CENTRAL COLLINEATIONS OF FINITE PROJECTIVE PLANES

by

RUSSELL GRANT WOODS

A THESIS

PRESENTED TO THE

FACULTY OF GRADUATE STUDIES AND RESEARCH

OF THE

UNIVERSITY OF MANITOBA

IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

APRIL 1965

ABSTRACT

CENTRAL COLLINEATIONS OF FINITE PROJECTIVE PLANES

by Russell Grant Woods

It is well-known that the structure of the finite projective plane is determined to a great extent by the structure of the collineation group of the plane. In this thesis certain assumptions are made concerning the nature of the action of the collineation group considered as a permutation group on the points and lines of the plane. Assumptions are also made concerning the number and nature of the central collineations that occur in the collineation group, and the way in which these assumptions determine the structure of the plane is investigated. The approach used is that employed in recent papers of Piper and Wagner. In order to carry out this investigation, a development of the elementary theory of the finite projective plane and of aspects of the theory of permutation groups is also given.

The writer wishes to express his thanks to Dr. W. J. Jonsson of the Department of Mathematics for his advice and helpfulness, to Mrs. Elaine Halliday for her patience during the typing of this thesis, and to the late Tom Lehrer, one of whose songs provided the basic idea of the thesis.

TABLE OF CONTENTS

INTRODUCTION

The purpose of this thesis is to develop several recent results concerning the structure of the projective plane. It is shown that the structure of the plane can be deduced to a great extent from a knowledge of the structure of the collineation group of the plane, and more particularly from a knowledge of the properties of the central collineations of the plane.

The thesis is divided into five chapters. In the first chapter a number of elementary properties of central collineations are obtained. In the second chapter the method of co-ordinatizing the projective plane by means of a ternary ring is developed, and the important theorem that a projective plane is alternative if and only if its ternary ring is an alternative field is proved. The third chapter is devoted to a study of finite alternative fields, and it is shown that all finite alternative fields are commutative fields. This, coupled with the result of Chapter 2, yields the important result that all finite alternative planes are Desarguesian.

In the fourth chapter a number of combinatorial theorems, many relying heavily on the theory of permutation groups, are proved. In addition, a purely grouptheoretic result (theorem 4.1) is obtained. The results of Chapter 4 are used repeatedly in Chapter 5.

Chapter 5 is essentially a synthesis of the results of several recent papers of Wagner and Piper (10), (11), and (13). Certain conditions imposed on the collineation group of the projective plane are shown to be sufficient to ensure that the plane is Desarguesian; conditions under which the plane is a translation plane, or the dual of a translation plane, are also found. Thus the structure of the projective plane is shown to be determined to a great extent by the properties of the collineation group of the plane considered as a permutation group on the points and lines of the plane.

FOREWORD

In the body of this thesis it is assumed that the reader is familiar with the terminology and notation of projective geometry, and with the basic properties of the projective plane. The purpose of this foreword is to summarize these basic properties and to define notation not defined elsewhere. The results quoted below can be found in Pickert (9) and in Hall (5).

A projective plane π is a triple $(\mathcal{P}, \mathcal{L}, \varepsilon)$ consisting of a set $\mathcal{P}$ whose elements are called points, a collection $\mathcal{L}$ of distinguished subsets of $\mathcal{P}$, and the set-theoretic membership relation ε relating elements of $\mathcal{P}$ and elements of $\mathcal{L}$. The elements of $\mathcal{L}$ are called lines. If ℓ is a line and P is a point, then "$P \varepsilon \ell$" is defined to mean that P is a member of the distinguished subset ℓ of $\mathcal{P}$. Geometrical language is used throughout; hence "P is on ℓ", "P belongs to ℓ", "ℓ is a line through P", "ℓ contains P", "P is incident with ℓ", and "P is a point of ℓ", are all phrases meaning "$P \varepsilon \ell$". If $P_1, \cdots, P_n$ are all on the same line ℓ, then the points $P_1, \cdots, P_n$ are said to be collinear, and this is symbolized by writing $\equiv P_1, \cdots, P_n$. Similarly, if lines $\ell_1, \cdots, \ell_n$

all pass through the same point P, then the lines $\ell_1, \cdots, \ell_n$ are said to be concurrent. On occasion the symbol ε will be used in its more general sense of denoting set membership. The use of the symbol will always be clear from the context.

A projective plane π obeys the following axioms of incidence :

(1) If $P_1 \varepsilon \mathcal{P}$, $P_2 \varepsilon \mathcal{P}$, $P_1 \neq P_2$, then there exists exactly one line $\ell \varepsilon \mathcal{L}$ such that $P_1 \varepsilon \ell$, $P_2 \varepsilon \ell$.

(2) If $\ell_1 \varepsilon \mathcal{L}$, $\ell_2 \varepsilon \mathcal{L}$, $\ell_1 \neq \ell_2$, then there exists exactly one $P \varepsilon \mathcal{P}$ such that $P \varepsilon \ell_1$, $P \varepsilon \ell_2$.

(3) There exist four distinct points of $\mathcal{P}$, no three of which are collinear.

It immediately follows that there exist four distinct lines of $\mathcal{L}$, no three concurrent. Since a knowledge of two distinct points P_1 and P_2 on a line uniquely determines the line, we shall often denote by P_1P_2 the (unique) line containing both P_1 and P_2. Similarly, if ℓ_1 and ℓ_2 are distinct lines, $\ell_1 \cap \ell_2$ will denote the unique point incident with each.

