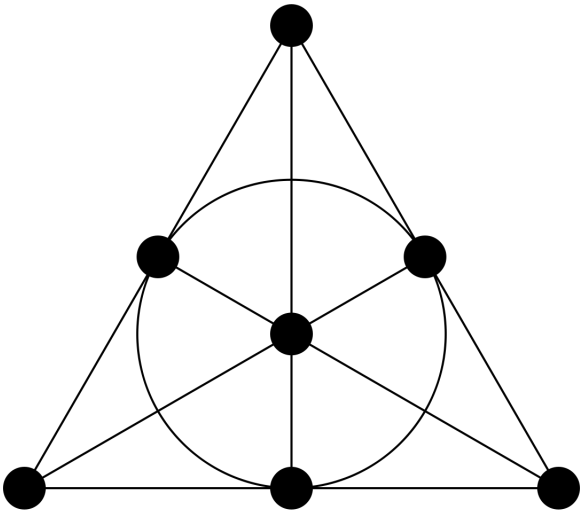
Imperial College
London

An Introduction to Finite Projective Planes



Group 28

Supervised by Dr Ambrus Pál

Abrunho, Jonathan	ja1416
Angdinata, David Kurniadi	dka316
Kim, Hyun Mog	hmk16
Pan, Yue	yp2415
Xing, Xuewei	xx1116

M2R
Second Year Mathematics Group Project
Department of Mathematics
Imperial College London
29 May 2018 - 20 June 2018

Contents

Preface

The aim of the project is to introduce the theory of finite projective planes of small orders to the reader. This is done by giving proofs of general propositions and widely-known theorems in the field without going into too much detail, as well as providing interesting side remarks throughout. The structure of the project is so as to fully explain the following table in an accessible order:

order	non-isomorphic planes
2	unique: Desarguesian
3	unique: Desarguesian
4	unique: Desarguesian
5	unique: Desarguesian
6	impossible (by Bruck-Ryser)
7	unique: Desarguesian
8	unique: Desarguesian
9	exactly 4: Φ, Ω, Ω^D, Ψ (by Lam, Kolesova, Thiel)
10	impossible (by Lam, Thiel, Scwierz)
11	at least 1: Desarguesian
12	unknown (conjectured to be impossible)
13	at least 1: Desarguesian
14	impossible (by Bruck-Ryser)

Chapter 1 introduces the axiomatic definition of projective planes and proves several elementary results derivable directly from the axioms. Chapter 2 discusses the existence and uniqueness of Desarguesian planes as well as some of its properties. Chapter 3 proves the non-existence of certain planes due to the Bruck-Ryser theorem and briefly touches on undiscovered planes of other orders. Chapter 4 justifies that there are in fact non-Desarguesian planes coordinatisable with quasi-fields that are not skew-fields. Each chapter has its own style of discussion, with the first chapter being geometric, the second chapter being algebraic, the third chapter being number theoretic, and the fourth chapter being a combination of all three.

An assumption is made that the reader has elementary background knowledge of a few algebraic structures, including definitions and properties of groups, rings, and modules. The flow of information throughout each chapter should be highly accessible and easily followed by undergraduates with relatively little experience in algebra. An attempt is made to link these new ideas to their past experiences.

Throughout the project, most sources of information were obtained from several library textbooks, but web resources were also used extensively for inaccessible articles of the past. The bibliography would contain most if not all of these sources, but some are explicitly mentioned in the text for direct references. All write-ups are done by the group unless otherwise stated.

We would like to thank our supervisor Dr Ambrus Pál for support and guidance, as well as clarifications of any doubts we had, throughout the project duration. Without him, this project would be an impossibility.

Chapter 1

Introduction

Informally, as in [32], a projective plane is a surface without boundary derived from a usual plane by addition of a line at infinity. Just as a straight line in projective geometry contains a single point at infinity at which the endpoints meet, a plane in projective geometry contains a single line at infinity at which the edges of the plane meet. A projective plane can be constructed by gluing both pairs of opposite edges of a rectangle together giving both pairs a half-twist. It is a one-sided surface, but cannot be realized in three-dimensional space without crossing itself.

1.1 Background

A more formal definition is as follows.

Definition (Projective plane)**.** A projective plane $\mathbb{P}$ is an ordered triple (P, L, I), where P is the **set of points** p of $\mathbb{P}$, L is the **set of lines** l of $\mathbb{P}$, and $I \subseteq P \times L$ is the **incidence relation** $(\cdot, \cdot)$ satisfying the following axioms:

(P1) for any two distinct points $p_1, p_2 \in P$, there is a unique line $l \in L$, such that $(p_1, l), (p_2, l) \in I$,

(P2) for any two distinct lines $l_1, l_2 \in L$, there is a unique point $p \in P$, such that $(p, l_1), (p, l_2) \in I$, and

(P3) there are four distinct points in P such that no line in L is incident with more than two of them.

$\mathbb{P}$ is said to be **finite** if the number of points in P is finite, otherwise it is said to be **infinite**. Intuitively, incidence relates points and lines in a familiar fashion, such that "points being incident with lines" can be interpreted as "points lying on lines" or as "lines passing through points". As such:

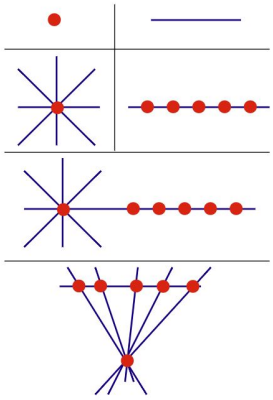
(P1) implies that a line can alternatively be defined as the unique edge joining any two points,

(P2) states that no lines are parallel to each other, and

(P3) rules out certain degenerate cases that are trivial or uninteresting.

These degenerate cases include two general families of degenerate planes as in [1]:

1. all projective planes $\mathbb{P} \equiv (P, L, I)$ with:
   (a) $P \equiv \{p_1, ..., p_n\}$ for some $n \in \mathbb{N}$,
   (b) $L \equiv \{l_1, ..., l_m\}$ for some $m \in \mathbb{N}$,
   (c) $I \equiv \{(p_i, l_1) \mid i \in \{1...n\}\} \cup \{(p_1, l_i) \mid i \in \{2...m\}\}$, and
2. all projective planes $\mathbb{P} \equiv (P, L, I)$ with:
   (a) $P \equiv \{p_1, ..., p_n\}$ for some $n \in \mathbb{N}$,
   (b) $L \equiv \{l_1, ..., l_n\}$ for the same n,
   (c) $I \equiv \{(p_i, l_1) \mid i \in \{2...n\}\}$
   $\cup \{(p_1, l_i) \mid i \in \{2...n\}\} \cup \{(p_i, l_i) \mid i \in \{2...n\}\}$.



Families of degenerate planes

They include trivial cases like empty points or empty lines, which do not have enough structure to be considered interesting. Although they are presented as finite cases, they can be naturally extended to infinite cases, and hence hold for infinite projective planes as well. For historical reasons, these are not considered projective planes in any discussion.

For convenience, an abuse of notation will be used in the rest of the project. Let $\mathbb{P} \equiv (P, L, I)$ be a projective plane. Then for any $p, p' \in P$ and any $l, l' \in L$:

- $P(l) \coloneqq \{p \in P \mid (p, l) \in I\}$,
- $L(p) \coloneqq \{l \in L \mid (p, l) \in I\}$,
- $l = p \cup p' \Leftrightarrow (p, l), (p', l) \in I$, and
- $p = l \cap l' \Leftrightarrow (p, l), (p, l') \in I$.

This allows for the three axioms to be redefined in a less cumbersome manner.

1.2 Properties

For this section, let $\mathbb{P} \equiv (P, L, I)$ be a finite projective plane, unless otherwise stated.

1.2.1 Duality

At first glance, it stands out that there is an inherent symmetry to the roles of points and lines in projective planes. In fact, exchanging their roles will still yield a valid definition of projective planes. This crucial notion is known as **duality**, as illustrated in the theorem below.

Theorem 1.2.1 (Principle of plane duality)**.** *Let S be a statement of projective planes directly proven from the three axioms P1, P2, and P3. Let S' be the statement derived directly from S by exchanging every instance of "point" with "line" and vice versa. Then S', called the **dual statement** to S, is still a valid statement of projective planes.*

However, axiom P3 presents a tiny subtlety, which needs to be justified in the following lemma.

Lemma 1.2.2. *There are four distinct lines in L such that no point in P is incident with more than two of them.*

Proof. Axiom P3 gives four distinct points $p_1, ..., p_4 \in P$, such that no line in L is incident with more than two of them. Set the distinct lines as $l_1 = p_1 \cup p_2$, $l_2 = p_2 \cup p_3$, $l_3 = p_3 \cup p_4$, and $l_4 = p_4 \cup p_1$. Clearly all points are incident with exactly two of these lines. Axiom P2 gives two additional distinct points $p_5 = l_1 \cap l_3$ and $p_6 = l_2 \cap l_4$. Clearly they are also incident with exactly two of these lines. Thus no points in P are incident with more than two of these four lines. □

The proof of the lemma introduces two fundamental substructures in any projective plane.

Definition (Quadrangle)**.** A **quadrangle** is any four distinct points in P that satisfies axiom P3.

Definition (Quadilateral)**.** A **quadilateral** is any four distinct lines in L that satisfies Lemma 1.2.2.

The proof of the theorem is then trivial by the lemma.

Proof (of Theorem 1.2.1). It is sufficient to show that the three axioms P1, P2, and P3 imply the three derived dual axioms Q1, Q2, and Q3. Clearly P1 and P2 are dual axioms, so Q1 $\Leftrightarrow$ P2 and Q2 $\Leftrightarrow$ P1. Lemma 1.2.2 shows that Q3 can be derived from P1, P2, and P3. □

Applying this exchange to a particular finite projective plane will indeed result in a related valid finite projective plane, albeit labelled differently.

Definition (Dual plane)**.** The **dual plane** of $\mathbb{P}$, derived directly from $\mathbb{P}$ by exchanging every instance of "point" with "line" and vice versa, is a finite projective plane $\mathbb{P}^D := (L, P, I^*)$, where $I^* = \{(l, p) \mid (p, l) \in I\} \subseteq L \times P$ is the inverse relation of I.

This exchange will be named appropriately for the sake of brevity.

Definition (Plane duality)**.** A **plane duality** is a map transforming $\mathbb{P}$ to its dual plane $\mathbb{P}^D$.

1.2.2 Order

Now it is worth noting that the number of points and lines of any projective plane are restricted by a lower bound. This is a direct consequence of the previous section ruling out trivial cases.

Proposition 1.2.3. *$|P| \geq 7$ and $|L| \geq 7$.*

Proof. Axiom P3 gives four points in the quadrangle, of which must be pairwise incident to a unique line by P2. A simple combinatorial argument gives $|L| \geq \binom{4}{2} = 6$. Out of the $\binom{6}{2} = 15$ pairs of these lines, three pairs are not yet incident to a unique point. Axiom P2 assigns three points to these, so with the initial four points, we have $|P| \geq 4 + 3 = 7$. A similar dual argument shows that $|L| \geq 7$ as well. □

The three points not in the initial quadrangle are given names for easy reference.

Definition (Diagonal point)**.** A **diagonal point** is any one of the three additional points in $\mathbb{P}$ not in the quadrangle in Proposition 1.2.3.

It is entirely possible that the simplest finite projective plane has exactly 7 points and 7 lines, which will be explored in the next chapter. For now, it can be seen that points and lines are heavily related.

Proposition 1.2.4. *There is a unique $n \in \mathbb{N}_{\geq 2}$ such that:*

(i) for any line $l \in L$, we have $|P(l)| = n + 1$, and

(ii) for any point $p \in P$, we have $|L(p)| = n + 1$.

Two lemmas will be introduced to prove this more succinctly.

Lemma 1.2.5. *Let $p \in P$ be a point and $l \in L$ be a line. Then:*

1. *$|P(l)| \geq 3$, and*
2. *$|L(p)| \geq 3$.*

Proof. Check both parts.

1. Axiom P3 gives four points $p_1, ..., p_4 \in P$ in the quadrangle. For any line $l \in L$, assume without loss of generality that $p_1, p_2 \notin P(l)$. Axiom P1 gives unique distinct lines $l_1 = p_2 \cup p_3$, $l_2 = p_1 \cup p_3$, and $l_3 = p_1 \cup p_2$. Axiom P2 gives three distinct unique points $q_i = l \cap l_i$, so $|P(l)| \geq 3$.

2. A similar dual argument shows that $|L(p)| \geq 3$ for any point $p \in P$ as well.

□

Lemma 1.2.6. *For any point $p \in P$, there is a line $l \in L$ such that $p \notin P(l)$.*

Proof. Fix a point $p \in P$. Lemma 1.2.5 gives a line $l \in L(p)$, a second distinct point $p' \in P(l)$, and a second distinct line $l' \in L(p')$. By axiom P2, since l is uniquely incident to p and p', it must be that $p \notin P(l')$. □

The proof, albeit slightly longer, follows easily from the axioms and previous lemmas.

Proof (of Proposition 1.2.4). Proof adopted from [23].

