two-dimensional, we have $l = l'$.
Now let l_1, l_2 be two distinct lines in $\mathbb{P}(F)_V$. Let $l_1 = \text{span}(u_1, w_1)$, $l_2 = \text{span}(u_2, w_2)$. Note that if $\dim(l_1 \cap l_2) = 0$, then u_1, w_1, u_2, w_2 is a set of linearly independent vectors, contradicting the fact that $dim(V) = 3$. If $\dim(l_1 \cap l_2) = 2$, then $l_1 = l_2$. Hence we must have $\dim(l_1 \cap l_2) = 1$. This point is unique as any point contained in l_1 and l_2 must be contained in $l_1 \cap l_2$ and any one-dimensional subspace of a one-dimensional space must be itself.
Finally, take three linearly independent vectors - say e_1, e_2, e_3, and consider the four points $\langle e_1 \rangle, \langle e_2 \rangle, \langle e_3 \rangle, \langle e_1 + e_2 + e_3 \rangle$. Suppose there exists a line l that contains three of the points. If l contains $\langle e_1 \rangle, \langle e_2 \rangle, \langle e_3 \rangle$, then since e_1, e_2, e_3 are linearly independent, $\dim(l) \geq 3$. Otherwise, l contains $e_1 + e_2 + e_3$, e_i, e_j where $i, j = 1, 2, 3$, $i \neq j$. We can obtain the remaining e_k from $e_1 + e_2 + e_3 - e_i - e_j$, hence l also contains e_1, e_2, e_3.
Since $\dim(l) = 2$, it follows that such a line cannot exist. Hence we have found four distinct points such that no three are collinear. □

We now show that this if V and W are three-dimensional vector spaces over F, then $\mathbb{P}(F)_V$ and $\mathbb{P}(F)_W$ are isomorphic.

Proposition 4.4. *Let V, W be n-dimensional vector spaces over F and $\phi : V \to W$ be an injective F-linear map from V to W. Then ϕ is a bijective F-linear map and there is a one-to-one correspondence between subspaces of V and subspaces of W.*

Proof. Note that any injective linear map between finite-dimensional vector spaces maps basis to basis. Indeed, let $\{v_i\}_{i=1}^n$ be a basis for V. Then $\{\phi(v_i)\}_{i=1}^n$ is a set of n vectors. Since

$\sum_{i=1}^{n} c_i\phi(v_i) = \phi(\sum_{i=1}^{n} c_i v_i)$ and ϕ maps zero to zero, we have that $\{\phi(v_i)\}_{i=1}^{n}$ is linearly independent. Since W is n-dimensional, it follows that $\{\phi(v_i)\}_{i=1}^{n}$ is a basis.
Let U be a subspace of V of dimension m, then since ϕ maps basis to basis, $\phi(V)$ also has dimension m. Since ϕ is invertible,the reverse direction is proved by considering ϕ^{-1}. □

Hence for three-dimensional vector spaces V and W and their corresponding projective planes $\mathbb{P}(F)_V$ and $\mathbb{P}(F)_W$, ϕ maps points to points and lines to lines.
Let $p(\phi) : p(\mathbb{P}(F)_V) \to p(\mathbb{P}(F)_W)$ and $l(\phi) : l(\mathbb{P}(F)_V) \to l(\mathbb{P}(F)_W)$ be defined by $p(\phi(P)) = \phi(P)$, $l(\phi(L)) = \phi(L)$. By the previous proposition, $p(\phi)$ and $l(\phi)$ are bijective, hence the pair $p(\phi), l(\phi)$ defines an isomoprhism between $\mathbb{P}(F)_V$ and $\mathbb{P}(F)_W$ as projective planes.
Hence we can unambiguously define the projective plane over F, $\mathbb{P}(F)$ as $\mathbb{P}(F)_V$ for some three-dimensional vector space V over F.

4.2 Order of Projective Planes over fields

Using this construction, we can construct a projective plane from any vector space over any field. We now show that every finite field has order p^n, where p is a prime, which would allow us to show the existence of a projective plane of a prime power order.

Definition 4.5. Let F be a field. The characteristic of a field, char(F), is the smallest positive number (if exists) n such that $n \cdot 1 = 0$, where $n \cdot 1$ is defined to be $\underbrace{1 + \ldots + 1}_{\text{n times}}$. If it does not exist, we define char$(F) = 0$.