Suppose that the number of points of a projective plane π is finite (such a plane is called a finite projective plane). Then the following statements are shown to be equivalent:

(1) One line contains exactly (n+1) points.

(2) One point is on exactly (n+1) lines.

(3) Every line contains exactly (n+1) points.

(4) Every point is on exactly (n+1) lines.

(5) There are exactly (n^2+n+1) points in $\mathcal{P}$.

(6) There are exactly (n^2+n+1) lines in $\mathcal{L}$.

These equivalences will be used repeatedly. The <u>order</u> of a finite projective plane π will be said to be n if some line of π contains exactly (n+1) points.

Although the lines of π were defined to be distinguished subsets of the points of π, it is evident from the axioms of incidence that an equivalent characterization of the plane can be obtained by considering the lines to be the primitive elements and defining the points of π to be distinguished subsets of the lines of π; thus a point could be considered to be the set of all lines passing through it. Consequently if the triple $\pi = (\mathcal{P}, \mathcal{L}, \varepsilon)$ is a projective plane, the triple $\pi^* = (\mathcal{L}, \mathcal{P}, \varepsilon^*)$ is also a projective plane where the binary relation ε is defined by

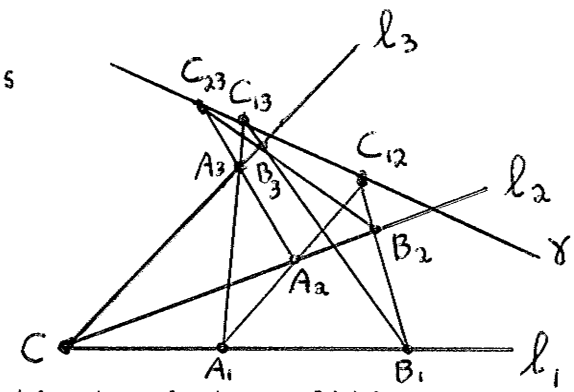
$$\ell \, \varepsilon^* P \Longleftrightarrow P \varepsilon \ell \qquad \text{for all } P \varepsilon \mathcal{P}, \ \ell \varepsilon \mathcal{L}.$$

That π^* is indeed a projective plane can be verified by noting that π^* satisfies the axioms of incidence for a projective plane. π^* is called the projective plane dual to π. It is evident that $(\pi^*)^* = \pi$. Thus every statement about a projective plane π can be "dualized" to a statement about π^* by interchanging the roles of points and lines and replacing ε by ε^*. It follows that if an assertion A is true of a projective plane π, the "dual" assertion A^* will be true of π^*. More generally, if all projective planes satisfying hypotheses H have property K, then all projective planes satisfying the dual hypotheses H^* will have the dual property K^*. This "principle of duality" will be used repeatedly throughout the thesis.

If π is a projective plane and ℓ is a line of π, then by the <u>affine plane</u> π_ℓ we shall mean the projective plane π with the line ℓ and the points thereof deleted. The line ℓ will be called the "line at infinity". Points not on ℓ and lines distinct from ℓ will be called affine points and lines. The concept of the affine plane will be used chiefly to facilitate notation and to aid in the co-ordinatization of the projective plane (see chapter II).

Let C be a point of π and γ a line of π. Let ℓ_1, ℓ_2, ℓ_3 be three arbitrary distinct lines through C (and $\neq \gamma$) and let A_i and B_i be two distinct points of $\ell_i - \{C\}$ $(i = 1,2,3)$. If, for all such A_i, B_i, and ℓ_i, $(A_1A_3 \cap B_1B_3)\varepsilon\gamma$ and $(A_1A_2 \cap B_1B_2)\varepsilon\gamma$ together imply that $(A_2A_3 \cap B_2B_3)\varepsilon\gamma$, then we shall say that Desargues'

(C,γ) theorem holds. If Desargues (C,γ) theorem holds for all points C and lines γ of π, then π will be said to be Desarguesian. The fundamental problem of



this thesis will be to investigate what conditions determine the number of point-line pairs (C,γ) for which Desargues' (C,γ) theorem holds in a given projective plane.

The theory of groups, and in particular the theory of permutation groups, is used extensively throughout the thesis. A self-contained development of the theory of permutation groups appears in chapter IV, and several abstract group theoretical results are proved there as well. However, it is assumed that the reader is familiar with elementary abstract group theory, and with the standard notation employed in that subject. The results used can be found, for instance, in Hall (5).

Lemmas and theorems are numbered independently. Thus for example there is both a lemma 4.4 and a theorem 4.4, and these are distinct.

CHAPTER I

ELEMENTARY PROPERTIES OF COLLINEATIONS

In this chapter several elementary lemmas and theorems about collineations will be proved. Continual reference to these will be made throughout the rest of the paper.

Lemma 1.1 (i) The product of two collineations is a collineation.

(ii) The inverse of a collineation is a collineation.

Proof: (i) Let π be a projective plane with a point set $\mathcal{P}$ and a line set $\mathcal{L}$. Let σ and τ be two collineations of π.

Define a mapping $\sigma\tau$ as follows:

$$P \varepsilon \mathcal{P} \Longrightarrow P^{(\sigma\tau)} = (P^{\sigma})^{\tau}$$
$$\ell \varepsilon \mathcal{L} \Longrightarrow \ell^{(\sigma\tau)} = (\ell^{\sigma})^{\tau}.$$

As $\mathcal{P} \xrightarrow{\sigma} \mathcal{P}$, $\mathcal{L} \xrightarrow{\sigma} \mathcal{L}$ are one-to-one onto mappings and as τ is similarly one-to-one onto, $\sigma\tau$ is a one-to-one onto mapping of $\mathcal{P} \longrightarrow \mathcal{P}$ and $\mathcal{L} \longrightarrow \mathcal{L}$.