(i) Fix two distinct lines $l, l' \in L$, which is possible by Proposition 1.2.3, which has a unique point $p = l \cap l'$ by axiom P2. Lemma 1.2.5 gives a third distinct line $l'' \in L(p)$ and a second distinct point $p' \in P(l'')$. Now assume $P(l) = \{p, q_1, ..., q_m\}$, which is possible by Lemma 1.2.5. Axiom P1 gives unique distinct lines $m_i = p' \cup q_i$. Axiom P2 gives unique distinct points $q_i' = l' \cap m_i$. Hence $p, q_1', ..., q_m' \in P(l')$, such that $|P(l')| \geq m + 1 = |P(l)|$. Swapping the roles of l and l' shows that $|P(l)| \geq m + 1 = |P(l')|$, so that $|P(l)| = m + 1 = |P(l')|$. Now set $n \coloneqq m$.

(ii) Fix a point $p \in P$. By Lemma lemma:otherline, there is a line $l \in L$ such that $p \notin P(l)$. Now assume $P(l) = \{p_1, ..., p_{n+1}\}$. Axiom P1 gives unique distinct lines $l_i = p \cup p_i$, so $|L(p)| \geq n + 1$. ↯ Suppose there is another distinct line $l' \in L(p)$. Axiom P2 gives a unique distinct point $p'' = l \cap l'$, so $p'' \in P(l)$. ↯ Thus indeed $|L(p)| = n + 1$.

□

This strong relation between points and lines allows the order, the most important property of a finite projective plane, to be defined.

Definition (Order)**.** An **order** of a finite projective plane is the unique $n \in \mathbb{N}_{\geq 2}$ satisfying Proposition 1.2.4.

A combinatorial argument arising from this yields the equivalence between the number of points and lines of any finite projective plane.

Corollary 1.2.7. *Let $\mathbb{P}$ be of order n. Then $|P| = |L| = n^2 + n + 1$.*

Proof. Proof adopted from [22].
Assume $\mathbb{P}$ has order n, and fix a point $p \in P$. Proposition 1.2.4 gives $|L(p)| = n+1$, and $|P(l)| = n+1$ for any line $l \in L(p)$, so $|P(l) \backslash \{p\}| = n$. Since the points and lines are distinct, we have $|P| \geq n(n+1)+1 = n^2+n+1$. ↯ Suppose there is another distinct point $p' \in P$. Axiom P2 gives a unique distinct line $l' = p \cup p'$, so $l' \in L(p)$. ↯ Thus indeed $|P| = n^2 + n + 1$. A similar dual argument shows that $|L| = n^2 + n + 1$ as well. □

1.2.3 Isomorphism

With order being defined, it can be said that plane duality does preserve order. However, despite the similarity of roles between points and lines, it is not the case that plane duality necessarily preserves the structure of the plane. In other words, duality applies to the theory of projective planes but not the individual projective planes. As with any algebraic or geometric structure, it is useful to define a notion of isomorphism between projective planes for this purpose.

Definition (Isomorphism)**.** Let $\mathbb{P}_1 \equiv (P_1, L_1, I_1)$ and $\mathbb{P}_2 \equiv (P_2, L_2, I_2)$ be two projective planes. An **isomorphism** from $\mathbb{P}_1$ to $\mathbb{P}_2$ is an ordered pair of bijections (π, λ), where $\pi : P_1 \to P_2$ and $\lambda : L_1 \to L_2$, such that for all $(p, l) \in I_1$, we have $(\pi(p), \lambda(l)) \in I_2$. $\mathbb{P}_1$ is said to be **isomorphic** to $\mathbb{P}_2$, denoted by $\mathbb{P}_1 \cong \mathbb{P}_2$, if there exists an isomorphism from $\mathbb{P}_1$ to $\mathbb{P}_2$. Otherwise $\mathbb{P}_1$ is said to be **non-isomorphic** to $\mathbb{P}_2$, denoted by $\mathbb{P}_1 \ncong \mathbb{P}_2$.

Remark. The isomorphism relation $\cong$ between finite projective planes is an equivalence relation. This is a trivial result from realising that the identity isomorphism imply reflexivity, inverse isomorphisms imply symmetry, and bijective composition of isomorphisms imply transitivity.

Isomorphic finite projective planes are hence considered structurally equivalent and are virtually indistinguishable from each other. A common notion among isomorphisms is to consider the isomorphisms from a plane to itself.

Definition (Automorphism)**.** Let $\mathbb{P} \equiv (P, L, I)$ be a finite projective plane. An **automorphism** ϕ of $\mathbb{P}$ is an isomorphism from $\mathbb{P}$ to itself.

The set of all automorphisms and their relation to each other also forms a group.

Definition (Automorphism Group)**.** Let $\mathbb{P}$ be a finite projective plane. The **automorphism group** of $\mathbb{P}$, denoted by $Aut(\mathbb{P})$, is a group $(S(\mathbb{P}), \circ)$, where $S(\mathbb{P})$ is the set of all automorphisms of a projective plane $\mathbb{P}$, and $\circ$ is the composition operation between automorphisms.

It is tempting to say that plane duality is isomorphism-invariant, but this is only restricted to a class of planes which have a certain property.

Definition (Self-dual)**.** Let $\mathbb{P}^D$ be the dual plane of $\mathbb{P}$. If $\mathbb{P} \cong \mathbb{P}^D$, then $\mathbb{P}$ is said to be **self-dual**.

Most finite projective planes are not self-dual, but a class of planes known as Desarguesian planes are always self-dual, provided they are finite. Indeed, when considering the planes of order 9, there are exactly four non-isomorphic finite projective planes, of which two are self-dual and the other two being duals of each other. However, it is also a known fact that there is exactly one unique plane of, say, order 3, yet there are no planes of, say, order 6. The mere subtlety in the number of non-isomorphic finite projective planes of each order is interesting in its own way, that it has become a subject of great interest for mathematicians. Many results have been proved, including the fact that there must exist a plane for certain orders but not other orders. However, the classification of all finite projective planes is still far from complete. For instance, it still remains an open problem whether there exists a plane of order 12. All these facts will be heavily justified in the next few chapters.

Chapter 2

Existence of planes of special orders

For this chapter, denote $(x, y, z)^T$ as xyz, for ease of notation.

2.1 The projective plane of order 2 (Fano plane)

Prior to this chapter, there has yet been a discussion or even an example of a particular finite projective plane, which might lead one to question if they truly exist, especially due to the unfamiliar axioms proposed. This chapter assures the existence of these planes implicitly by providing proofs.

2.1.1 Construction

Due to Proposition 1.2.3, if a finite projective plane exists, it must have at least seven points and seven lines. With the properties of order in Proposition 1.2.7, it is clear that a plane of order 1, which would theoretically have three points and three lines, cannot possibly exist. Hence the smallest plane would need to be of order at least 2, which would have exactly seven points and seven lines. Indeed, **a plane of order 2 exists**, as illustrated in the following informal construction.

Example. Let $\mathbb{P} \equiv (P, L, I)$ be labelled such that:

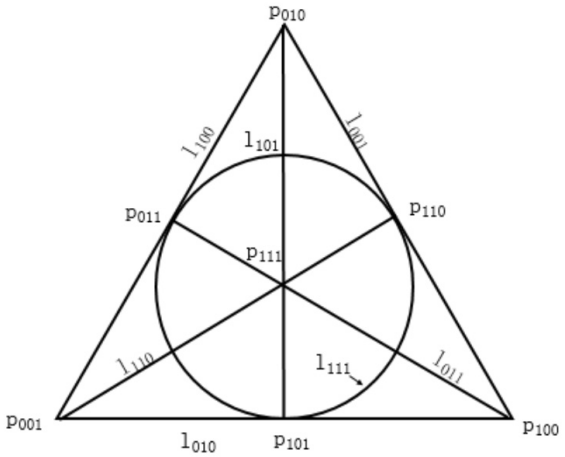
$$P \coloneqq \{p_{001}, p_{010}, p_{011}, p_{100}, p_{101}, p_{110}, p_{111}\},$$

$$L \coloneqq \{l_{001}, l_{010}, l_{011}, l_{100}, l_{101}, l_{110}, l_{111}\},$$

and the incidence relation as

$$\begin{aligned} I \coloneqq \{&(p_{001}, l_{010}), (p_{001}, l_{100}), (p_{001}, l_{110}),\\ &(p_{010}, l_{001}), (p_{010}, l_{100}), (p_{010}, l_{101}),\\ &(p_{011}, l_{011}), (p_{011}, l_{100}), (p_{011}, l_{111}),\\ &(p_{100}, l_{001}), (p_{100}, l_{010}), (p_{100}, l_{011}),\\ &(p_{101}, l_{010}), (p_{101}, l_{101}), (p_{101}, l_{111}),\\ &(p_{110}, l_{001}), (p_{110}, l_{110}), (p_{110}, l_{111}),\\ &(p_{111}, l_{011}), (p_{111}, l_{101}), (p_{111}, l_{110})\}, \end{aligned}$$

as seen in the diagram below. A simple verification shows that this is indeed a projective plane. It is labelled in this fashion using binary representations of $1, ..., 7$ for many pedantic reasons. They will be made clear over later sections and chapters, which will periodically refer back to this explicit construction as an example.



Projective plane of order 2

This notation, despite being very explicit, is clearly extremely cumbersome, especially if used on finite projective planes of higher orders, if they exist. An alternative algebraic construction representing the same plane would be useful, and would possibly generalise better. The following proposition presents exactly this and a proof that it is indeed a finite projective plane.

Proposition 2.1.1. *Let V be a three-dimensional vector space over the finite field $\mathbb{F}_2$, and let:*

1. $P \coloneqq \{p_n \mid n \in V\}$,
2. $L \coloneqq \{l_m \mid m \in V\}$, *and*
3. $I \coloneqq \{(p_n, l_m) \mid p_n \in P, l_m \in L, \langle n, m\rangle = 0\}$.

Then $\mathbb{P} \coloneqq (P, L, I)$ is a finite projective plane of order 2 as constructed above.

Proof. It is sufficient to check the three axioms of projective planes.

1. For any two distinct points $p_n, p_m \in P$, the line $l_{n+m} = p_n \cup p_m$ is unique.
2. For any two distinct lines $l_n, l_m \in L$, the point $p_{n+m} = l_n \cap l_m$ is unique.
3. The four distinct points $p_{001}, p_{010}, p_{100}, p_{111} \in P$ are such that no line in L is incident with more than two of them.

A simple verification shows that the above indeed holds for all points and lines. □

2.1.2 Uniqueness

An informal way of constructing a finite projective plane of order 2 could be to argue axiomatically as in [23]. Restricted by a lower bound of seven points and seven lines, a diagram of a plane equivalent to the plane constructed above will be drawn inevitably. This suggests that it the plane in question may be unique up to isomorphism and order, as illustrated in the following proposition.

Proposition 2.1.2. *Let $\mathbb{P}$ and $\mathbb{P}'$ be two finite projective planes of order 2. Then $\mathbb{P} \cong \mathbb{P}'$.*

Proof. It is sufficient to show that there is an isomorphism from any finite projective plane $\mathbb{P} \equiv (P, L, I)$ of order 2 to the plane $\mathbb{P}' \equiv (P', L', I')$ constructed in Proposition 2.1.1.
Corollary 1.2.7 gives $|P| = |L| = 2^2 + 2 + 1 = 7$, so let $p_1, ..., p_7 \in P$ and $l_1, ..., l_7 \in L$. Axiom P3 gives a quadrangle, which can be labelled as p_1, p_2, p_4, p_7. Proposition 1.2.3 gives six explicit lines, each unique to a pair of points in the quadrangle, which can be labelled as $l_1 = p_2 \cup p_4$, $l_2 = p_1 \cup p_4$, $l_3 = p_4 \cup p_7$, $l_4 = p_1 \cup p_2$,

$l_5 = p_2 \cup p_7$, and $l_6 = p_1 \cup p_7$. There are also three additional diagonal points, which can be labelled as $p_3 = l_3 \cap l_4$, $p_5 = l_2 \cap l_5$, and $p_6 = l_1 \cap l_6$. By this labelling, Proposition 1.2.4 holds for all lines and all points in the quadrangle, but not for any diagonal point. It is easy to see that only $(p_3, l_7), (p_5, l_7), (p_6, l_7) \in I$ will make Proposition 1.2.4 hold for diagonal points.
Let V be the vector space over $\mathbb{F}_2$ representing $\mathbb{P}'$. Now let $\pi : P \to P'$ and $\lambda : L \to L'$ be such that $\pi(p_n) = p_{n'}$ and $\lambda(l_m) = l_{m'}$, where n' and m' are the binary representations in V of n and m respectively, such that $\beta(1) = 001$, $\beta(2) = 010$, $\beta(4) = 100$, etc. Then π and λ are clear bijections. It is also simple to verify that indeed $\langle p_{n'}, l_{m'} \rangle = 0$ for all points $p_n \in P$ and all lines $l_m \in L$ such that $(p_n, l_m) \in I$. Thus $\phi \coloneqq (\pi, \lambda)$ is an isomorphism. □

Indeed, **the finite projective plane of order 2 is unique**. This particular plane is of such historical and mathematical importance that it was entitled a name after the Italian mathematician G Fano for his massive contributions to finite geometry.

Definition (Fano plane)**.** The **Fano plane** is the unique finite projective plane of order 2.

The Fano plane is indeed the smallest non-trivial finite projective plane, having an automorphism group of 168 elements. This particular group is the projective special linear group $PSL(2, 7)$, which is in fact the second smallest non-abelian finite simple group, only to be preceeded by the alternating group A_5.