Lemma 4.6. *Let F be a finite field. Then $char(F)$ is prime.*

Proof. Let $n = char(F)$. Suppose $n = pq$, then we have $n \cdot 1 = pq \cdot 1 = (p \cdot 1)(q \cdot 1) = 0$. Since F is a field, it is an integral domain, hence either $p \cdot 1 = 0$ or $q \cdot 1 = 0$, contradicting the minimality of n. Hence n is prime. □

Lemma 4.7. *Let $char(F) = p$. The set $F' = \{0, 1, \ldots, (p-1) \cdot 1\}$ is a subfield of F of order p.*

Proof. Since associativity, commutativity and distributivity are inherited from F, it suffices to check closure and the existence of inverses for addition and multiplication.
Fix $n, m \in \{0, 1, \ldots, p-1\}$. If $n + m < p$, we have $n \cdot 1 + m \cdot 1 = (n + m) \cdot 1 \in F'$. Otherwise,

let $n + m \equiv m' \pmod{p}$ where $m' \in \{0, 1, \ldots, p-1\}$, then $n \cdot 1 + m \cdot 1 = m' \cdot 1 \in F'$. Let $n' \in \{0, \ldots, p-1\}$ such that $n' \equiv -n \pmod{p}$. Then $n' \cdot 1 + n \cdot 1 = 0$.

Now let $nm \equiv y \pmod{p}$, where $y \in \{0, 1, \ldots, p-1\}$. Then $(n \cdot 1)(m \cdot 1) = y \cdot 1 \in F'$. Moreover, if $m \neq 0$, choose $m' \in \{0, 1, \ldots, p-1\}$ such that $mm' \equiv 1 \pmod{p}$. Then $(m \cdot 1)(m' \cdot 1) = 1$.

□

Lemma 4.8. *Given a field F and a subfield F', we can view F as a vector space over F'.*

Proof. Define $+$ as addition in fields and $\cdot$ (scalar multiplication) as multiplication in fields. Since F is a field, $(F, +)$ is an abelian group. Associativity and distributivity of scalar mulitiplication are inherited from the axioms of a field. □

Theorem 4.9. *F has order p^n for some $n \in \mathbb{N}$.*

Proof. Since F is finite, it must be a finite dimensional vector space over F'. Let $n = dim(F)$, $v_1, \ldots, v_n$ be a basis of F. Every element $v \in F$ can be written uniquely as $v = \sum_{i=1}^{n} a_i v_i$ where $v_i \in F'$. There are p^n choices for the n-tuple $(a_1, \ldots, a_n)$, hence $|F| = p^n$. □

So far we have shown that every finite field F has some prime power order. In fact, the converse is also true - for every prime power p^n, there exists a finite field F_{p^n} of that order. To prove the converse, we shall quote some basic results from field theory.

Definition 4.10. Let F, K be fields such that $F \subset K$ and $p(x) \in F[x]$. Then K is called the splitting field of $p(x)$ if $p(x)$ factors completely into linear factors in $K[x]$ and $p(x)$ does not factor into linear factors over any proper subfield of K containing F.

Theorem 4.11. *Let $f(x) \in F[x]$. Then the splitting field of $f(x)$ always exists.*

The proof of the above can be found in Appendix A.

Theorem 4.12. *Fix p prime and $n \in \mathbb{N}$, then a field of order p^n exists.*

Proof. Let F be a finite field of order p and let $f(x) = x^{p^n} - x \in F[x]$. Let K be the splitting field of $f(x)$ and let $S = \{t \in K : t^{p^n} - t = 0\}$. We claim that this is a field of order p^n.
Since $f(x)$ can be factored completely into linear factors over K, there are at most p^n roots of

$f(x)$. To see that all roots are distinct, suppose λ is a repeated root of $f(x)$. Then $f(x) = x^{p^n} - x = (x-\lambda)^2 g(x)$. Taking derivatives on both sides (in the algebraic sense) gives $p^n x^{p^n-1} - 1 = 2(x-\lambda)g(x) + (x-\lambda)^2 g'(x)$. Since F has characteristic p, K has characteristic p (as it contains F as a subfield). Hence we have $-1 = 2(x-\lambda)g(x) + (x-\lambda)^2 g'(x)$, which is clearly false when $x = \lambda$. Hence all roots are distinct, i.e. S contains p^n elements.