To demonstrate that the mapping $\sigma\tau$ preserves incidence, suppose that for $P \varepsilon \mathcal{P}$ and $\ell \varepsilon \mathcal{L}$, $P \varepsilon \ell$. Then $P^{\sigma} \varepsilon \ell^{\sigma}$ (as σ is a collineation), and similarly $(P^{\sigma})^{\tau} \varepsilon (\ell^{\sigma})^{\tau}$ (as τ is a collineation). By definition of $\sigma\tau$, this implies that $P^{(\sigma\tau)} \varepsilon \ell^{(\sigma\tau)}$. Hence

$$P \varepsilon \ell \Longrightarrow P^{(\sigma\tau)} \varepsilon \ell^{(\sigma\tau)};$$

thus $\sigma\tau$ preserves incidence and by definition is a collineation.

(ii) Let σ be a collineation of π projective plane π.

Define a mapping $\mathcal{P} \xrightarrow{\sigma^{-1}} \mathcal{P}$ and $\mathcal{L} \xrightarrow{\sigma^{-1}} \mathcal{L}$ by

$$P^{\sigma^{-1}} = Q \iff Q^{\sigma} = P \quad (P, Q \varepsilon \mathcal{P})$$

$$\ell^{\sigma^{-1}} = m \iff m^{\sigma} = \ell \quad (\ell, m \varepsilon \mathcal{L}).$$

Then σ^{-1} is a one-to-one onto mapping, since σ is. In addition, σ^{-1} preserves incidence; for suppose that it did not. Then there exist $P \varepsilon \mathcal{P}$ and $\ell \varepsilon \mathcal{L}$ such that

$$P \varepsilon \ell \text{ but } P^{\sigma^{-1}} \not\varepsilon \ell^{\sigma^{-1}} .$$

But as σ is a collineation, it preserves non-incidence; hence

$$(P^{\sigma^{-1}})^{\sigma} \not\varepsilon (\ell^{\sigma^{-1}})^{\sigma} ;$$

$$P \not\varepsilon \ell \quad \text{(from the definition of } \sigma^{-1}\text{)}.$$

This contradicts the assumption that $P \varepsilon \ell$, and thus σ^{-1} is an incidence-preserving mapping and hence a collineation. It is the inverse of σ since by definition of σ^{-1}, the mappings $\sigma\sigma^{-1}$ and $\sigma^{-1}\sigma$ fix π elementwise.

<u>Corollary</u>: The set of all collineations of a projective plane π forms a group.

<u>Proof</u>: This follows from the theorem and from the associativity of mappings.

<u>Definition</u>: The trivial collineation (also called the identity collineation) is the collineation that fixes every point and line of the plane.

<u>Lemma 1.2</u> Let π be a projective plane and σ a non-trivial collineation of π. Let there exist a line $\ell \varepsilon \pi$ such that σ fixes every point on ℓ. Then there exists a point $A \varepsilon \pi$ such that σ fixes every line through A.

<u>Proof</u>: Pick an arbitrary point $P \varepsilon \pi$ such that $P \not\varepsilon \ell$, and consider the point P^σ. Then $P^\sigma \not\varepsilon \ell$; for otherwise $(P^\sigma)^\sigma = P^\sigma$, and application of σ^{-1} gives $P^\sigma = P$, which implies that $P \varepsilon \ell$, contrary to hypothesis. There are now two cases:

(i) $P^\sigma \neq P$. Then $PP^\sigma \cap \ell$ is a well-defined point which we will denote as Q.

Now $\qquad \equiv P, P^\sigma, Q$;

thus $\qquad (PQ)^\sigma = P^\sigma Q^\sigma = P^\sigma Q \quad (\text{as } Q \varepsilon \ell)$

$$= PQ$$

and thus the line PQ is fixed by σ.

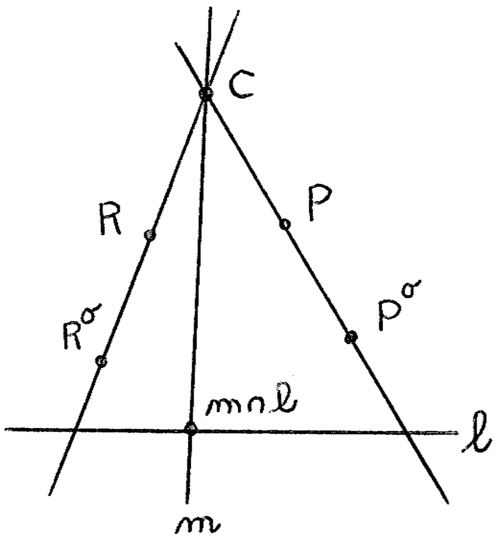
Pick an arbitrary point R, $R \not\varepsilon \ell$, $R \not\varepsilon PQ$, and consider the line RR^σ (assuming that $R \neq R^\sigma$). It too is fixed by σ, by the above argument; thus the point

$RR^\sigma \cap PP^\sigma$ is also fixed by σ.

Let $\qquad RR^\sigma \cap PP^\sigma = C.$

(ii) $P^\sigma = P$ (or $R^\sigma = R$). In this case substitute P (or R) in place of C in the following argument.

Again there are two cases; either $C \notin \ell$ or $C \varepsilon \ell$.