2.2 Desarguesian planes of prime power order

As per the previous section, the plane of order 2 does indeed exist. In the previous chapter, albeit briefly as a remark, it was mentioned that the plane of order 3 exists, but a plane of order 6 does not. These curious facts suggest that there may be a pattern among "valid" orders, which is the case, as illustrated in the following theorem.

Theorem 2.2.1. *Let $n \in \mathbb{N}$ be a **prime power**, so that $n = p^q$ for $q \in \mathbb{N}$ and prime $p \in \mathbb{N}$. Then there exists a finite projective plane of order n.*

2.2.1 Skew-fields

The proof of this theorem relies on an alternate representation of a finite projective plane with algebraic methods. In particular, linear algebra in the form of modules, which are vector spaces generalised to arbitrary rings, over a field-like structure will be used in the construction of a projective plane. For this purpose, the ring structure required will be defined as follows.

Definition (Skew-field)**.** A **skew-field** is a ring $(R, +, \cdot, 0, 1)$, where for all $r \in R \setminus \{0\}$, there is a unique $s \in R \setminus \{0\}$ such that $r \cdot s = s \cdot r = 1$.

It is clear, both in definition and nomenclature, that all fields are skew-fields, and that skew-fields differ from fields only in that commutativity of the multiplication operation is not required. However, as the scope of discussion is limited to finite projective planes, only finite skew-fields will be considered, leading directly to the following well-known theorem.

Theorem 2.2.2 (Wedderburn's little theorem)**.** *Let F be a finite skew-field. Then F is a finite field.*

Proof. Omitted, see [2]. □

This amazing result implies that modules over finite skew-fields are equivalent to vector spaces over finite fields, and that all properties of finite fields, such as necessarily having orders equal to prime powers, are inherited. As such, using the term "vector space over finite skew-field" is clear by context.

2.2.2 Homogeneous coordinates

The construction of the projective plane is then similar to Proposition 2.1.1, but it will be presented with the standard method of construction known as **homogeneous coordinates**. This is done by considering a three-dimensional vector space over a finite skew-field, then defining points as one-dimensional linear subspaces, lines as two-dimensional linear subspaces, and incidence as orthogonality. A more concrete statement is as follows.

Proposition 2.2.3. *Let V be a three-dimensional vector space over a finite skew-field F, and let $V^* \coloneqq V \setminus \{000\}$ and $F^* \coloneqq F \setminus \{0\}$. For any $v \in V^*$, let the equivalence class of all scalar multiples be $[v] \coloneqq \{\lambda v \mid \lambda \in F^*\}$ and let the set of all equivalence classes be $V^*/F^* \coloneqq \{[v] | v \in V^*\}$. Now let:*

1. $P \coloneqq \{p_{[v]} \mid [v] \in V^*/F^*\}$,
2. $L \coloneqq \{l_{[v]} \mid [v] \in V^*/F^*\}$, *and*
3. $I \coloneqq \{(p_{[n]}, l_{[m]}) \mid p_{[n]} \in P, l_{[m]} \in L, \langle n, m\rangle = 0\}$.

*Then $\mathbb{P}(F) \coloneqq (P, L, I)$ is a finite projective plane, **coordinatised** by V and F.*

Remark. It is clear that points in P are indeed one-dimensional linear subspaces. Lines in L are also two-dimensional linear subspaces, as each two-dimensional subspace can be uniquely represented by its normal line.

Proof. Proof adopted from [23].
Let V be a vector space over a finite skew-field F. Theorem 2.2.2 says that V is a vector space over a finite field F. Again, the three axioms of projective planes will be checked.

1. For any two distinct points $p_{[n]}, p_{[m]} \in P$, we have that n and m are distinct up to scalar multiples, so that $rank(n, m) = 2$. Then if $n \equiv n_1n_2n_3$ and $m \equiv m_1m_2m_3$, there is a unique $v \coloneqq v_1v_2v_3 \in V^*$ such that for all $\lambda \in F^*$,
$$\begin{pmatrix} n_1 & n_2 & n_3 \\ m_1 & m_2 & m_3 \end{pmatrix} \left(\lambda \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
. Thus $[v] \coloneqq \{\lambda v \mid \lambda \in F^*\}$ is the unique equivalence class for the line $l_{[v]} = p_{[n]} \cup p_{[m]}$.
2. For any two distinct lines $l_{[n]}, l_{[m]} \in L$, it can be shown similarly that there is a unique $v \in V^*$ such that $[v] = \{\lambda v \mid \lambda \in F^*\}$ is the unique equivalence class for the point $p_{[v]} = l_{[n]} \cap l_{[m]}$.
3. Since $0, 1 \in F$, we have $001, 010, 100, 111 \in V^*$. Then the four distinct points $p_{[001]}, p_{[010]}, p_{[100]}, p_{[111]} \in P$ are such that no line in L is incident with more than two of them.

□

The construction of the Fano plane can now be restated as in the following example.

Example. Let V be a three-dimensional vector space over the finite skew-field $\mathbb{F}_2 \equiv \{0, 1\}$, and let P, L, and I be as in Proposition 2.2.3. Then $\mathbb{P} \equiv (P, L, I)$ is the Fano plane.

With this identification, it is then trivial to prove Theorem 2.2.1.

Proof (of Theorem 2.2.1). Theorem 2.2.2 says that V is a vector space over the finite field F. Then $|F| = n$, where n is a prime power. By Proposition 2.2.3, this coordinatises a finite projective plane $\mathbb{P}(F) \equiv (P, L, I)$. Now fix a two-dimensional vector subspace $W \subset V$, defined to be a line $l \in L$. A simple combinatorial argument gives $|W| = n^2$, such that there are $n^2 - 1$ distinct one-dimensional non-zero vectors. There are also $n - 1$ distinct bases for one-dimensional vector subspaces $U \subset W$. Thus, there are $\frac{n^2-1}{n-1} = n + 1$ distinct one-dimensional vector subspaces U, defined to be points $p \in P$, such that $|P(l)| = n+1$. Thus the definition of order defined in Proposition 1.2.4 says $\mathbb{P}(F)$ has order n. □

Indeed, for every prime power, there is a finite projective plane of that order, which immediately establishes the existence of countably infinite planes.

Remark. For an explicit list of "valid" orders less than a fixed small order, an easy way is to simply loop across primes and exponentiate them with natural numbers, leading to the sequence A246655 on the Online Encyclopaedia of Integer Sequences (OEIS) [18] (2, 3, 4, 5, 7, 8, 9, 11, 13, ...). Note that 6, 10, and 12 are missing from this list for reasons that will be discussed in the next chapter. All known finite projective planes have orders in this list, and it is currently an open problem if there exists a finite projective plane of order not in this list.

The class of all projective planes constructed by this method was named after the French mathematician G Desargues, one of the founders of projective geometry.

Definition (Desarguesian plane)**.** A finite **Desarguesian plane** of order n is a finite projective plane of order n constructed as in Proposition 2.2.3. If a finite projective plane cannot be constructed as in Proposition 2.2.3, it is said to be **non-Desarguesian**.

Remark. It is easy to see that any Desarguesian plane is self-dual due to its inherent symmetry.

As a side note, infinite Desarguesian planes can be naturally extended by considering infinite skew-fields rather than finite ones. In this case, vector spatial properties are not inherited, as infinite skew-fields are not necessarily fields by Theorem 2.2.2. However, attempting to consider vector spaces over fields directly in the construction leads to another class of projective planes, named after Pappus of Alexandria, as follows.

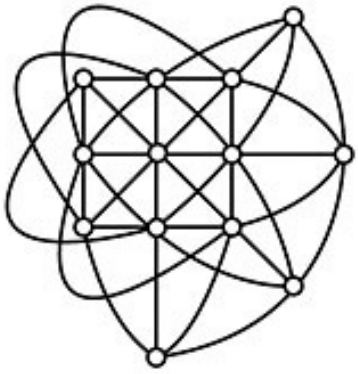
Definition (Pappian plane)**.** A **Pappian plane**, also known as a **field plane**, is a Desarguesian plane constructed over fields rather than skew-fields. A finite Pappian plane is also called a **Galois plane**.

All finite Pappian planes are clearly Desarguesian planes and vice versa, but infinite Desarguesian planes constructed over certain infinite skew-fields, such as the quaternions, are not Pappian planes.

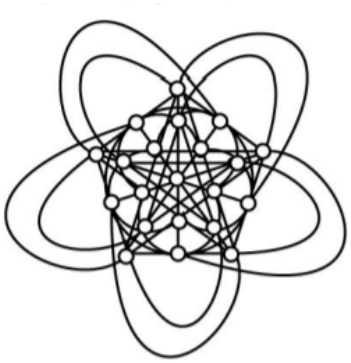
Remark. Most textbooks define Desarguesian planes and Pappian planes as projective planes that satisfy **Desargues's theorem** and **Pappus's theorem** respectively, then deriving an equivalence with these methods of construction afterwards.

2.2.3 Other Desarguesian planes

As mentioned above every finite projective plane of order 2 is isomorphic to the Fano plane, but this does not hold in general. In other words, for a given prime power order, there may be other planes that are non-isomorphic to their corresponding Desarguesian plane. This was highlighted briefly in the previous chapter in the case of order 9, which is indeed the lowest order for a non-Desarguesian plane. In fact, **each of the planes of order 3, 4, 5, 7, and 8 is unique up to isomorphism**. The unique planes of order 3 and 4 are illustrated below.



Projective plane of order 3



Projective plane of order 4

The proofs for each of these are lengthy and not generalised easily, and as such will be omitted for the sake of further discussion. As the order of a finite projective plane increases, the current approach makes it clear that the complexity of the proof of its uniqueness increases rapidly. For instance, the plane of order 8 was proven to be unique in [19], after checking over a hundred cases of structures by hand. At the present, is still unknown if finite projective planes of a general valid order higher than 9, such as order 11, is unique.

2.3 Incidences of planes of small orders

As demonstrated in previous sections, a linear algebraic construction of finite projective planes is sufficient to imply their existence. However, this method of construction is not easily visualised due to the definition of incidence, so a semi-pictorial approach is taken to increase geometrical intuition.

2.3.1 Examples

An incidence matrix, defined below, is an explicit representation of a finite projective plane.

Definition (Incidence matrix)**.** An **incidence matrix** of a finite projective plane $\mathbb{P} \equiv (P, L, I)$ of order n, with $m \coloneqq |P| = |L| = n^2 + n + 1$, where $P \equiv \{p_1, ..., p_m\}$ and $L \equiv \{l_1, ..., l_m\}$, is a square matrix $A \in \mathbb{F}_2^{m \times m}$, such that for all $i, j \in \{1, ..., m\}$:

$$A_{ij} = \begin{cases} 1 & (p_i, l_j) \in I \\ 0 & (p_i, l_j) \notin I \end{cases}.$$

For the rest of this section, let $\mathbb{P}$ be a finite projective plane of order n with $m \coloneqq n^2 + n + 1$, and let $A \in \mathbb{F}_2^{m \times m}$ be an incidence matrix of $\mathbb{P}$.

Incidence matrices provide an explicit but exact way of describing the incidence relation of a finite projective plane, so as to be reproduced easily. The following example constructs the incidence matrix for the Fano plane constructed in Proposition 2.1.1.

Example. $A \in \mathbb{F}_2^{7 \times 7}$

	p_{001}	p_{010}	p_{011}	p_{100}	p_{101}	p_{110}	p_{111}
l_{001}	0	1	0	1	0	1	0
l_{010}	1	0	0	1	1	0	0
l_{011}	0	0	1	1	0	0	1
l_{100}	1	1	1	0	0	0	0
l_{101}	0	1	0	0	1	0	1
l_{110}	1	0	0	0	0	1	1
l_{111}	0	0	1	0	1	1	0

It is also immediately obvious that incidence matrices are not unique in the sense that the points and lines are arbitrarily labelled. There are several canonical forms of these matrices for Desarguesian planes, such as the Paige-Wexler normal form in [17], constructed by L J Paige and C Wexler. The following example constructs this canonical form for the unique finite projective plane of order 3, labelling the points as $p_1, ..., p_{13}$ and the lines as $l_1, ..., l_{13}$.

Example. $A \in \mathbb{F}_2^{13 \times 13}$

	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8	l_9	l_{10}	l_{11}	l_{12}	l_{13}
p_1	1	1	1	1	0	0	0	0	0	0	0	0	0
p_2	1	0	0	0	1	1	1	0	0	0	0	0	0
p_3	1	0	0	0	0	0	0	1	1	1	0	0	0
p_4	1	0	0	0	0	0	0	0	0	0	1	1	1
p_5	0	1	0	0	1	0	0	1	0	0	1	0	0
p_6	0	1	0	0	0	1	0	0	1	0	0	1	0
p_7	0	1	0	0	0	0	1	0	0	1	0	0	1
p_8	0	0	1	0	1	0	0	0	1	0	0	0	1
p_9	0	0	1	0	0	1	0	0	0	1	1	0	0
p_{10}	0	0	1	0	0	0	1	1	0	0	0	1	0
p_{11}	0	0	0	1	1	0	0	0	0	1	0	1	0
p_{12}	0	0	0	1	0	1	0	1	0	0	0	0	1
p_{13}	0	0	0	1	0	0	1	0	1	0	1	0	0

Incidence matrices of finite projective planes of higher orders will not be explicitly shown due to their size, but their constructions are simple routines provided their incidence relation sets are fully known.