It remains to check that S is indeed a field. Associativity, commutativity and distributiy are inherited from K, hence it suffices to prove closure and the existence of inverses for both operations.

Let $a, b \in S$. Note that $(a+b)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} a^i b^{p^n-i} = a^{p^n} + b^{p^n}$ since F has characteristic p. Hence $(a+b)^{p^n} - (a+b) = a^{p^n} - a + b^{p^n} - b = 0$. If $p > 2$, then $(-a)^{p^n} - a = -a^{p^n} + a = 0$. If $p = 2$, then we have $-1 = 1$ since $1 + 1 = 0$. Hence $(-a)^{p^n} + a = a^{p^n} + a = a^{p^n} - a = 0$. Hence $-a \in S$.

Let $a, b \in S$. Then $(ab)^{p^n} - ab = (ab)^{p^n} - a^{p^n} b + a^{p^n} b - ab = a^{p^n}(b^{p^n} - b) + b(a^{p^n} - a) = 0$. Moreover, if $a \neq 0$, then $a^{-1} \in S$ as $(a^{-1})^{p^n} - a^{-1} = a^{-p^n-1}(a - a^{p^n}) = 0$.

Hence S is a field of order p^n. □

Remark 4.13. In fact, any two finite fields of the same order are isomorphic. See [9, page 5].

Corollary 4.14. *There exists a projective plane of order p^n.*

Proof. Let $\mathbb{F}_{p^n}$ be a finite field of order p^n and V be a three-dimensional vector space over $\mathbb{F}_{p^n}$. Consider the projective plane $\mathbb{P}(\mathbb{F}_{p^n})$. Fix a two dimensional subspace U in V. Then $U = \{au + bv : a, b \in \mathbb{F}_{p^n}\}$ for some linearly independent vectors $u, v \in U$. Notice that when $a \neq 0$, $au + bv$ and $u + \frac{b}{a}v$ define the same point in the projective plane, hence it suffices to count the number of choices of $u + cv$ for $c \in \mathbb{F}_{p^n}$, which is p^n. Adding the case when $a = 0$, corresponding to the point $\langle v \rangle$, gives $p^n + 1$ points passing through the line U. Hence $\mathbb{P}(\mathbb{F}_{p^n})$ has order p^n. □

Corollary 4.15. *The Fano plane is isomoprhic to $\mathbb{P}(\mathbb{F}_2)$.*

Proof. By 4.14, $\mathbb{P}(\mathbb{F}_2)$ has order 2. By 3.2, $\mathbb{P}(\mathbb{F}_2)$ is isomorphic to the Fano plane. □

So far we have only seen examples of projective planes that are constructed from vector spaces over fields. This construction can be generalised where we consider a vector space over

a skew field - see [6, pages 55-59]. Projective planes constructed from fields and skew-fields have the advantage of being able to use tools from linear algebra to study their structure.

However, not all projective planes are constructed from vector spaces over fields or skew fields - see [7] for an example of a projective plane of order nine not constructed from fields or skew-fields, hence more effort has to be done if one wishes to classify all projective planes. As of right now, all known projective planes have prime power order. This naturally leads to the question whether every projective plane has prime power order. This is as of now an open problem, but in the next section we will discuss a theorem (Bruck-Ryser) which gives a partial result to the problem.

5 Bruck-Ryser

In this section we aim to prove the Bruck-Ryser theorem about non-existence of certain orders of finite projective planes. The original first proof can be found at [10], we will prove it based on [1, page 10-14] and [5], rewritten with added details.

Theorem 5.1 (Bruck-Ryser)**.** *Let P be a projective plane of order n, then if $n \equiv 1$ or $2 \pmod 4$, we have n is the sum of two squares.*

To prove Bruck-Ryser, we will use incidence matrices, plus five facts from number theory.