Case (i)

(i) Suppose $C \notin \ell$. Let m be an arbitrary line through C. Then $m \cap \ell \neq C$, and we have

$$m = (m \cap \ell)C.$$

Thus

$$m^\sigma = [(m \cap \ell)C]^\sigma = (m \cap \ell)^\sigma C^\sigma = (m \cap \ell)C = m.$$

Thus all lines through C are fixed by σ, and C is the desired point A.

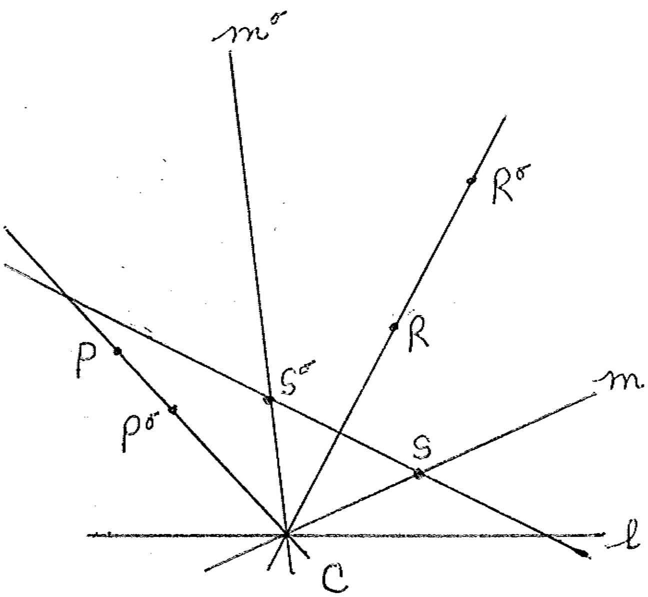
(ii) Suppose $C \varepsilon \ell$. Let m be an arbitrary line through C and let S be a point on m ($S \neq C$). Then $S^\sigma \varepsilon m^\sigma$, and by the argument used above, SS^σ is fixed by σ. Hence if $S^\sigma \varepsilon m$, we have

$$m = CS$$

$$m^\sigma = C^\sigma S^\sigma = CS^\sigma = m$$ (as $\ell^\sigma = \ell$, and if $m \neq \ell$, $S \notin \ell$ implies $S^\sigma \notin \ell$)

and m is fixed by σ. If $S^\sigma \notin m$, then $SS^\sigma \neq m$ and $SS^\sigma \notin m^\sigma$. Thus

$$SS^\sigma \cap PP^\sigma \neq SS^\sigma \cap RR^\sigma \quad \text{(see diagram)}$$



and so $SS^\sigma \cap PP^\sigma$ and $SS^\sigma \cap RR^\sigma$ are distinct points $\notin \ell$ and fixed by σ. By the argument of case (i), it follows that all lines through each point are fixed, and thus σ fixes all points and lines of π. This contradicts the assumption that σ is non-trivial; hence $S^\sigma \notin m$ is impossible and all lines through C are fixed.

The dual of this theorem is also true:

<u>Corollary</u>: If σ is a collineation of π and P a point of π such that σ fixes all lines through P, then there exists a line ℓ of π such that σ fixes all points on ℓ.

<u>Definition</u>: A collineation σ that fixes all points on the line ℓ and all lines through the point C is called a (C,ℓ)-collineation, or a central collineation. ℓ is called the axis of the collineation, and C is called its centre.

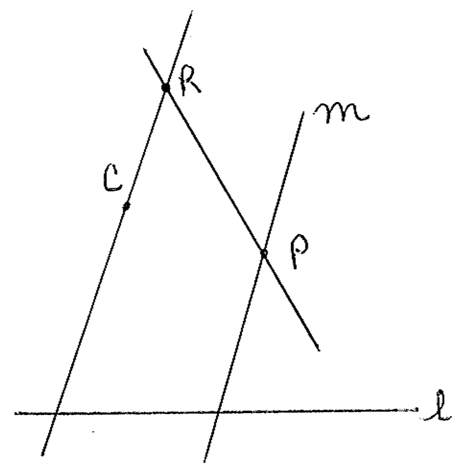
If $C \in \ell$, then σ is called a (C,ℓ)-elation; if $C \notin \ell$, then σ is called a (C,ℓ)-homology.

<u>Lemma 1.3</u> A (C,ℓ)-collineation σ that fixes a point P, $P \neq C$ and $P \notin \ell$, is the identity collineation.

<u>Proof</u>: Let m be an arbitrary line through P. Then m is of the form PQ, where $Q = m \cap \ell$ and hence $Q \neq P$. Thus

$$m^{\sigma} = (PQ)^{\sigma} = P^{\sigma}Q^{\sigma} = PQ$$

since P and Q are both fixed points of σ. The two distinct points P and C then have the property that a line through either of them is fixed. Let R be a point not on CP. Then $R = PR \cap CR$ and $R^{\sigma} = (PR \cap CR)^{\sigma} = PR \cap CR = R$. Thus all points of the plane not on CP are fixed by σ. A similar argument in which P is replaced by $\bar{P}$, where



$\bar{P} \notin CP$, $\bar{P} \in \ell$, shows that all points on CP are fixed by σ. Hence σ fixes all points of the plane, and as it preserves incidence, it fixes all lines of the plane. Hence $$\sigma = 1.$$

By the principle of duality, we have the

<u>Corollary</u> A (C, ℓ)-collineation σ that fixes a line m, $m \neq \ell$ and $C \notin m$, is the identity collineation.