2.3.2 Properties

Now incidence matrices are clearly not symmetric, but they do have interesting properties worth investigating. Several propositions will be presented for this, as follows.

Proposition 2.3.1. *For any row A_i and any column A_j in A:*

$$\langle A_i, A_j \rangle = \begin{cases} n+1 & i = j \\ 1 & i \neq j \end{cases}.$$

Proof. If $i \neq j$, since two lines are incident with a unique point, there is only one unique $1 \leq k \leq m$, such that $A_{ik} = A_{jk} = 1$, thus $\langle A_i, A_j \rangle = 1$. Otherwise if $i = j$, since $|P(l)| = n+1$, there are distinct $1 \leq k_1, ..., k_{n+1} \leq m$, such that $A_{ik} = A_{jk} = 1$, thus $\langle A_i, A_j \rangle = n+1$. □

Proposition 2.3.2. *It holds that $AA^T = nI_m + J_m$, where $I_m \in \mathbb{F}_2^{m \times m}$ is the identity matrix and $J_m \in \mathbb{F}_2^{m \times m}$ is the matrix with entries all 1.*

Proof. Clearly $[AA^T]_{ij} = \langle A_i, A_j \rangle$, which is given by Proposition 2.3.1 as:

$$[AA^T]_{ij} = \begin{cases} n+1 & i = j \\ 1 & i \neq j \end{cases}.$$

This is exactly $AA^T = nI_m + J_m$ as required. □

Proposition 2.3.3. *The determinant $det(A) = \pm(n+1)n^{\frac{n^2+n}{2}}$.*

Proof. Proof adopted from [15].
By properties of determinants, we have $det(AA^T) = det(A)det(A^T) = det(A)^2 \geq 0$. As adding scalar multiples of rows to rows and columns to columns preserve the absolute value of the determinant, subtracting the first row from all other rows and then adding all other columns to the first column gives, by Proposition 2.3.2:

$$\left|det(AA^T)\right| = \begin{vmatrix} n+1 & 1 & \dots & 1 & 1 \\ 1 & n+1 & \dots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & n+1 & 1 \\ 1 & 1 & \dots & 1 & n+1 \end{vmatrix} = \begin{vmatrix} n+1 & 1 & \dots & 1 & 1 \\ -n & n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -n & 0 & \dots & n & 0 \\ -n & 0 & \dots & 0 & n \end{vmatrix} = \begin{vmatrix} (n+1)^2 & 1 & \dots & 1 & 1 \\ 0 & n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & n & 0 \\ 0 & 0 & \dots & 0 & n \end{vmatrix}.$$

This is upper diagonal with all diagonal elements positive, hence giving $det(AA^T) = (n+1)^2 n^{n^2+n}$. Thus $det(A) = \pm(n+1)n^{\frac{n^2+n}{2}}$. □

These properties can easily be verified for the two examples given above.

Chapter 3

Non-existence of planes of certain orders

The previous chapter has made it clear that finite projective planes do actually exist, and that there is an entire class of countably infinite planes. Again, one might suspect, based on this fact and the lack of proof for "invalid" orders, that there are planes of any order. This chapter attempts to prove that there are certain orders for which, if a plane should exist, it would lead to a contradiction, and hence cannot possibly exist.

3.1 Ruling out planes of invalid orders

As a start, **a plane of order 6 does not exist**. This has been historically proven in several ways, such as being an indirect result stemming from the separate work of G Tarry in [27] and R C Bose in [3]. The slick method discussed here will be through the Bruck-Ryser theorem for projective planes, which in turn generalises another class of orders for which planes cannot exist. This theorem, proven earlier as a special case of the more general Bruck-Ryser-Chowla theorem in combinatorics named after R H Bruck, H J Ryser, and S D S Chowla, is illustrated as follows.

Theorem 3.1.1 (Bruck-Ryser theorem)**.** *Let $n \in \mathbb{N}$ be such that:*

1. *$n \equiv 1 \mod 4$ or $n \equiv 2 \mod 4$, and*
2. *there are no $a, b \in \mathbb{N}$ such that $n = a^2 + b^2$.*

Then there are no finite projective planes of order n.

3.1.1 Lagrange's four square theorem

The theorem hinges on several fundamental ideas in number theory, which will be formulated in this section. The first of which is Lagrange's four square theorem, stated as follows.

Theorem 3.1.2 (Lagrange's four square theorem)**.** *Let $n \in \mathbb{N}$. Then there are $a, b, c, d \in \mathbb{N}$ such that $n = a^2 + b^2 + c^2 + d^2$, called a* ***sum of four squares****.*

The proof of this theorem requires several elementary but important lemmas introduced below.

Lemma 3.1.3 (Euler's four square identity)**.** *Let $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}$. Then:*

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \quad & (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 \\ & + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ & + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 \\ & + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.\end{aligned}$$

Proof. Indeed:

$$\begin{aligned} RHS = &\quad (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 \\ &+ (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &+ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 \\ &+ (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2 \\ = &\quad a_1^2b_1^2 + a_2^2b_2^2 + a_3^2b_3^2 + a_4^2b_4^2 \\ &+ a_1^2b_2^2 + a_2^2b_1^2 + a_3^2b_4^2 + a_4^2b_3^2 \\ &+ a_1^2b_3^2 + a_2^2b_4^2 + a_3^2b_1^2 + a_4^2b_2^2 \\ &+ a_1^2b_4^2 + a_2^2b_3^2 + a_3^2b_2^2 + a_4^2b_1^2 \\ = &\quad (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ = &\quad LHS. \end{aligned}$$

□

Lemma 3.1.4. *Let $n \in \mathbb{N}$ be even. Then $\frac{n}{2}$ is a sum of four squares.*

Proof. Fix an even $n \in \mathbb{N}$. Theorem 3.1.2 gives that $n = a^2 + b^2 + c^2 + d^2$ for some $a, b, c, d \in \mathbb{N}$. Since n is even, an even number of $\{a, b, c, d\}$ is odd, so assuming without loss of generality that a and b have the same parity and c and d have the same parity gives $\frac{a\pm b}{2}, \frac{c\pm d}{2} \in \mathbb{N}$. Thus:

$$\frac{n}{2} = \frac{a^2}{2} + \frac{b^2}{2} + \frac{c^2}{2} + \frac{d^2}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2.$$

□

Lemma 3.1.5. *Let $p \in \mathbb{N}$ be an odd prime. Then there are $a, b, c, d, m \in \mathbb{N}$ such that:*

$$0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2} < p^2.$$

Proof. Fix an odd prime $p \in \mathbb{N}$ and $S \coloneqq \{n^2 \mid n \in \mathbb{N}, 0 \leq n < \frac{p-1}{2}\}$. ↯ Suppose for two distinct $a^2, b^2 \in S$, we have $a^2 \equiv b^2 \bmod p$, then either $a \equiv b \bmod p$ or $a \equiv -b \bmod p$. ↯ Thus elements in S are pairwise non-congruent modulo p, which by the Pigeonhole principle gives $u^2, v^2 \in S$ such that $u^2 \equiv -v^2 - 1$ modulo p. Then there is a $m \in \mathbb{N}$ such that $u^2 = -v^2 - 1 + mp$, so $0 < u^2 + v^2 + 1^2 + 0^2 = mp$. Since $u^2, v^2 \leq \left(\frac{p-1}{2}\right)^2$, we also have $u^2 + v^2 + 1^2 \leq 1 + 2\left(\frac{p-1}{2}\right)^2 = \frac{p^2-2p+3}{2} < \frac{p^2}{2} < p^2$. □

The theorem can then be proven as follows.

Proof (of Theorem 3.1.2). Proof adopted from [28].
Fix $n \in \mathbb{N}$.
By the Fundamental Theorem of Arithmetic, if n is not prime, there are primes $p_1, ..., p_k \in \mathbb{N}$ such that $n = p_1...p_k$. If any two $a, b \in \mathbb{N}$ are both sums of four squares, then ab is also a sum of four squares by Lemma 3.1.3. Thus by induction, if all primes p_i are sums of four squares, then n is also a sum of four squares. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we have that 2^q is also a sum of four squares for any $q \in \mathbb{N}$. Thus it is sufficient to consider when n is an odd prime.
Lemma 3.1.5 gives $a, b, c, d, m \in \mathbb{N}$ such that $0 < m < n$ and $mn = a^2 + b^2 + c^2 + d^2$. Assume that m is minimal. Now suppose for a contradiction that $m \neq 1$.
↯ Suppose also that m is even, then Lemma 3.1.4 shows that it is is not minimal. ↯ ↯ Suppose instead that m divides all of a, b, c, d, then m^2 divides $a^2 + b^2 + c^2 + d^2 = mn$, so $m \mid n$, which contradicts $0 < m < n$

since n is prime. ↯ Thus m is odd and does not divide all of a, b, c, d.
Since $\frac{m-1}{2}, ..., \frac{m+1}{2}$ is a full set of residues, there are $w, x, y, z \in \mathbb{Z}$ such that:

$$\begin{aligned} w &\equiv a \mod m, & w^2 &\leq \left(\frac{m-1}{2}\right)^2, \\ x &\equiv b \mod m, & x^2 &\leq \left(\frac{m-1}{2}\right)^2, \\ y &\equiv c \mod m, & y^2 &\leq \left(\frac{m-1}{2}\right)^2, \quad \textit{and} \\ z &\equiv d \mod m, & z^2 &\leq \left(\frac{m-1}{2}\right)^2. \end{aligned}$$

Then $w^2 + x^2 + y^2 + z^2 \equiv 0 \mod m$ and $w^2 + x^2 + y^2 + z^2 < 4\left(\frac{m}{2}\right)^2 = m^2 < p^2$. Hence there is a $n \in \mathbb{N}$ such that $0 < l < m < n$ and $w^2 + x^2 + y^2 + z^2 = lm$. Multiplying with $a^2 + b^2 + c^2 + d^2 = mn$ gives

$$(aw - bx - cy - dz)^2 + (ax + bw + cz - dy)^2 + (ay - bz + cw + dx)^2 + (az + by - cx + dw)^2 = lm^2n.$$

This is 0 modulo m^2, so dividing by m^2 makes ln a sum of four squares, contradicting the minimality of $m \neq 1$. Thus $m = 1$, so $n = a^2 + b^2 + c^2 + d^2$. □

In addition to the theorem, it is worth noting that Lemma 3.1.3 can be written in a more succinct manner with a matrix, which has an important property.

Proposition 3.1.6. *Let $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, c_1, c_2, c_3, c_4 \in \mathbb{Z}$ be such that:*

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2.$$

Let $B \in \mathbb{Z}^{4\times 4}$ be a matrix where:

$$B = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ -b_2 & b_1 & -b_4 & b_3 \\ -b_3 & b_4 & b_1 & -b_2 \\ -b_4 & -b_3 & b_2 & b_1 \end{pmatrix}.$$

Then $(c_1, c_2, c_3, c_4) = (a_1, a_2, a_3, a_4)B$ and $det(B) = 0$ if and only if $b_1 = b_2 = b_3 = b_4 = 0$.

Proof. It is easy to verify that indeed $(c_1, c_2, c_3, c_4) = (a_1, a_2, a_3, a_4)B$ and $det(B) = (a^2+b^2+c^2+d^2)^2$. □

3.1.2 Sums of integral squares

The second being that any sum of two rational squares is a sum of two integral squares.

Proposition 3.1.7. *Let $n \in \mathbb{N}$. If there are $\frac{a}{c}, \frac{b}{c} \in \mathbb{Q}$ such that $n = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2$, then there are $x, y \in \mathbb{N}$ such that $n = x^2 + y^2$.*

Again, several lemmas will be introduced for this.

Lemma 3.1.8. *Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Then:*

$$\left(a_1^2 + a_2^2\right)\left(b_1^2 + b_2^2\right) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2.$$

Proof. Indeed:

$$\left(a_1^2 + a_2^2\right)\left(b_1^2 + b_2^2\right) = a_1^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2 = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2.$$

□

Lemma 3.1.9. *Let $p \in \mathbb{N}$ be an odd prime. If there are $a, b \in \mathbb{N}$ such that $a^2+b^2 \equiv 0 \mod p$, then $p = a^2+b^2$.*

Proof. This is a similar but a simpler version of Theorem 3.1.2. Fix an odd prime $p \in \mathbb{N}$, and let $a, b \in \mathbb{N}$ be such that $a^2 + b^2 \equiv 0 \mod p$, so $a^2 + b^2 = np$ for some $n \in \mathbb{N}$.
Assume that n is minimal, and suppose for a contradiction that $n \neq 1$. Since the set of all integers in $\left[\frac{m-1}{2}, \frac{m+1}{2}\right]$ is a full set of residues, there are $x, y \in \mathbb{Z}$ such that:

$$\begin{aligned} x &\equiv a \mod n, \qquad x^2 \leq \left(\frac{n}{2}\right)^2, \quad \textit{and} \\ y &\equiv -b \mod n, \qquad y^2 \leq \left(\frac{n}{2}\right)^2. \end{aligned}$$

Then $x^2 + y^2 \equiv a^2 + b^2 \equiv 0 \mod n$, so that there is a $m \in \mathbb{N}$ such that $x^2 + y^2 = nm$. It holds that:

$$m = \frac{x^2 + y^2}{n} \leq \frac{\left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2}{n} = \frac{n}{2} < n.$$

By Lemma 3.1.8 $mn^2p = (np)(nm) = (a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay + bx)^2$, which is 0 modulo n^2. Thus dividing by n^2 makes mp a sum of two squares, contradicting the minimality of $n \neq 1$. Thus $n = 1$ and $p = a^2 + b^2$. □

The proposition can then be proven as follows.