Lemma 5.2. *The following identities hold,*

$$(a_1^2 + a_2^2)(x_1^2 + x_2^2) = (a_1x_1 - a_2x_2)^2 + (a_1x_2 + a_2x_1)^2 \tag{1}$$

and

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2 \tag{2}$$

where

$$y_1 = a_1x_1 - a_2x_2 - a_3x_3 - a_4x_4,$$

$$y_2 = a_1x_2 + a_2x_1 + a_3x_4 - a_4x_3,$$

$$y_3 = a_1x_3 + a_2x_1 + a_4x_2 - a_2x_4,$$

$$y_4 = a_1x_4 + a_2x_1 + a_2x_3 - a_3x_2.$$

Proof. The proof is a long algebraic exercise, but requires no tricks, so we will not prove it here, however we note that if $\mathbf{a} = a_1 + ia_2, \mathbf{x} = x_1 + ix_2$, then the fact that $\|\mathbf{a}\|\|\mathbf{x}\| = \|\mathbf{ax}\|$ (where $\|\mathbf{a}\|$ is the normal norm in $\mathbb{C}$) gives us (1) straight away. Similarly (2) can be found by looking at a norm on another mathematical structure, the quaternions. (The quaternions are an extension of $\mathbb{C}$, with not only i, but also j, k, with $i^2 = j^2 = k^2 = ijk = -1$, a general element is $q_1 + iq_2 + jq_3 + kq_4,\ q_1, q_2, q_3, q_4 \in \mathbb{R}$, for more details on quaternions see [11]). □

Lemma 5.3. *Let p be a prime, then if there are two integers x, y such that,*

$$x^2 + y^2 \equiv 0 \pmod{p}$$

then p is the sum of two squares.

Proof. Let r be the smallest integer such that there exist x, y such that $x^2 + y^2 = rp$, now assume $r > 1$, (if $r = 1$ then the proof is already finished). Now let $u \equiv x \pmod{r}$ and $v \equiv -y \pmod{r}$, where $|u|, |v| \leq \frac{r}{2}$. Then

$$u^2 + v^2 = x^2 + y^2 = 0 \pmod{r}$$

so $u^2 + v^2 = sr$ for some $s < r$. Now

$$(u^2 + v^2)(x^2 + y^2) = r^2sp = (ux - vy)^2 + (vx + uy)^2 \quad \text{by identity (1),}$$

and

$$ux - vy = x^2 + y^2 = 0 \pmod{r}, \text{so } ux - vy = \alpha r,$$

similarly

$$vx + uy = -yx + xy = 0 \pmod{r}, \text{so } vx + uy = \beta r.$$

Both of these imply that

$$(ux - vy)^2 + (vx + uy)^2 = (\alpha r)^2 + (\beta r)^2 = r^2 sp,$$

therefore

$$\alpha^2 + \beta^2 = sp,$$

with $s < r$, but r was minimal, which is a contradiction, so $r = 1$. □

Lemma 5.4. *Let p be a prime, then if there are four integers x, y, u, v such that*

$$x^2 + y^2 + u^2 + v^2 \equiv 0 \pmod{p}$$

then p is the sum of four squares.

Proof. The proof is basically the same as 5.3, but using identity (2). □

Lemma 5.5. *Every natural number is the sum of four squares.*

Proof. By 5.2 it is sufficient to prove for prime numbers (seeing as all integers are products of primes and identity (2) can be applied multiple times). Note that $2 = 1^1 + 1^2 + 0^2 + 0^2$, so can consider only odd primes p.

If -1 is a quadratic residue modulo p, (m is a quadratic residue modulo p if there exists an integer x such that $x^2 \equiv m \pmod{p}$), then there exists an integer x such that $x^2 \equiv -1 \pmod{p}$. Therefore $x^2 + 1 \equiv 0 \pmod{p}$ and by 5.3, p is the sum of two squares.