<u>Lemma 1.4</u> A (C, ℓ)-collineation σ is determined by the image under σ of a point P (or, by the principle of duality, a line m) if $P \neq C$ and $P \notin \ell$ (dually, $m \neq \ell$ and $C \notin m$).

<u>Proof</u>: Let σ_1 and σ_2 be two (C, ℓ)-collineations. By lemma 1, $\sigma_1\sigma_2^{-1}$ is also a (C, ℓ)-collineation.

Let P be a point such that $P^{\sigma_1} = P^{\sigma_2}$ ($P \neq C$, $P \not\in \ell$).

Then

$$P^{\sigma_1 \sigma_2^{-1}} = P,$$

and by the previous lemma, $\sigma_1 \sigma_2^{-1} = 1$.

As inverses are unique, this means that $\sigma_1 = \sigma_2$, which proves the lemma.

<u>Lemma 1.5</u> Let σ_1 be a (C_1, ℓ)-elation and σ_2 a (C_2, ℓ)-elation. Then either one of the following occurs:

(i) $C_1 = C_2$ and $\sigma_1 \sigma_2$ is a (C_1, ℓ)-elation.

(ii) $C_1 \neq C_2$ and $\sigma_1 \sigma_2$ is a (C_3, ℓ)-elation for some point C_3 with $C_1 \neq C_3 \neq C_2$.

<u>Proof</u>: (i) If P is a point and m a line such that $P \varepsilon \ell$ and $C \varepsilon m$, then

$$P^{\sigma_1} = P = P^{\sigma_2}, \; m^{\sigma_1} = m = m^{\sigma_2} \; ;$$

hence $P^{\sigma_1 \sigma_2} = P$ and $m^{\sigma_1 \sigma_2} = m$. Thus $\sigma_1 \sigma_2$ is a (C_1, ℓ)-elation.

(ii) As both σ_1 and σ_2 fix each point on ℓ, $\sigma_1 \sigma_2$ does. Hence by lemma 2, there exists a point C_3 such that $\sigma_1 \sigma_2$ fixes all lines through C_3. In order to prove that $C_3 \varepsilon \ell$, it suffices to show that $\sigma_1 \sigma_2$ fixes no point of $\pi - \{\ell\}$. If $P \not\in \ell$ and $P^{\sigma_1 \sigma_2} = P$, then $P^{\sigma_1} = P^{\sigma_2^{-1}}$. But σ_2^{-1} is evidently a (C_2, ℓ)-collineation, so $P^{\sigma_1} \varepsilon C_1 P$ and $P^{\sigma_1} \varepsilon C_2 P$. Thus as $\not\equiv C_1, C_2, P$, it follows that $P^{\sigma_1} = P^{\sigma_2^{-1}} = P$; thus both σ_1 and σ_2 are trivial (i.e. are the identity collineation) by lemma 1.3, contrary to hypothesis. Hence $\sigma_1 \sigma_2$ fixes only points on , and is thus an elation.

If $C_3 = C_1$, then $\sigma_2 = \sigma_1^{-1}(\sigma_1\sigma_2)$ is a (C_1, ℓ)-elation (by case (i)), contradicting the hypothesis that $C_1 \neq C_2$. Thus $C_1 \neq C_3 \neq C_2$.

<u>Corollary I</u>: The set of all (C_1, ℓ)-elations forms a group, provided that the identity collineation is counted as a (C, ℓ)-elation for all point-line pairs (C, ℓ).

<u>Corollary II</u>: The set of all elations with a given axis ℓ forms a group, provided that the identity collineation is considered to be such an elation.

<u>Definition</u>: A projective plane π is said to be (C, ℓ)-transitive if, for arbitrary points $P, Q \not\in \ell$ such that $\equiv P, Q, C$, and $P \neq C \neq Q$ there is a (C, ℓ)-collineation σ such that $P^\sigma = Q$.

<u>Lemma 1.6</u> Let π be a projective plane that is (C, γ)-transitive, and let σ be a (C, γ)-collineation and φ an arbitrary collineation. Then $\varphi^{-1}\sigma\varphi$ is a $(C^\varphi, \gamma^\varphi)$-collineation and π is $(C^\varphi, \gamma^\varphi)$-transitive.

<u>Proof</u>: Let $P \varepsilon \gamma^\varphi$; then $P^{\varphi^{-1}} \varepsilon \gamma$, and $P^{\varphi^{-1}\sigma} \varepsilon \gamma^\sigma = \gamma$ (as σ is a (C,γ)-collineation). Hence $P^{\varphi^{-1}\sigma\varphi} \varepsilon \gamma^\varphi$. But as $P^{\varphi^{-1}} \varepsilon \gamma$, $P^{\varphi^{-1}\sigma} = P^{\varphi^{-1}}$ as σ fixes points on γ. Hence $P^{\varphi^{-1}\sigma\varphi} = P^{\varphi^{-1}\varphi} = P$, i.e. $\varphi^{-1}\sigma\varphi$ fixes points on γ^φ. The dual argument gives that $\varphi^{-1}\sigma\varphi$ fixes all lines through C^φ, and hence $\varphi^{-1}\sigma\varphi$ is a $(C^\varphi, \gamma^\varphi)$-collineation.