Proof (of Proposition 3.1.7). Proof adopted from [15].
Fix $n \in \mathbb{N}$, such that $n = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2$ for some $\frac{a}{c}, \frac{b}{c} \in \mathbb{Q}$, so $a^2 + b^2 = nc^2$.
If a, b, c have common factors, then they can be cancelled out to give a similar equation $a'^2 + b'^2 = nc'^2$, so assume they are coprime. If n is not square-free, it can be written as $n = mu^2$ for some $u \in \mathbb{N}$ and square-free $m \in \mathbb{N}$, such that it can be merged to give a similar equation $a^2 + b^2 = m(uc)^2$, so assume n is square-free. By the Fundamental Theorem of Arithmetic, there are distinct primes $p_1, ..., p_k \in \mathbb{N}$ such that $n = p_1...p_k$.
↯ Suppose that there is a prime p_i such that $p_i \mid a$ and $p_i \mid b$. Then either $p_i^2 \mid n$, or $p_i \mid c$. ↯ Thus there is no such prime p_i.
Rewriting gives $a^2 + b^2 = p_1...p_kc^2$, so that $a^2 + b^2 \equiv 0 \mod p_i$ for all primes p_i. Lemma 3.1.9 gives that each prime $p_i = x_i^2 + y_i^2$ for some $x_i, y_i \in \mathbb{N}$, so that $n = (x_1^2 + y_1^2)...(x_k^2 + y_k^2)$. Thus by induction with Lemma 3.1.8, n is a sum of two squares. □

Remark. Note that the above proposition holds for any two general rational numbers, since they can be rewritten such that their denominators are equal.

3.1.3 The Bruck-Ryser theorem

The previous lemmas allow the proof to be more conveniently presented.

Proof (of Theorem 3.1.1). Proof adopted from [12] and [15].
Fix $n \in \mathbb{N}$ such that $n \equiv 1 \bmod 4$ or $n \equiv 2 \bmod 4$.
Let $\mathbb{P}$ be a finite projective plane of order n with $m \coloneqq n^2+n+1$, and let $A \in \mathbb{F}_2^{m\times m}$ be an incidence matrix of $\mathbb{P}$. Now let $x \coloneqq (x_1, ..., x_m)$ and x_{m+1} be variables to be determined later, and $z \equiv (z_1, ..., z_m)$ be such that $z = xA$. Then each z_i is a linear combination of $x_1, ..., x_m$, so $z_i = \sum_{j=1}^m a_{ij}x_j$ for some $a_{ij} \in \mathbb{Z}$.
By Proposition 2.3.2:

$$zz^T = xA(xA)^T = x(AA^T)x^T = x(nI_m + J_m)x^T = nxx^T + xJ_mx^T.$$

Letting $t \coloneqq \sum_{i=1}^m x_i$, we have $xJ_mx^T = t^2$, and so this can be rewritten as:

$$\sum_{i=1}^m z_i^2 = n\sum_{i=1}^m x_i^2 + xJ_mx^T = n\sum_{i=1}^m x_i^2 + t^2.$$

Since $m+1 = n^2+n+2 \equiv 0 \bmod 4$, adding nx_{m+1}^2 to both sides gives:

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = n\sum_{i=1}^{m+1} x_i^2 + t^2 = n\sum_{i=1}^{\frac{m+1}{4}} \left(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2\right) + t^2.$$

Theorem 3.1.2 gives $n = a^2+b^2+c^2+d^2$ for some $a, b, c, d \in \mathbb{N}$, so this can be rewritten as:

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = \sum_{i=1}^{\frac{m+1}{4}} \left(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2\right)(a^2+b^2+c^2+d^2) + t^2.$$

Let $y \coloneqq (y_1, ..., y_{m+1})$ be such that $(y_i, y_{i+1}, y_{i+2}, y_{i+3}) = (x_i, x_{i+1}, x_{i+2}, x_{i+3})B$ with invertible B constructed as in Proposition 3.1.6, with $b_1 = a, b_2 = b, b_3 = c, b_4 = d$. Then by construction:

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = \sum_{i=1}^{\frac{m+1}{4}} \left(y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2\right) + t^2 = \sum_{i=1}^{m+1} y_i^2 + t^2.$$

Additionally, each y_i is also a linear combination of $x_1, ..., x_{m+1}$, so $y_i = \sum_{j=1}^m b_{ij}x_j$ for some $b_{ij} \in \mathbb{Z}$. As $x_1, ..., x_{m+1}$ are variables, it is possible to choose $x_1, ..., x_m$ depending on a_{ij} and b_{ij}, such that $z_i = \pm y_i$ for all $i \in \{1..m\}$, giving:

$$\sum_{i=1}^m y_i^2 + nx_{m+1}^2 = \sum_{i=1}^{m+1} y_i^2 + t^2 \implies nx_{m+1}^2 = y_{m+1}^2 + t^2.$$

Finally, this can be rewritten as $n = \left(\frac{y_{m+1}}{x_{m+1}}\right)^2 + \left(\frac{t}{x_{m+1}}\right)^2$, which by Proposition 3.1.7 proves that n is a sum of two squares. □

Remark. Considering orders less than a fixed small order, say 24, it is not difficult to check if an order is a sum of two squares. One method would be through a simple number sieve, by first systematically enumerating all the possibly sums of two squared integers less than 24, then remove all of these sum of two squares, prime powers, as well as natural numbers congruent to 0 or 3 modulo 4. This eventually results to the sequence A046712 on the OEIS [25], which begins with 6, 14, 21, and 22. By this argument, there are no finite projective planes of order 6, 14, 21, or 22.

3.2 Search of planes of other orders

With finite projective planes of orders ruled out by the Bruck-Ryser theorem out of the way, the focus is shifted to the existence of planes of orders that are not.

Remark. The orders of finite projective planes not more than 100 that are not ruled out by Theorem 2.2.1 and Theorem 3.1.1 are 10, 12, 15, 18, 20, 24, 26, 28, 34, 35, 36, 39, 40, 44, 45, 48, 50, 51, 52, 55, 56, 58, 60, 63, 65, 68, 72, 74, 75, 76, 80, 82, 84, 85, 87, 88, 90, 91, 92, 95, 96, 98, 99, and 100.

Unfortunately, it is still currently an open problem if there is another restriction, possibly stronger than the Bruck-Ryser theorem, which can be placed on the order of a projective plane. As such, several ad-hoc methods have been developed to tackle planes of each order separately, many of them computational in nature to quickly eliminate cases generated by theory.

Due to the sheer size of the structure in question and the number of considerations for each plane, it is often computationally intensive. There is also an inherent difficulty in translating the theory into cases checkable by a computer, and in reducing the number of cases to be considered viable in terms of CPU time.

Despite this, it has been proven with computer assistance that **a plane of order 10 does not exist**. This is taken from a joint publication in [5], that checked about 2×10^{14} cases, and took over 800 days on a VAX-11/780 at the year of publication. The search was, in brief, to classify all the cases for a 111×111 valid incidence matrix to exist, which would directly correspond to the plane of order 10.

However, a computational proof do entail certain issues. For instance, performing a brute-force search, rather than through relating proven ideas, sheds less light to the underpinnings of the theory. As pointed out by the authors of the paper themselves, this should not be considered as a "proof", in the traditional sense, that a plane of order 10 cannot exist. They even presented reasons for claiming that the probability of the existence of an undiscovered plane of order 10 is very small, but not zero.

Software errors, particularly programming errors, were the most common. Several checks for correctness to minimise errors were made, including having two different independent programs checking the same configurations at different paces. They found no discrepancies in the results, leading to confidence of having no programming errors whatsoever, but encouraged others to do independent verifications of their work.

Hardware errors were unavoidable due to the presence of non-determinism in computer hardware, such as the random changing of bits in a computer word that removes an entire branch of cases during the search. They predicted that such errors occur one in a thousand hours of computing, and even discovered a hardware failure during one of the searches before restarting it.

After the proof of the non-existence of a finite projective plane of order 10, no full proofs of other orders have been proposed, the first one merely conjectured to not exist being order 12.

Chapter 4

Non-uniqueness of planes of order nine

In the previous two chapters, discussions were mainly on the existence or non-existence of finite projective planes of various orders, while several claims were made that uniqueness of such planes do not hold in general, and the first plane of which this fails happens to be of order 9. This chapter will justify that there indeed are at least three planes of order 9 that are non-isomorphic, but only a short discussion will be provided on the fact there are exactly four of these.

4.1 Algebraic preliminaries

As a direct result of Theorem 2.2.1, since 9 is a prime power, it is known that a Desarguesian plane of order 9 exists, which will be denoted as follows.

Definition (Φ)**.** The finite projective plane Φ is the Desarguesian plane of order 9.

This chapter hence amounts to justifying that there are non-Desarguesian planes of order 9.

4.1.1 Planar ternary rings

For the proof of this, much algebraic preliminaries would be needed to even describe the existence of these planes. It was mentioned in Proposition 2.2.3 that finite Desarguesian planes can be constructed as homogeneous coordinates, but this is restrictive. For instance, attempting to generalise to modules over rings where scalars do not have multiplicative inverses would not work. This section will introduce a different algebraic method that allows the generalisation to work for arbitrary ring-like structures. To start, the following definition of a family of algebraic structures, known as planar ternary rings, is crucial.

Definition (Planar ternary ring)**.** A **planar ternary ring** (PTR) is an ordered quadruple $(R, T, 0, 1)$, where R is a set, with two distinguished and different elements $0, 1 \in R$, and a ternary operation $T : R \times R \times R \to R$, which satisfies these five axioms:

1. for all $a, b \in R$, we have $T(a, 0, b) = T(0, a, b) = b$,
2. for all $a \in R$, we have $T(1, a, 0) = T(a, 1, 0) = a$,
3. for all $a, b, c, d \in R$ such that $a \neq c$, there is a unique $x \in R$ such that $T(x, a, b) = T(x, c, d)$,
4. for all $a, b, c \in R$, there is a unique $x \in R$, such that $T(a, b, x) = c$, and
5. for all $a, b, c, d \in R$ such that $a \neq c$, there are unique $x, y \in R$ such that $T(a, x, y) = b$ and $T(c, x, y) = d$.

Define the addition operation $+ : R \times R \to R$ such that for all $a, b \in R$, we have $a + b = T(a, 1, b)$, and define the multiplication operation $\cdot : R \times R \to R$ such that for all $a, b \in R$, we have $a \cdot b = T(a, b, 0)$. A PTR $(R, T, 0, 1)$ is also said to be **linear** if for all $a, b, c \in R$, we have $T(a, b, c) = ab + c$.

Remark. It is clear that in linear PTRs, the ternary operation depends entirely on the two binary operations, leaving it redundant. As such, they can be instead written as the ordered quintuple $(R, +, \cdot, 0, 1)$.

To motivate the reason in using PTRs for finite projective planes, a relation to the familiar skew-fields definition in a previous chapter is as follows.

Proposition 4.1.1. *Let $(R, +, \cdot, 0, 1)$ be a skew-field. Then $(R, +, \cdot, 0, 1)$ is a linear PTR.*

Proof. Fix $a, b, c, d \in R$. It is sufficient to check the five axioms of PTRs, defining the ternary operation as $T(a, b, c) = a \cdot b + c$.

1. $a \cdot 0 + b = 0 \cdot a + b = b$ holds by the additive identity.
2. $1 \cdot a + 0 = a \cdot 1 + 0 = a$ holds by the multiplicative identity.
3. Let $a \neq c$. Then $x = (a - c)^{-1} \cdot (d - b)$ is the unique solution to the equation $x \cdot a + b = x \cdot c + d$.
4. $x = c - a \cdot b$ is the unique solution to the equation $a \cdot b + x = c$.
5. Let $a \neq c$. Then $x = (b-d) \cdot (a-c)^{-1}$ and $y = b - a \cdot x$ are unique solutions to the equations $a \cdot x + y = b$ and $c \cdot x + y = d$.

□

4.1.2 Non-homogeneous coordinates

With this in mind, the method of constructing general projective planes using general PTRs in discussion, known as **non-homogeneous coordinates**, is defined in the following proposition.

Proposition 4.1.2. *Let $(R, T, 0, 1)$ be a PTR and $\infty \notin R$ be an additional symbol, and let:*

1. $P \coloneqq \{p_{(a,b)} \mid a, b \in R\} \cup \{p_a \mid a \in R\} \cup \{p_\infty\}$,
2. $L \coloneqq \{l_{(a,b)} \mid a, b \in R\} \cup \{l_a \mid a \in R\} \cup \{l_\infty\}$, *and*
3. $I \coloneqq I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5 \cup I_6$, *where*
   (a) $I_1 \coloneqq \{(p_{(x,y)}, l_{(m,k)}) \mid p_{(x,y)} \in P, l_{(m,k)} \in L, T(m, x, y) = k\}$,
   (b) $I_2 \coloneqq \{(p_{(x,y)}, l_k) \mid p_{(x,y)} \in P, l_k \in L, x = k\}$,
   (c) $I_3 \coloneqq \{(p_x, l_{(m,k)}) \mid p_x \in P, l_{(m,k)} \in L, x = m\}$,
   (d) $I_4 \coloneqq \{(p_x, l_\infty) \mid p_x \in P\}$,
   (e) $I_5 \coloneqq \{(p_\infty, l_k) \mid l_k \in L\}$, *and*
   (f) $I_6 \coloneqq \{(p_\infty, l_\infty)\}$.