If -1 is not a quadratic residue, then let m be the smallest positive quadratic non-residue, we then have that both $-m$ and $m - 1$ are quadratic residues (non-residue×non-residue = residue, m is minimal and $m > 1$, because 1 is a quadratic residue). Therefore there exists x, y such that $x^2 \equiv -m \pmod{p}, y^2 \equiv m - 1 \pmod{p}$, this implies that $x^2 + y^2 + 1 \equiv 0 \pmod{p}$, and by 5.4, p is the sum of four squares. □

Lemma 5.6. *If $nx^2 = w^2 + y^2$ has a solution in integers then n is the sum of two squares.*

Proof. First consider the case where n is square-free, $n = p_1 p_2 \dots p_s$ for some distinct primes p_i. Then $w^2 + y^2 \equiv 0 \pmod{p_i}$, therefore by 5.3, p_i is the sum of two squares, and so is n (apply

the identity (1) multiple times). If n is not square-free, then $n = m^2 r$ where $r = q_1 q_2 \dots q_t$, q_j distint primes. By the above r can be written as the sum of two squares, $r = a^2 + b^2$. Therefore $n = m^2(a^2 + b^2) = (am)^2 + (bm)^2$. □

Now we are finally ready to prove Bruck-Ryser.

Proof of 5.1. Let P be a projective plane of order n, Let $N = n^2+n+1$ be the number of points and lines of P, and let A be an incidence matrix of P. Consider $\mathbf{z} = A\mathbf{x}$ where $\mathbf{x} = (x_1, x_2, \dots, x_N)^T$. Then by 2.8,

$$\mathbf{z}^T\mathbf{z} = \mathbf{x}^T A^T A\mathbf{x} = \mathbf{x}^T B\mathbf{x} + n\mathbf{x}^T I\mathbf{x}$$

where B is the matrix of one's and I is the identity matrix. Therefore

$$z_1^2 + z_2^2 + \dots + z_N^2 = w^2 + n(x_1^2 + x_2^2 + \dots + x_N^2)$$

where $w = x_1 + x_2 + \dots + x_N$. The next step is to add nx_{N+1}^2 to each side,

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

Now $n \equiv 1$ or $2 \pmod 4$, therefore $N + 1 \equiv 0 \pmod 4$, and by 5.5 we have that $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Applying identity (2) to each group of four x_i's, we get y_i's that are linear combinations of the x_i.

$$z_1^2 + z_2^2 + \dots + z_N^2 + nx_{N+1}^2 = w^2 + y_1^2 + y_2^2 + \dots + y_N^2 + y_{N+1}^2$$

Now by definition, the z_i are also linear combinations of the x_i. We must have that there is a z_i and a y_j such that both contain some multiple of x_1. Without loss of generality, assume they are z_1, y_1. Set $z_1 = y_1$ if the coefficient of x_1 is different in z_1 and y_1, if not set $z_1 = -y_1$. Then we get x_1 in terms of the other x_i, and the z_1^2 and y_1^2 terms cancel out. Continue doing this, each time expressing x_j in terms of the x_k, where $k > j$, in such a way that without loss of generality z_j^2 cancels out y_j^2. We get in the end,

$$nx_{N+1}^2 = w^2 + y_{N+1}^2 \tag{3}$$

with w, y_{N+1} being some rational multiple of x_{N+1}. Now there were no conditions on x_{N+1} so we can pick it in such a way that both y_{N+1} and w are integers. (x_{N+1} is the product of the two respective denominators of w, y_{N+1}). Therefore (3) has integer solutions, and by 5.6, n is the sum of two squares. □

The orders of projective planes which Bruck-Ryser deals with are $2, 5, 6, 9, 10, 13, 14, 17, 18, 21, 22, 25, 26 \ldots$ and of those $6, 14, 21, \ldots$ are not the sum of two squares. Therefore there is no projective plane of order $6, 14, 21$. However Bruck-Ryser does not prove that if n is the sum of two squares then there is a projective plane, in fact it has been proved that there is no projective plane of order 10 - see [8].

It has been conjectured that all finite projective planes have prime power order, currently the first possible counter-example is 12.

A Appendix - Rings and Fields

In this subsection we will develop the tools needed to prove that for a field F and a polynomial $p(x)$, the splitting field of $p(x)$ always exists. The following proofs are influenced by [9] and [12].

All rings considered in this section are assumed to be commutative and with unity.

Theorem A.1. *Let R be a ring and I be an ideal. Note that $(R,+)$ is an abelian group and $(I,+)$ is a subgroup of $(R,+)$. Any subgroup of an abelian group is normal, hence $R/I = \{a+I : a \in R\}$ is a well-defined group under addition. Define multiplication on R/I by $(a+I)(b+I) = ab+I$. This gives R/I a ring structure.*

Proof. We check that this multiplication is well-defined. It then follows from the ring axioms that this muliplication satisfies the axioms for a ring.