Pick distinct points A and B in the plane, arbitrary except that $\equiv A, B, C^{\varphi}$, $A \neq C^{\varphi}$, $B \neq C^{\varphi}$, and $A, B \notin {}^{\varphi}$. As φ^{-1} is a collineation, this means that $\equiv A^{\varphi^{-1}}, B^{\varphi^{-1}}, C$. As the plane is (C, γ)-transitive, there exists a (C, γ)-collineation σ such that $(A^{\varphi^{-1}})^{\sigma} = B^{\varphi^{-1}} \therefore A^{\varphi^{-1}\sigma\varphi} = B^{\varphi^{-1}\varphi} = B$. But $\varphi^{-1}\sigma\varphi$ is a $(C^{\varphi}, \gamma^{\varphi})$-collineation; hence, as A and B were arbitrary, the plane is $(C^{\varphi}, \gamma^{\varphi})$-transitive.

<u>Definition</u>: (a) A projective plane π is said to be a translation plane with respect to the line ℓ if π is (C, ℓ)-transitive for all points C on ℓ.

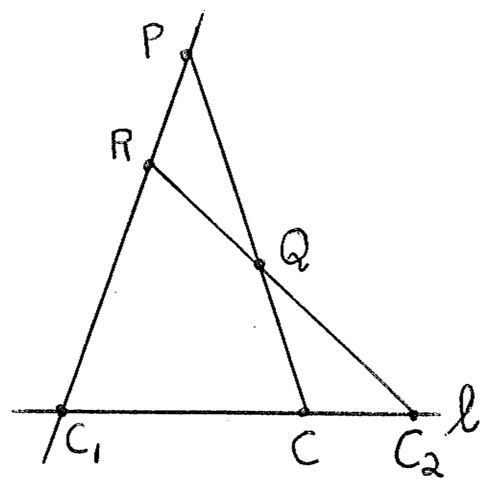
(b) The projective plane π is said to be the dual of a translation plane with respect to the point P if π is (P, ℓ)-transitive for all lines through P.

(c) If π is a translation plane with respect to a line ℓ, then the group of all elations with axis ℓ is called the translation group of π.

<u>Lemma 1.7</u> Let π be a projective plane containing a line ℓ and distinct points C_1 and C_2 on ℓ. If π is (C_1, ℓ)- and (C_2, ℓ)-transitive, then it is a translation plane with respect to ℓ.

<u>Proof</u>: Let C be an arbitrary point on ℓ, $C_1 \neq C \neq C_2$. Let P and Q be arbitrary points of π such that $\equiv P, Q, C$ and $P, Q \notin \ell$. As $C_1 \neq C_2$, the point $C_1P \cap C_2Q$ is well-defined; denote it by R.

As π is (C_1, ℓ)-transitive and as $\equiv P, R, C_1$, there exists a (C_1, ℓ)-elation σ_1 such that $P^{\sigma_1} = R$. Similarly there exists a (C_2, ℓ)-elation σ_2 such that $R^{\sigma_2} = Q$. Hence $P^{\sigma_1\sigma_2} = Q$. But by lemma 1.5, $\sigma_1\sigma_2$ is a (C, ℓ)-elation, and evidently it maps P onto R. Hence as C was arbitrary in π, and as P and Q were arbitrary points satisfying $\equiv P, Q, C$, it follows that π is (C, ℓ)-transitive for all $C \varepsilon \ell$. Hence π is a translation plane with respect to ℓ.



<u>Lemma 1.8</u> Let π be a translation plane with respect to the line ℓ. If α is a collineation then π is a translation plane with respect to ℓ^{α}.

<u>Proof</u>: Let C be an arbitrary point of ℓ^{α}. Then there exists a point $\bar{C} \varepsilon \ell$ such that $\bar{C}^{\alpha} = C$. As π is a translation plane with respect to ℓ, π is $(\bar{C}, \ell)$-transitive. Then by lemma 1.6, π is $(\bar{C}^{\alpha}, \ell^{\alpha})$-transitive, i.e. (C, ℓ^{α})-transitive. As C was arbitrary on ℓ^{α}, π is a translation plane with respect to ℓ^{α}.

<u>Corollary</u>: If π is a translation plane with respect to two lines ℓ_1 and ℓ_2 intersecting at a point P, then it

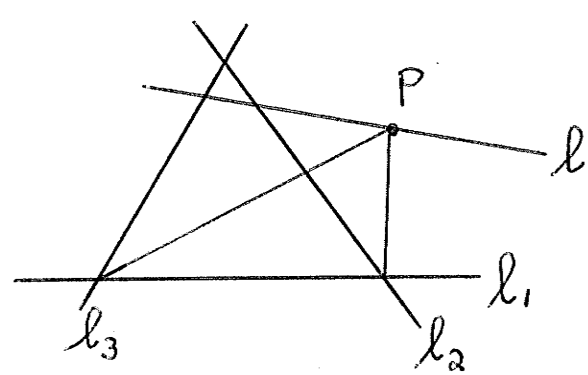
is a translation plane with respect to every line of the plane that passes through P.

Proof: Let m be an arbitrary line through P ($\ell_1 \neq m$). As π is a translation plane with respect to ℓ_1, there is a (C, ℓ_1)-elation σ ($C \neq P$) such that $\ell_2^{\sigma} = m$. By lemma 1.8, since π is a translation plane with respect to ℓ_2, it is also a translation plane with respect to m. As m was arbitrary, π is a translation plane with respect to all lines through P.

Definition: An alternative plane π is a projective plane that is a translation plane with respect to every line of the plane.

Lemma 1.9 If π is a translation plane with respect to three non-concurrent lines ℓ_1, ℓ_2, ℓ_3, then it is an alternative plane.