Then $\mathbb{P}(R) \coloneqq (P, L, I)$ is a finite projective plane, ***coordinatised*** *by the PTR $(R, T, 0, 1)$.*

Remark. The primary motivation for constructing finite projective planes in this way is that, given a finite projective plane $\mathbb{P} \equiv (P, L, I)$, the four points $p_1, p_2, p_3, p_4 \in P$ in the quadrangle can be chosen as $p_1 \coloneqq p_0$, $p_2 \coloneqq p_\infty$, $p_3 \coloneqq p_{(0,0)}$, and $p_4 \coloneqq p_{(1,1)}$. With the lines and the incidence relation defined appropriately, we have that $\mathbb{P}$ naturally satisfies the axioms of PTRs. A more detailed explanation can be found in [12].

Proof. Proof directly taken from [12].
Fix $a, b, c, d \in R$. It is sufficient to check the three axioms of projective planes.

1. If $a \neq c$, then by axiom 3, for any given $b, d \in R$, there is a unique $m \in R$ such that $T(m, a, b) = T(m, c, d)$. Then the points $p_{(a,b)}$ and $p_{(c,d)}$ are on the unique line $l_{(m,T(m,a,b))}$.
   Clearly, the two points $p_{(a,b)}$ and $p_{(a,d)}$ are on the line l_a. If both of these points were also on the line $l_{(m,k)}$, then we would have $T(m, a, b) = k = T(m, a, d)$, which contradicts axiom 4. Thus there is a unique line joining any two distinct points such that neither is on l_∞.
   Let p_m be any point not p_∞ on l_∞, and $p_{(a,b)}$ be any point also not on l_∞. Any line through p_m is

either l_∞ or is of the form $l_{(m,k)}$ for some $k \in R$, and the line $l_{(m,k)}$ passes through $p_{(a,b)}$ if and only if $T(m,a,b) = k$. However, since $T(m,a,b)$ is uniquely determined by m, a, and b, so that $l_{(m,T(m,a,b))}$ is the unique line containing p_m and $p_{(a,b)}$. Since any line not on l_∞ which contains p_∞ is of the form l_k for some $k \in R$, the unique line joining p_∞ and $p_{(a,b)}$ is l_a. Finally, p_{m_1} and p_{m_2} clearly have l_∞, and no other line, in common.

2. It is sufficient to show that any two distinct lines have at least one point in common. Consider the lines $l_{(m_1,k_1)}$ and $l_{(m_2,k_2)}$. If $m_1 \neq m_2$, then, by axiom 5, there exists a unique ordered pair (a,b) such that $T(m_1,a,b) = k_1$ and $T(m_2,a,b) = k_2$ so that the point $p_{(a,b)}$ is on both $l_{(m_1,k_1)}$ and $l_{(m_2,k_2)}$. If $m_1 = m_2$, then p_{m_1} is on both lines, hence any pair of distinct lines of the form $l_{(m,k)}$ have a common point. Clearly, the line $l_{(m,k)}$ meets l_∞ at p_m, so, in order to show that this intersects any other line, it is sufficient to only consider the intersection of $l_{(m,k)}$ with l_h, where $h \in R$ and $h \neq m$. However, these two lines intersect in the point (h,h') where h' exists by axiom 4 and is given by $T(x,h,h') = k$. Since any two lines l_{m_1} and l_{m_2} intersect at p_∞, we have that any two lines intersect in a unique point.

3. The points p_0, p_∞, $p_{(0,0)}$, and $p_{(1,1)}$ clearly forms a quadrangle.

□

In fact, with a slight change in perspective, non-homogeneous coordinates of a finite projective plane can be derived from its homogeneous coordinates if it is possible to construct it in that way. A possible transformation is as follows, as described in [30].

Example. Let $\mathbb{P} \equiv (P,L,I)$ be a finite Desarguesian plane over a skew-field F constructed with the notation in Proposition 2.2.3, and S be the set of all symbols of $\mathbb{P}(R)$ in Proposition 4.1.2 written as elements of F. With this notation, let the map $\phi : V^*/F^* \to S$ be such that for all $[(x,y,z)^T] \in V^*$:

$$\phi\left(\left[\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right]\right) = \begin{cases} (\frac{x}{z}, \frac{y}{z}) & z \neq 0 \\ (\frac{y}{x}) & x \neq 0, z = 0 \\ (\infty) & x = z = 0 \end{cases}.$$

Then applying ϕ to all equivalence classes $[v] \in V^*/F^*$ in all points $p_{[v]} \in P$ and all lines $l_{[v]} \in L$ indeed gives a valid non-homogeneous coordinatisation of $\mathbb{P}$.

As a concrete example of non-homogeneous coordinatisation, the Fano plane is provided as follows.

Example. The coordinatising skew-field of the Fano plane has the symbols $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, (0), (1), and (∞) in its points and lines, with the quadrangle being $p_0, p_\infty, p_{(0,0)}, p_{(1,1)}$.

4.1.3 Properties of planar ternary rings

Any finite projective plane can now be solely defined by its coordinatising PTR together with the initial choice of the quadrangle. As in other algebraic structures, the notion of isomorphism of PTRs is often useful, defined as follows.

Definition (Isomorphism)**.** Let $P \equiv (R,T,0,1)$ and $P' \equiv (R',T',0',1')$ be two PTRs. An **isomorphism** from P to P' is a bijection $\alpha : R \to R$ such that for all $a,b,c \in R$, we have $\alpha(T(a,b,c)) = T(\alpha(a),\alpha(b),\alpha(c))$.

Remark. It is trivial to verify that isomorphism of PTRs is an equivalence relation.

It is then clear that two finite projective planes are isomorphic if their coordinatising PTRs are isomorphic. As such, to study the structure of a plane, it is sufficient to study the properties of its coordinatising PTR, especially those of its two binary operations that define its ring-like structure. In particular, the definition of a group-like structure is as follows.

Definition (Loop)**.** A **loop** is an ordered triple $(R,\cdot,1)$, where R is a set, with a distinguished $1 \in Q$, and with a binary operation $\cdot : R \times R \to R$ such that:

1. for all $a \in R$, we have $1 \cdot a = a \cdot 1 = a$,

2. for all $a, b \in R$, there are unique $x, y \in R$ such that $a \cdot x = b = y \cdot a$.

A loop is hence simply a group without requiring associativity. The loop structure of the two binary operations of a PTR is illustrated in the following proposition.

Proposition 4.1.3. *Let $(R, T, 0, 1)$ be a PTR. Then:*

1. *$(R, +, 0)$ is a loop, and*
2. *$(R \setminus \{0\}, \cdot, 1)$ is a loop.*

Proof. Check the two axioms of loops in both parts.

1. Clearly 0 is the additive identity. Fix $a, b \in R$. Then there is a unique $x \in R$ such that $a + x = T(a, 1, x) = b$. Similarly there is a unique $y \in R$ such that $y + a = T(y, 1, a) = T(y, 0, b) = b$.
2. Clearly 1 is the multiplicative identity. Fix $a, b \in R$. Then there is a unique solution $y \in R$ such that $y \cdot a = T(y, a, 0) = T(y, 0, b) = b$. Similarly there is a unique $x, z \in R$ such that $a \cdot x + z = T(a, x, z) = b$ and $z = T(0, x, z) = 0$. The latter implies that there is a unique solution to $a \cdot x = b$.

□

4.1.4 Quasi-fields

These digressions are not for naught, as they lead to the different types of PTRs coordinatising non-Desarguesian projective planes, namely quasi-fields, near-fields, and semi-fields. Most of these definitions are adopted from [16], with that of a quasi-field as follows.

Definition (Quasi-field)**.** A left **quasi-field**, also known as a Veblen-Wedderburn system, is an ordered quintuple $(R, +, \cdot, 0, 1)$, where R is a set, with two distinguished and different $0, 1 \in R$, and with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$, which satisfies the following weakening of the axioms of skew-fields:

1. the ordered triple $(R, +, 0)$ is a group,
2. the ordered triple $(R \setminus \{0\}, \cdot, 1)$ is a loop,
3. for all $a, b, c \in R$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$ (left distributivity),
4. for all $a, b, c \in R$ such that $a \neq b$, there is a unique $x \in R$ such that $ax = bx + c$.

A right quasi-field is similarly defined. A quasi-field is said to be **abelian** if it is a field.

Clearly every skew-field is a left quasi-field. In fact, a quasi-field can alternatively be defined from a PTR, as illustrated in the following proposition.

Proposition 4.1.4. *A left quasi-field $(R, +, \cdot, 0, 1)$ is a linear PTR such that the ordered triple $(R, +, 0)$ is a group (associativity of $+$), and for all $a, b, c \in R$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$ (left distributivity).*

Proof. Fix $a, b, c, d \in R$. It is sufficient to check the five axioms of PTRs, defining the ternary operation as $T(a, b, c) = a \cdot b + c$.

1. $a \cdot 0 + b = 0 \cdot a + b = b$ holds by the additive identity.
2. $1 \cdot a + 0 = a \cdot 1 + 0 = a$ holds by the multiplicative identity.
3. Let $a \neq c$, and $x \in R$ be a solution to the equation $x \cdot a + b = x \cdot c + d$, so $b - d = -x \cdot a + x \cdot c$. By the left distributivity property, $b - d = x \cdot (-a + c)$, which by the loop property gives a unique solution x.
4. By the abelian group property of quasi-fields, $a \cdot b + x = c$ has the unique solution $x = c - a \cdot b$.

5. Let $a \neq c$, and $x, y \in R$ be solutions to the equations $a \cdot x + y = b$ and $c \cdot x + y = d$, so $-a \cdot x + b = y = -c \cdot x + d$. By the last axiom, $a \cdot x = c\dot{x} + (b - d)$, so there is a unique solution x. Thus $y = -a \cdot x + b$ is also unique.

□

Remark. A left quasi-field is actually defined as a **cartesian group** with left distributivity, which is in turn defined as an associative linear PTR. A right quasi-field is similarly defined. Cartesian groups will not be discussed here for simplicity.

4.1.5 Properties of quasi-fields

Several interesting properties can be derived directly from the axioms of quasi-fields. The following proposition is rather fundamental, but is not stated as an axiom as it can be derived from the other axioms.

Proposition 4.1.5. *Let $(R, +, \cdot, 0, 1)$ be a left quasi-field. Then the group $(R, +, 0)$ is abelian.*

Proof. Proof adopted from [26].
Fix $a, b \in R$. If $a = 0$ or $b = 0$, then $a + b = b + a$ holds trivially. Otherwise $a \neq 0$ and $b \neq 0$, then there is a $c \in R$ such that $c \cdot a = b + a - b$. Suppose for a contradiction that $c \neq 1$. ↯ Also suppose that there are distinct $x, y \in R$ such that $-c \cdot x + x = b = -c \cdot y + y$, so $x - y = c \cdot x - c \cdot y$. By left distributivity, $x - y = c \cdot (x - y)$, which gives $x = y$. ↯ Hence there is a unique $x \in R$ such that $-c \cdot x + x = b$. However, this also implies that, despite $x \neq x + a$:

$$-c \cdot (x+a) + (x+a) = -c \cdot a - c \cdot x + x + a = -(b+a-b) - c \cdot x + (c \cdot x + b) + a = b - a - b - c \cdot x + c \cdot x + b + a = b,$$

contradicting the uniqueness of x. Thus $c = 1$, so $a + b = b + a$ and the group $(R, +, 0)$ is abelian. □

A related structure is a quasi-field without one of the axioms, defined as follows.

Definition (Weak quasi-field)**.** A left **weak quasi-field** is a quasi-field as defined above without axiom 4. A right weak quasi-field is defined similarly.

It is clear that a quasi-field is a weak quasi-field. However, as the scope of discussion is again limited to finite projective planes, only finite weak quasi-fields will be considered, leading directly to the following proposition.

Proposition 4.1.6. *Let $(R, +, \cdot, 0, 1)$ be a finite left weak quasi-field. Then $(R, +, \cdot, 0, 1)$ is a left quasi-field.*

Proof. Fix $a, b, c \in R$ such that $a \neq b$. ↯ Suppose there are two distinct $x, x' \in R$ such that $ax = bx + c$ and $ax' = bx' + c$. Subtracting gives $ax - bx = ax' - bx'$, which can be rewritten as $a(x - x') = b(x - x')$ by commutativity of $+$ and left distributivity. Right cancellation of $x - x' \neq 0$ gives $a = b$. ↯ Thus there is a unique $x \in R$ such that $ax = bx + c$, so $(R, +, \cdot, 0, 1)$ is a left quasi-field. □

This shows that finite quasi-fields are equivalent to weak quasi-fields, as such can be used interchangeably in finite contexts. This also implicitly means that axiom 4 in the above definition of a finite quasi-field can actually be implied from the other three axioms. Now an important notion of any algebraic structure is its kernel, defined for a general weak quasi-field as follows.

Definition (Kernel)**.** The **kernel** K of a left weak quasi-field $(R, +, \cdot, 0, 1)$ is the set of all elements $c \in R$, such that for all $a, b \in R$:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of $\cdot$), and
2. $(a + b) \cdot c = a \cdot c + b \cdot c$ (right distributivity).