Suppose $a+I = a'+I$,$b+I = b'+I$, then we have $a-a' \in I$ and $b-b' \in I$. We need to show that $ab+I = a'b'+I$, i.e. $ab-a'b' \in I$. Note that $ab-a'b' = ab-a'b+a'b-a'b' = b(a-a')+a'(b-b')$. Since $a-a', b-b' \in I$, $b(a-a') \in I$ and $a'(b-b') \in I$. Hence $ab-a'b' \in I$.

□

Proposition A.2. *Let R be a ring, I be an ideal of R. Then there is a one-to-one correspondence between ideals in R that contain I and ideals in R/I.*

Proof. Let $\pi : R \to R/I$ be the canonical projection, i.e. $\pi(a) = a+I$. Let

$\mathcal{I} = \{J : J$ is an ideal in R containing $I\}$ and $\mathcal{I}' = \{J : J$ is an ideal in $R/I\}$. π induces a map $\pi' : \mathcal{I} \to \mathcal{I}'$ defined by $\pi(J) = \{a \in R/I : a = \pi(r)$for some $r \in J\}$.

We first check that this is a well-defined map from $\mathcal{I}$ to $\mathcal{I}'$. Let J be an ideal in R that contains I, we show that $\pi(J)$ is indeed an ideal of R/I. Let $a, b \in \pi(J)$. Then $a = r+I, b = s+I$ for some $r, s \in J$. We have $r+s \in J$, hence $r+s+I \in \pi(J)$ and this addition is clearly abelian as $(R,+)$ is abelian. Hence $(\pi(J),+)$ forms an abelian group. Next, let $c \in R/I$, i.e. $c = t+I$ for some $t \in R$. Then $ca = (t+I)(r+I) = tr+I$ where $tr \in J$ as $r \in J$. Hence $ca \in \pi(J)$. Therefore, $\pi(J)$ is an ideal.

Define $\pi^{-1} : \mathcal{I}' \to \mathcal{I}$ by $\pi^{-1}(J) = \{a \in R : \pi(a) \in J\}$, where J is an ideal in R/I. We check that this is also a well-defined map. Let $a, b \in \pi^{-1}(J)$. Then $a+I, b+I \in J$. Hence

$a + b + I \in J$, i.e. $a + b \in \pi^{-1}(J)$. This shows that $(\pi^{-1}(J), +)$ is an abelian group. Let $r \in R$. $ra + I = (r + I)(a + I) \in J$, hence $ra \in \pi^{-1}(J)$. Hence $\pi^{-1}(J)$ is an ideal. Let $i \in I$, then $\pi(i) = I \in J$. Hence $I \subset \pi^{-1}(J)$.

Since these two maps are inverses of each other, this shows that there is a one-to-one correspondence between ideals of R containing I and ideals in R/I.

□

Proposition A.3. *Let R be a ring. The only ideals of R are $\{0\}$ and R if and only if R is a field.*

Proof. Suppose R is a field. Let I be an ideal in R.Suppose I contains a non-zero element a, then $a^{-1}a \in I$, i.e. $1 \in I$. Let x be any element in F, then $x \cdot 1 \in I$. Hence $I = R$.

Now suppose the only ideals of R are $\{0\}$ and R. Let r be a non-zero element in R and consider the set $\{cr : c \in R\}$. This is clearly an ideal which contains a non-zero element, hence this is equal to R. In particular, there exists $c \in R$ such that $cr = 1$. Hence every non-zero element in R contains a multiplicative inverse. This shows that R is a field. □

Theorem A.4. *Let R be a ring and M be a maximal ideal. Then R/M is a field.*

Proof. By A.2, The ideals of R/M correspond to the ideals in R containing M. Since M is a maximal ideal, the only ideals in R containing M are M and R. Hence the only ideals in R/M are $\{M\}$ and R/M (note that M is the zero element in R/M). Hence R/M is a field. □

Proposition A.5. *Let F be a field, $p(x) \in F[x]$ be an irreducible polynomial.*
Then $(p(x)) = \{f(x) \in F[x] : p(x)|f(x)\}$ is a maximal ideal.