Proof: Let ℓ be an arbitrary line of π. If ℓ passes through any of $\ell_1 \cap \ell_2$, $\ell_1 \cap \ell_3$, $\ell_2 \cap \ell_3$, then by the corollary of lemma 1.8, π is a translation plane with respect to ℓ . If ℓ passes through none of these, choose an arbitrary point $P \varepsilon \ell$, and without loss of generality, assume $P \notin \ell_1$. Then as above, π is a translation plane with respect to the distinct lines $(\ell_1 \cap \ell_2)P$ and



$(\ell_1 \cap \ell_3)P$. Thus it is a translation plane with respect to all lines through P, and in particular ℓ. As ℓ was arbitrary, π must be an alternative plane.

<u>Theorem 1.1</u> Let π be a projective plane and let ℓ be a line of π. Let there exist non-trivial elations σ_1 and σ_2 with axis ℓ and with centres C_1 and C_2, $C_1 \neq C_2$. Then $G(\ell)$, the group of all elations with axis ℓ, is either infinite abelian or elementary abelian.

<u>Proof</u>: We first prove that $G(\ell)$ is abelian. By lemma 1.4, it suffices to show that for an arbitrary point $A \notin \ell$, $A^{\sigma_1\sigma_2} = A^{\sigma_2\sigma_1}$.

Since σ_2 fixes all lines through C_2,

$$(A^{\sigma_1}C_2)^{\sigma_2} = A^{\sigma_1}C_2$$

But $(A^{\sigma_1}C_2)^{\sigma_2} = A^{\sigma_1\sigma_2}C_2$

and so $\equiv A^{\sigma_1}, A^{\sigma_1\sigma_2}, C_2$.

However, $\equiv A^{\sigma_1}, A, C_1$

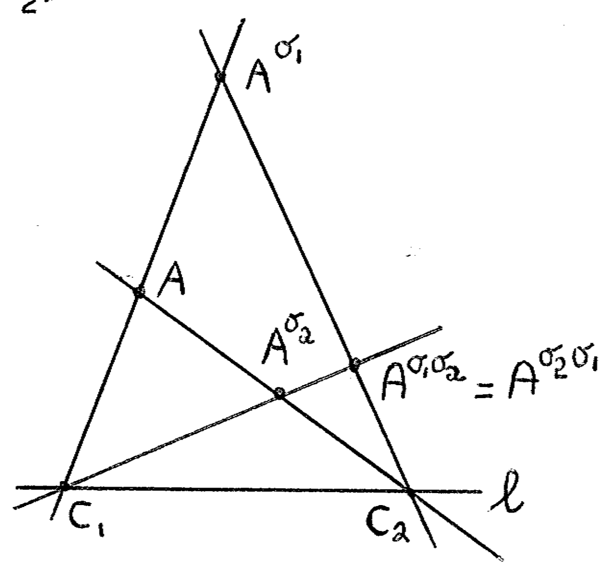
and hence $\equiv A^{\sigma_1\sigma_2}, A^{\sigma_2}, C_1$.

Thus as $A^{\sigma_2}C_1 \neq A^{\sigma_1}C_2$ (as $C_1 \neq C_2$), it follows that

$$A^{\sigma_1\sigma_2} = C_1A^{\sigma_2} \cap C_2A^{\sigma_1}$$

Analogously $A^{\sigma_2\sigma_1} = C_2A^{\sigma_1} \cap C_1A^{\sigma_2}$

$$= A^{\sigma_1\sigma_2}.$$



Thus $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Evidently by the same argument, any two elations with distinct centres and the same axis ℓ will commute. Further, two distinct elations of

$G(\mathcal{L})$ with the same centre will commute; for let σ_1 and σ_1^* be $(C_1, \mathcal{L})$-elations. Then by lemma 5, $\sigma_1^*\sigma_2$ and $\sigma_1\sigma_2$ have centres $\neq C_1, C_2$; thus by the above

$$\begin{aligned}\sigma_2(\sigma_1\sigma_1^*) &= (\sigma_1\sigma_1^*)\sigma_2 = \sigma_1(\sigma_1^*\sigma_2)\\ &= (\sigma_1^*\sigma_2)\sigma_1 = (\sigma_2\sigma_1^*)\sigma_1\\ &= \sigma_2(\sigma_1^*\sigma_1).\end{aligned}$$

Multiplying on the left by σ_2^{-1},

$$\sigma_1\sigma_1^* = \sigma_1^*\sigma_1.$$

Thus $G(\mathcal{L})$ is abelian as claimed.

If $G(\mathcal{L})$ has an element of finite order, then it has an element σ_1 with centre C_1 of prime order p. If σ_2 is an arbitrary non-trivial element of $G(\mathcal{L})$ with centre $C_2 \neq C_1$, then

$$\begin{aligned}(\sigma_1\sigma_2)^p &= \sigma_1^p\sigma_2^p \qquad \text{(as } G(\mathcal{L}) \text{ is abelian)}\\ &= \sigma_2^p.\end{aligned}$$

As any power of an elation has the same centre as the elation, $(\sigma_1\sigma_2)^p$ has centre C_2, as σ_2^p has. This contradicts lemma 1.5 unless $(\sigma_1\sigma_2)^p = 1$, i.e. unless

$$\sigma_2^p = 1.$$

Thus all elations of $G(\mathcal{L})$ with centre $\neq C_1$, are of order p. By extension of the above argument with σ_2 playing the role of σ_1, all elations with centre C_1 are of order p as well. Hence $G(\mathcal{L})$ is an elementary abelian group.