The kernel of a right weak quasi-field is defined similarly.

Note that the above definition applies similarly to a general quasi-field. The kernel of a weak quasi-field has an interesting enough structure, such that equipping it with the restricted binary operations of the quasi-field would almost make it a field.

Proposition 4.1.7. *Let $(R, +, \cdot, 0, 1)$ be a left weak quasi-field. Then the kernel $K \subset R$ is such that $(K, +, \cdot, 0, 1)$ is a skew-field.*

Proof. It is sufficient to check that $(K, +, \cdot, 0, 1)$ is a ring and for any $k \in K \setminus \{0\}$, there is a unique $j \in K \setminus \{0\}$ such that $j \cdot k = k \cdot j = 1$.

1. It is easy to see that $0, 1 \in K$. Associativity of $+$ follows from the definition of a weak quasi-field and commutativity of $+$ follows from Proposition 4.1.5. For any $j, k \in K$, we have:

$$a \cdot (b \cdot (j - k)) = a \cdot (b \cdot j - b \cdot k) = a \cdot (b \cdot j) - a \cdot (b \cdot k) = (a \cdot b) \cdot j - (a \cdot b) \cdot k = (a \cdot b) \cdot (j - k),$$

$$(a + b) \cdot (j - k) = (a + b) \cdot j - (a + b) \cdot k = a \cdot j + b \cdot j - a \cdot k - b \cdot k = a \cdot (j - k) + b \cdot (j - k).$$

   Hence $j - k \in K$ and $(K, +, 0)$ is an abelian group. Finally, left distributivity follows from the definition of a left weak quasi-field, while associativity of $\cdot$ and right distributivity follows from the definition of its kernel. Thus $(K, +, \cdot, 0, 1)$ is indeed a ring.

2. Now fix any $k \in K \setminus \{0\}$. The loop property of a weak quasi-field gives unique $x, y \in R$ such that $k \cdot x = 1$ and $y \cdot k = 1$. Then it holds that:

$$(k \cdot (x - y)) \cdot k = (k \cdot x - k \cdot y) \cdot k = (k \cdot x) \cdot k - (k \cdot y) \cdot k = (k \cdot x) \cdot k - k \cdot (y \cdot k) = 1 \cdot k - k \cdot 1 = k - k = 0.$$

   Since $k \neq 0$, we have $x - y = 0$ and hence $j \coloneqq x = y$ is unique. Clearly $j \neq 0$, and:

$$(a \cdot (b \cdot j)) \cdot k = a \cdot ((b \cdot j) \cdot k) = a \cdot (b \cdot (j \cdot k)) = a \cdot b = (a \cdot b) \cdot (j \cdot k) = ((a \cdot b) \cdot j) \cdot k,$$

$$((a + b) \cdot j) \cdot k = (a + b) \cdot (j \cdot k) = a + b = a \cdot (j \cdot k) + b \cdot (j \cdot k) = (a \cdot j) \cdot k + (b \cdot j) \cdot k = (a \cdot j + b \cdot j) \cdot k,$$

   Thus right cancellation of $k \neq 0$ gives $a \cdot (b \cdot j) = (a \cdot b) \cdot j$ and $(a + b) \cdot j = a \cdot j + b \cdot j$, so $j \in K \setminus \{0\}$.

□

In a different perspective, a weak quasi-field is simply a vector space over its kernel skew-field, with scalar multiplication being the multiplication operation. Again, Theorem 2.2.2 implies that finite skew-fields are finite fields and have prime power order, so finite quasi-fields as finite-dimensional vector spaces over finite kernel skew-fields indeed have prime power order. This means that any undiscovered finite non-Desarguesian planes of order not a prime power, if they exist, cannot be coordinatised with finite quasi-fields and hence cannot be proven to not exist with this method.

4.1.6 Near-fields and semi-fields

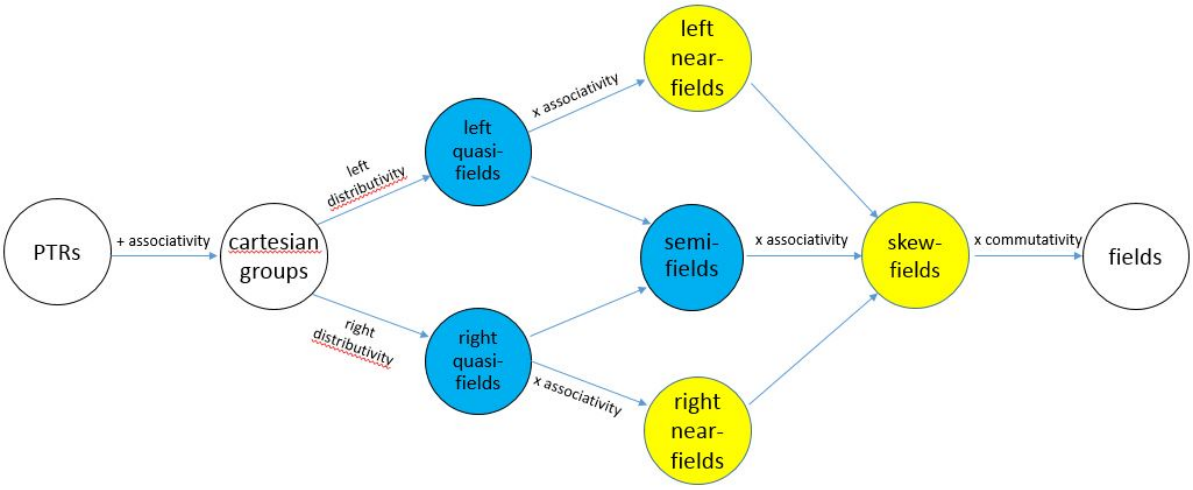
Although only the theory of quasi-fields is required for the next section, some have an additional associativity property that justify being called near-fields, defined as follows.

Definition (Near-field)**.** A finite left **near-field** $(R, +, \cdot, 0, 1)$ is a finite left quasi-field such that the ordered triple $(R \setminus \{0\}, \cdot, 1)$ is a group (associativity of $\cdot$). A finite right near-field is similarly defined.

Finally, the definition of a semi-field, often referred to in literature as a coordinatising PTR constructed from a quasi-field in a different way, will be provided below appropriately.

Definition (Semi-field)**.** A **semi-field** is a left quasi-field that is also a right quasi-field.

With these two definitions, a finite skew-field can be alternatively defined as a finite left near-field that is also a finite right near-field, or as a finite semi-field with a multiplicative group. In summary, it is obvious that the following chain of class inclusions for finite PTRs hold.



Relationship between different types of finite PTRs

Remark. As any finite skew-field is a finite field by Theorem 2.2.2, commutativity is indeed redundant here. Strictly speaking, the relation between near-fields and quasi-fields do not hold for infinite cases. The above definition is in fact of a **planar near-field**, but is a simplification justified as all finite near-fields are planar.

4.2 Existence of non-Desarguesian planes

For this section, denote $(x, y)^T$ as (x, y) and omit $\cdot$, for ease of notation.

With properties and definitions of several types of PTRs defined in the previous section, the existence of a non-Desarguesian plane of order 9 can be shown succinctly and constructively. The proof lies on the intuition that finite Desarguesian planes coordinatised by an arbitrary PTR implies that the PTR is in fact a skew-field. This is stated more precisely in the following proposition with the coordinatisation method by algebraic structures discussed in the previous section.

Proposition 4.2.1. *Let $\mathbb{P}(R)$ be a finite projective plane coordinatised by a finite near-field $(R, +, \cdot, 0, 1)$, and $\mathbb{P}(F)$ be a finite projective plane coordinatised by a finite skew-field $(F, +, \cdot, 0, 1)$. If $\mathbb{P}(R) \cong \mathbb{P}(F)$, then $(R, +, \cdot, 0, 1) \cong (F, +, \cdot, 0, 1)$.*

Proof. Omitted, see [13]. □

Remark. The statement does not generally hold if one of the finite projective planes given above is not coordinatised by a finite skew-field. That is, if two finite projective planes are isomorphic, their coordinatising PTRs are not necessarily isomorphic.

4.2.1 Hall quasi-fields

It follows that in order to construct a non-Desarguesian projective plane, it is sufficient to construct a left quasi-field that is not a skew-field. This can be done by showing that a given quasi-field is not right distributive, or vice versa, so that it is not a semi-field. Alternatively, this can be done by showing that a given left or right quasi-field is not associative in its multiplication operation, so that it is not a near-field. The quasi-field constructed in the definition below, named after M Hall, fits the former description.

Definition (Hall quasi-field)**.** Let $f(x) \coloneqq x^2 - gx - h$ be an irreducible quadratic polynomial over a finite field $\mathbb{F}_n \equiv (F, +, \cdot, 0, 1)$ of order n, such that $g, h \in \mathbb{F}_n$. Now let $\mathbb{G}$ be a two-dimensional vector space

$(G, \oplus, \cdot, (0,0), 1)$ over $\mathbb{F}_n$, where $G = \mathbb{F}_n \times \mathbb{F}_n$. Then a **Hall quasi-field** $\mathbb{H}$ of order n^2 is an ordered quintuple $(G, \oplus, \odot, (0,0), (1,0))$, where the multiplication operation $\odot : G \to G$ is such that:

$$(a,b) \odot (c,d) = \begin{cases} (ac, ad) & b = 0 \\ (ac - b^{-1}df(a), bc - ad + gd) & b \neq 0 \end{cases}.$$

$\mathbb{H}$ is said to be constructed by $f(x) \in \mathbb{F}_n[x]_{\leq 2}$.

Remark. The subtraction operation of Hall quasi-fields is denoted as $\ominus$.

It is not immediately clear that this is a quasi-field. To prove this, a useful lemma is as follows.

Lemma 4.2.2. *Let $\mathbb{H} \equiv (G, \oplus, \odot, (0,0), (1,0))$ be a Hall quasi-field constructed by $f(x) \equiv x^2 - gx - h \in \mathbb{F}_n[x]_{\leq 2}$. Then for all $(a,b), (c,d), (e,f) \in G$:*

1. *if $b \neq 0$, then $f((a,b)) = (0,0)$,*
2. *if $b = 0$, then $(a,b) \odot (c,d) = (c,d) \odot (a,b)$,*
3. *if $f = 0$, then $(a,b) \odot ((c,d) \odot (e,f)) = ((a,b) \odot (c,d)) \odot (e,f)$, and*
4. *if $f = 0$, then $((a,b) \oplus (c,d)) \odot (e,f) = (a,b) \odot (e,f) \oplus (c,d) \odot (e,f)$.*

Proof. The last two parts will be omitted for the sake of further discussion, as they are lengthy but can be derived by cases from the construction above. Check only the first two parts.

1. Fix $(a,b) \in G$ such that $b \neq 0$. Then:

$$\begin{aligned} f(a,b) &= (a,b) \odot (a,b) \ominus g(a,b) \ominus h(1,0) \\ &= (aa - b^{-1}bf(a), ba - ab + gb) \ominus (ga, gb) \ominus (h, 0) \\ &= (aa - b^{-1}b(a^2 - ga - h) - ga - h, ab - ab + gb - gb - 0) = (0,0). \end{aligned}$$

2. Fix $(a,0), (c,d) \in G$. Then:

$$(c,d) \odot (a,0) = (ca - d^{-1}0f(c), da - c0 + g0) = (ca, da) = (ac, ad) = (a,0) \odot (c,d).$$

□

The last two parts of the lemma are exactly the two conditions for being a kernel of a left weak quasi-field. This means that if a Hall quasi-field is a left weak quasi-field, all elements of the form $(a,0)$, are in the kernel. Now this is indeed the case, as illustrated in the following proposition.

Proposition 4.2.3. *Let $\mathbb{H}$ be a Hall quasi-field. Then $\mathbb{H}$ is a left quasi-field.*

Proof. Proof adopted from [12].
Let $\mathbb{H} \equiv (G, +, \cdot, (0,0), (1,0))$ be a Hall quasi-field. It is sufficient to check the three axioms of left weak quasi-fields.