Proof. Let I be an ideal containing $(p(x))$. Suppose it contains an element $f(x)$ not in $(p(x))$, then since $p(x)$ does not divide $f(x)$ and $p(x)$ is irreducible, we have that $hcf(f(x), p(x)) = 1$. Since $F[x]$ is an Euclidean domain, we know that there exists $a(x), b(x) \in F[x]$ such that $a(x)f(x) + b(x)p(x) = 1$. Since I is an ideal, it follows that $1 \in I$. Hence $I = F[x]$. □

Theorem A.6. *Let F be any field and $f(x) \in F[x]$. Then the splitting field of $f(x)$ always exists.*

Proof. We prove by induction on the degree of $f(x)$. If $\deg(f) = 1$, then F is the splitting field of $f(x)$. Suppose for every polynomial $g(x) \in F[x]$ where $deg(g(x)) \leq n - 1$, a splitting field for $g(x)$ exists. Let $\deg(f(x)) = n$. Suppose $f(x)$ does not factor completely into linear factors, then

there exists an irreducible factor $p(x)$ of degree at least 2. From A.5 and A.4, $E_1 := F[x]/(p(x))$ is a field. Note that by considering the canonical projection $\phi : F[x] \to F[x]/(p(x))$, i.e. $\phi(f(x)) = f(x) + (p(x))$, and restricting the domain to F, F can be viewed as a subfield of $F[x]/(p(x))$. Now let $\bar{x} = \phi(x)$. Then $p(\bar{x}) = \phi p(x) = 0$ in $F[x]/(p(x))$. Hence E_1 is a field containing $F[x]$ that contains a root of $p(x)$. Denoting this root by α, we see that $f(x) = (x-\alpha)p_1(x)$ in $E_1[x]$. By the inductive hypothesis, there exists a field E containing E_1 such that $f(x)$ factors completely into linear factors. Let K be the intersection of all subfields E_i of E containing F such that $f(x)$ factors completely into linear factors in E_i, then K is a splitting field of $f(x)$.

□

References

[1] Simeon Ball and Zsuzsa Weiner, *An introduction to finite geometry*, http://www-ma4.upc.es/∼simeon/IFG.pdf (accessed May 27, 2015) - page 9

[2] A. Heyting, *Axiomatic Projective Geometry - second edition*, North-Holland, Wolters-Noordhoff, (1980)

[3] Johan Kåhrström, *On Projective Planes*, Mid Sweden University http://kahrstrom.com/mathematics/documents/OnProjectivePlanes.pdf (accessed June 1, 2015)

[4] Danny Kalmanovich, *Finite Projective Planes*, http://www.math.bgu.ac.il/∼dannykal /research/fpp%20revised.pdf (accessed May 27, 2015) - pages 8-9

[5] Peter J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press - pages 141-143

[6] Albrecht Beutelspacher and Ute Rosenbaum, *Projective Geometry: From Foundations to Applications*, http://www.maths.ed.ac.uk/∼aar/papers/beutel.pdf (accessed June 1,2015)

[7] C.W.H. Lam, G. Kolesova and L. Thiel, *A computer search for finite projective planes of order 9*, http://ac.els-cdn.com/0012365X9190280F/1-s2.0-0012365X9190280F-main.pdf?_tid=a0202660-0874-11e5-b074-00000aacb35f&acdnat=1433173450_3af42e5f247ed30c8bd207b6048f9d8f (accessed June 1,2015)

[8] C. W. H. Lam and L. Thiel and S. Swiercz, *The Non-existence of Finite Projective Planes of Order 10*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.39.8684&rep=rep1&type=pdf (accessed June 5, 2015)

[9] K.Conrad, *Finite Fields*, http://www.math.uconn.edu/∼kconrad/blurbs/galoistheory/finitefields.pdf (accessed June 5,2015)

[10] R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canad. J. Math. 1(1949), 88-93

[11] *Wikipedia page on quaternions*, http://en.wikipedia.org/wiki/Quaternion (accessed June 7, 2015)

[12] D.Dummit and R.Foote, *Abstract Algebra - Third Edition*, John Wiley & Sons, (2004)