1. The addition operation $\oplus : G \times G \to G$ in the underlying vector space $\mathbb{G}$ forms an abelian group with the elements of G.
2. Fix $(a,b), (c,d) \in G \setminus \{(0,0)\}$. It is sufficient to check the two axioms of loops.
   Clearly the identity $(1,0)$ is such that $(1,0) \odot (a,b) = (a,b) \odot (1,0) = (a,b)$.
   Assume that there is a $(x,y) \in G \setminus \{(0,0)\}$ such that $(a,b) \odot (x,y) = (c,d)$. If $b = 0$, then $a \neq 0$, so solving $(ax, ay) = (c,d)$ gives a unique solution $(x,y) = (a^{-1}c, a^{-1}d)$. Otherwise if $b \neq 0$, then $(ax - b^{-1}yf(a), bx - ay + gy) = (c,d)$, which can be rewritten in a matrix form as:

$$\begin{pmatrix} a & -b^{-1}f(a) \\ b & -a + g \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}.$$

↯ Suppose the determinant $a(-a+g)-b(-b^{-1}f(a))=-h=0$, then $f(x)=x^2-gx=(x-g)x$, which is reducible. ↯ Thus the determinant is non-zero and there is a unique solution (x,y).
Assume that there is a $(x',y')\in G\setminus\{(0,0)\}$ such that $(x',y')\odot(a,b)=(c,d)$ and that $y'=0$ is a solution. If $b=0$, then $a\neq 0$, so solving $(x'a,x'b)=(c,d)$ gives a unique solution $x'=ca^{-1}$ if and only if $d=0$. If instead $a=0$, then $b\neq 0$, so solving $(x'a,x'b)=(c,d)$ gives a unique solution $x'=db^{-1}$ if and only if $c=0$. Otherwise if $b\neq 0$ and $a\neq 0$, then solving $(x'a,x'b)=(c,d)$ gives a unique solution if and only if $x'=ca^{-1}=db^{-1}$. Thus it remains to show that if either $a=c=0$, $b=d=0$, or $ca^{-1}=db^{-1}$, then there are no solutions for $y'\neq 0$.
Now assume instead that $y'\neq 0$ is a solution, so $(x'a-y'^{-1}bf(x'),y'a-x'b+gb)=(c,d)$, which can be written as $(y'x'a-bx'^2+bgx'+bh,x'y'a-x'^2b+x'gb)=(y'c,x'd)$. This subtracts to give the linear equation $bh=y'c-x'd$, which, with $y'a-x'b+gb=d$, gives the same solutions as the latter with $y'x'a-bx'^2+bgx'+bh=c$. This can be written in a matrix form as:

$$\begin{pmatrix}a & -b\\ c & -d\end{pmatrix}\begin{pmatrix}y'\\ x'\end{pmatrix}=\begin{pmatrix}d-gb\\ bh\end{pmatrix}.$$

If $b=0$, then $a\neq 0$, so solving this gives a solution $(x',y')=(ca^{-1},da^{-1})$, which gives $y=0$ if and only if $d=0$. If $b\neq 0$, then multiplying db^{-1} to $y'a-x'b+gb=d$ to give $y'adb^{-1}-dx'+dg=d^2b^{-1}$ and combining with $bh=y'c-x'd$ gives the equation $y'adb^{-1}-y'c=d^2b^{-1}-dg-bh$. Finally, this can be rewritten in a compact form as $y'(ad-bc)=b^2f(db^{-1})$.
↯ Suppose that either $a=c=0$, $b=d=0$, or $ca^{-1}=db^{-1}$, so that $ad-bc=0$. Then $y'(ad-bc)=0$, but $b^2f(db^{-1})\neq 0$. ↯ Thus there are no solutions for $y'\neq 0$ in this case. Otherwise, we have $ad-bc\neq 0$, so $y'=(b^2f(db^{-1}))(ad-bc)^{-1}\neq 0$ is a unique solution.

3. The multiplication operation $\odot: G\times G\to G$ is evidently a left linear transformation, making it left distributive.

Thus $\mathbb{H}$ is a left weak quasi-field. By Lemma 4.2.2, $\mathbb{H}$ is simultaneously a two-dimensional module over its finite kernel skew-field, and hence is finite. By Proposition 4.1.6, $\mathbb{H}$ is a left quasi-field. □

Now it is sufficient to show that for a given finite field of order $n\in\mathbb{N}$, if a Hall quasi-field of order n^2 constructed over it is not a semi-field, it would coordinatise a finite non-Desarguesian plane. However, it was mentioned in a previous chapter that the finite projective plane of order 4 is unique up to isomorphism and is in fact Desarguesian. This is not a contradiction, as specified in the following proposition.

Proposition 4.2.4. *Let $\mathbb{H}$ be a Hall quasi-field of order 4. Then $\mathbb{H}$ is a field.*

Proof. It is sufficient to show that $\mathbb{H}$ is right distributive, which is a straightforward verification of cases. □

Thus the non-Desarguesian argument does not hold for the Hall quasi-field of order 4. In fact, the converse of the above proposition also holds true, ultimately proving the existence of a non-Desarguesian plane of order 9, as illustrated below.

Proposition 4.2.5. *Let $\mathbb{H}$ be a Hall quasi-field of order greater than 4. Then $\mathbb{H}$ is not a semi-field.*

Proof. Let $\mathbb{H}\equiv(G,+,\cdot,(0,0),(1,0))$ be a right distributive Hall quasi-field constructed by $f(x)\equiv x^2-gx-h\in\mathbb{F}_n[x]_{\leq 2}$. It is sufficient to show that $n=2$. Since $0,1\in\mathbb{F}_n$, we have $(0,1),(1,0)\in G$, so that:

$$(-f(0),g-1)=(1,1)\odot(0,1)=((1,0)\oplus(0,1))\odot(0,1)=(1,0)\odot(0,1)\oplus(0,1)\odot(0,1)=(-f(0),g+1).$$

Thus $1=-1$, which holds only if $n=2$. □

This directly implies that there is an entire class of countably infinite finite projective planes, each coordinatised with a Hall quasi-field. Due to its importance, a name due to Hall was given as follows.

Definition (Hall plane)**.** A **Hall plane** is a finite non-Desarguesian plane coordinatised by a Hall quasi-field.

Remark. By construction, there are Hall planes of order $n=p^{2q}$ for $q\in\mathbb{N}$ and prime $p\in\mathbb{N}$. However, since Hall planes are generally defined to be non-Desarguesian, it is customary to exclude the plane of order $4=2^2$ in the definition, requiring $n>4$.

Finally, the titular plane will be denoted as follows.

Definition (Ω)**.** The finite projective plane Ω is the Hall plane of order 9.

Remark. It is easy to see that Ω is not self-dual as it is coordinatised by a left quasi-field that is not a right quasi-field.

An interesting note is that there are exactly four non-isomorphic non-abelian quasi-fields, all of which coordinatise Ω. Three of these are Hall quasi-fields constructed by three different initial irreducible quadratic polynomials, namely $f(x) = x^2 + 1$, $f(x) = x^2 + x - 1$, and $f(x) = x^2 - x - 1$, while the fourth by a different method. In fact, the first of these generates a near-field, as illustrated in the following stronger proposition.

Proposition 4.2.6. *Let $\mathbb{H}$ be a Hall quasi-field of order $n \in \mathbb{N}$ constructed over the irreducible quadratic polynomial $f(x) \in \mathbb{F}_n[x]_{\leq 2}$. Then $\mathbb{H}$ is a near-field if and only if $n = 2$ or $n = 3$, and $f(x) = x^2 + 1$.*

Proof. Proof adopted from [12].
Let $\mathbb{H} \equiv (G, \oplus, \odot, (0,0), (1,0))$ be a Hall quasi-field. It is sufficient to show the associativity property in both directions.

1. Let $\mathbb{H}$ be associative and constructed by $f(x) \equiv x^2 - gx - h \in \mathbb{F}_n[x]_{\leq 2}$, and fix $(a, 0) \in G \setminus \{(0,0)\}$. It holds by associativity that:

$$(ha^{-1}, g) = (0, a) \odot (0, 1) = (0, 1) \odot (a, 0) \odot (0, 1) = (0, 1) \odot (0, a) = (ha, ga).$$

   Hence $ha^{-1} = ha$ and $g = ga$. Now due to the irreducibility of f, we have $h \neq 0$, so that $a^2 = 1$. The only fields with this property are $\mathbb{F}_2$ and $\mathbb{F}_3$. In $\mathbb{F}_2$, the only irreducible quadratic polynomial is $f(x) = x^2 + 1$. In $\mathbb{F}_3$, since $a^2 = 1$ also holds for $a = -1$, we have $h = 0$, which also narrows down the only irreducible quadratic polynomial to $f(x) = x^2 + 1$.

2. Conversely, the Hall quasi-field of order 4 is a field, and as such is associative. For the Hall quasi-field of order 9, let $\mathbb{H}$ be constructed by $f(x) \equiv x^2 + 1 \in \mathbb{F}_3[x]_{\leq 2}$. Since $b^{-1} = -b$ for any $b \neq 0$, multiplication is simply:

$$(a, b) \odot (c, d) = \begin{cases} (ac, ad) & b = 0 \\ (ac - bd(a^2 + 1), bc - ad) & b \neq 0 \end{cases}.$$

   A simple verification shows that this indeed is associative.

□

4.2.2 Other non-Desarguesian planes

Due to Ω not being self-dual, it is easy to coordinatise a third non-Desarguesian plane. This is done by applying plane duality, giving the dual plane with the same order. Thus, by a symmetrical construction of a dual Hall quasi-field, the definition of its dual plane is as follows.

Definition (Ω^D)**.** The finite projective plane Ω^D is the dual plane of Ω.

As such, it is clear that there are at least three distinctively non-isomorphic finite projective planes of order 9. In the original paper by O Veblen and J H Maclagan-Wedderburn in [29], it was discovered that there is in fact a fourth plane of order 9, which was later generalised into another family of planes by D R Hughes. This fourth plane, named after him, will not be discussed here, but it shall be denoted as follows.

Definition (Ψ)**.** The **Hughes plane** Ψ is the fourth finite projective plane of order 9.

Remark. The Hughes plane Ψ is clearly self-dual, as otherwise a fifth plane would exist.

Unfortunately, proving that these are the only four finite projective planes of order 9 is far more difficult. A computer-aided search, like that of the planes of order 10, was conducted in [4], which ended in a negative. As such, it is now well-known that there are only exactly four non-isomorphic finite projective planes of order 9, namely Φ, Ω, Ω^D, and Ψ. This is the first order of a plane for which a significant volume of additional theory linking algebra and geometry is inevitably introduced, leading to further insight to the full understanding of finite projective planes. Ultimately, the theory of finite projective planes is still far from complete.

Bibliography

[1] A A Albert and R Sandler. *An introduction to finite projective planes*. New York: Holt, Rinehart, and Winston, 1968.

[2] S Asgarli. "Wedderburn's little theorem". In: (2013). URL: https://bit.ly/2yjJ8yK.

[3] R C Bose. "On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares". In: 3 (1938), pp. 323–338.

[4] L Thiel C W H Lam G Kolesova. "A computer search for finite projective planes of order 9". In: Discrete Mathematics 92 (1991), pp. 187–195. URL: https://bit.ly/2K56Of3.

[5] L Thiel C W H Lam and S Swiercz. "The non-existence of finite projective planes of order 10". In: (1989). URL: https://bit.ly/2lfdglj.

[6] H Coxeter. *Projective geometry*. 2nd ed. New York-Berlin: Springer-Verlag, 1987.

[7] F Forbes. "The Bruck–Ryser theorem for projective planes". In: (2014). URL: https://bit.ly/2HWa4UB.

[8] M Hall. "Projective planes". In: Transactions of the American Mathematical Society (1943), pp. 229–277.

[9] M Hall. *Theory of groups*. New York: Macmillan, 1959.

[10] A Heyting. *Axiomatic projective geometry*. 2nd ed. Groningen-Amsterdam: North-Holland & Wolters-Noorfhoff, 1980.

[11] D R Hughes. "A class of non-Desarguesian projective planes". In: (1956). URL: https://bit.ly/2K21qcu.

[12] D Hughes and F Piper. *Projective planes*. Vol. 6. Graduate Texts in Mathematics. New York: Springer-Verlag, 1973.

[13] N V Ivanov. "Affine planes, ternary rings, and examples of non-Desarguesian planes". In: (2016). URL: https://bit.ly/2yn3U0m.

[14] L Kadison and M T Kroman. *Projective geometry and modern algebra*. Boston-Basel-Berlin: Birkhaüser, 1996.

[15] J Kahrstrom. "On projective planes". In: (). URL: https://bit.ly/2HXUPuF.

[16] H Klein. 2001. URL: https://bit.ly/2t6PNqM.

[17] C Wexler L J Paige. "A canonical form for incidence matrices of finite projective planes and their associated latin squares". In: 12 (1953). URL: https://bit.ly/2K21nxk.

[18] P Luschny and F T Adams-Watters. *A246655*. 2014. URL: https://bit.ly/2taVq6G.

[19] J D Swift M Hall and R J Walker. "Uniqueness of the projective plane of order eight". In: Mathematical Tables and Other Aids to Computation 10 (1956), pp. 186–194. URL: https://bit.ly/2JTSVNi.

[20] R Killgrove M Hall J D Swift. "On projective planes Of Order nine". In: (1959). URL: https://bit.ly/2K21rx4.

[21] T Peil. *Duality in projective geometry*. URL: https://bit.ly/2JSYIT9.

[22] X Perrott. "Existence of projective planes". In: (2016). URL: https://bit.ly/2lgXTsR.

[23] J Richter-Gebert. *Perspectives on projective geometry*. Springer, 2011.

[24] T G Room and P B Kirkpatrick. *Miniquaternion geometry*. 1971.

[25] N J A Sloane. *A046712*. URL: https://bit.ly/2yn3OWy.

[26] F Stevenson. *Projective planes*. 1972.

[27] G Tarry. "Le probleme des 36 officiers". In: 1, 2 (1900, 1901), pp. 122–123, 170–203.

[28] R C Vaughan. *Lagrange's four square theorem*. URL: https://bit.ly/2leiv4N.

[29] O Veblen and J Wedderburn. "Non-desarguesian and non-pascalian geometries". In: Transactions of the American Mathematical Society (1907), pp. 379–388.

[30] T Vis. "Coordinatising a projective plane". In: (2009). URL: https://bit.ly/2MBIOyq.

[31] C Weibel. "Survey of non-desarguesian planes". In: Notices of the American Mathematical Society (2007), pp. 1294–1303.

[32] Eric W Weisstein. *Projective plane*. URL: https://bit.ly/2t5Hgoi.