By the principle of duality we obtain the following

<u>Corollary</u>: Let π be a projective plane and P a point of π. Let there exist non-trivial elations σ_1 and σ_2 with centre P and axes ℓ_1 and ℓ_2, $\ell_1 \neq \ell_2$. Then G(P), the group of all elations with centre P, is either infinite abelian or elementary abelian.

<u>Definition</u>: An involution is a (C,ℓ)-collineation σ such that $\sigma \neq 1$ but $\sigma^2 = 1$. If σ is an elation (homology) of order 2, it is said to be an involutory elation (homology).

<u>Theorem 1.2</u> Let σ be an involution of a projective plane π of order n. Then if n is even, σ is an elation; if n is odd, σ is a homology.

<u>Proof</u>: Let σ have axis ℓ and centre C, and let m be any line $\neq \ell$ such that $C \varepsilon m$. Then σ interchanges points of $m - \{C \cup (m \cap \ell)\}$ in pairs; thus $m - \{C \cup (m \cap \ell)\}$, considered as a point set, has an even number of points. If σ is an elation, then $C = m \cap \ell$ and $m - \{C \cup (m \cap \ell)\}$ contains n points; hence n is even. If σ is a homology, then $C \neq m \cap \ell$ and $m - \{C \cup (m \cap \ell)\}$ contains n-1 points. Thus n-1 is even, i.e. n is odd.

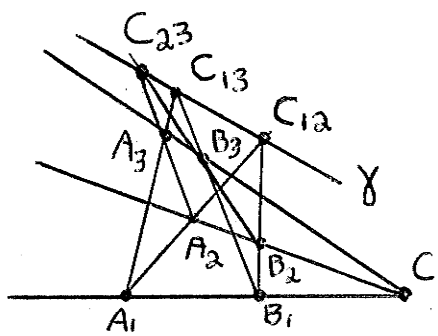
<u>Theorem 1.3</u> Desargues' (C, γ) theorem holds in a projective plane if and only if the plane is (C, γ)-transitive.

<u>Proof</u>: First suppose that for a particular line γ and point C the plane is (C, γ)-transitive. Let

C, A_1, A_2, A_3, B_1, B_2, B_3 be seven distinct points such that $\equiv C, A_1, B_1$, $\equiv C, A_2, B_2$, and $\equiv C, A_3, B_3$. Suppose that $C_{12} = A_1A_2 \cap B_1B_2 \varepsilon \gamma$ and that $C_{13} = A_1A_3 \cap B_1B_3 \varepsilon \gamma$. It must be shown that $C_{23} = A_2A_3 \cap B_2B_3$ also lies on γ.

From the above conditions it follows that γ does not pass through A_i or B_i $(i = 1,2,3)$, so as there exists (C,γ)-transitivity, there exists a (C,γ)-collineation σ such that $A_1^{\sigma} = B_1$.

$$\text{Thus } A_2^{\sigma} = (C_{12}A_1 \cap CA_2)^{\sigma}$$
$$= C_{12}^{\sigma}A_1^{\sigma} \cap CA_2$$
$$= C_{12}B_1 \cap CA_2 = B_2$$



A similar argument shows that $A_3^{\sigma} = B_3$.

Thus

$$A_2A_3 \cap \gamma = (A_2A_3 \cap \gamma)^{\sigma} = A_2^{\sigma}A_3^{\sigma} \cap \gamma = B_2B_3 \cap \gamma .$$

Hence $A_2A_3 \cap B_2B_3 \varepsilon \gamma$, and Desargues' (C,γ) theorem holds.

Conversely, assume that Desargues' (C,γ) theorem holds for a particular point-line pair C and γ. Let A_1 and B_1 be any pair of distinct points $\neq C$ and not on γ such that $\equiv A_1, B_1, C$. Construct a mapping σ, defined on the affine plane (obtained by considering CA_1B_1 to be the line at infinity) as follows:

$$A_1^{\sigma} = B_1$$
$$C^{\sigma} = C$$

$$P \in \gamma \Rightarrow P^\sigma = P$$

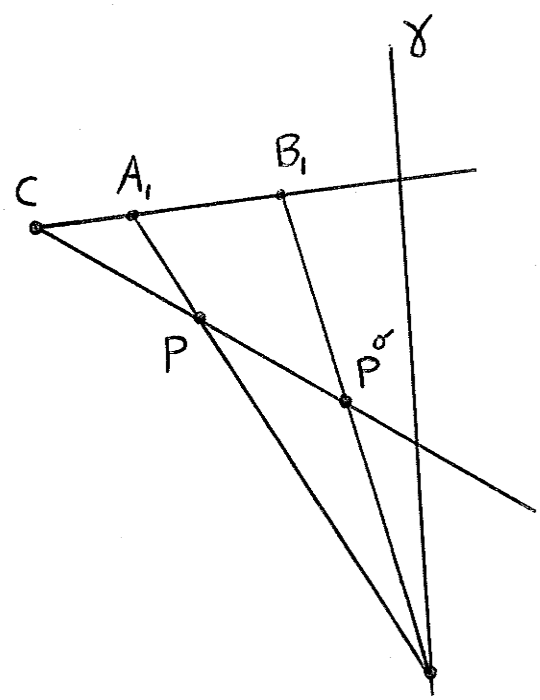
$$P \notin \gamma,\ P \notin A_1C, \Longrightarrow P^\sigma = CP \cap ((A_1P \cap \gamma)B_1).$$

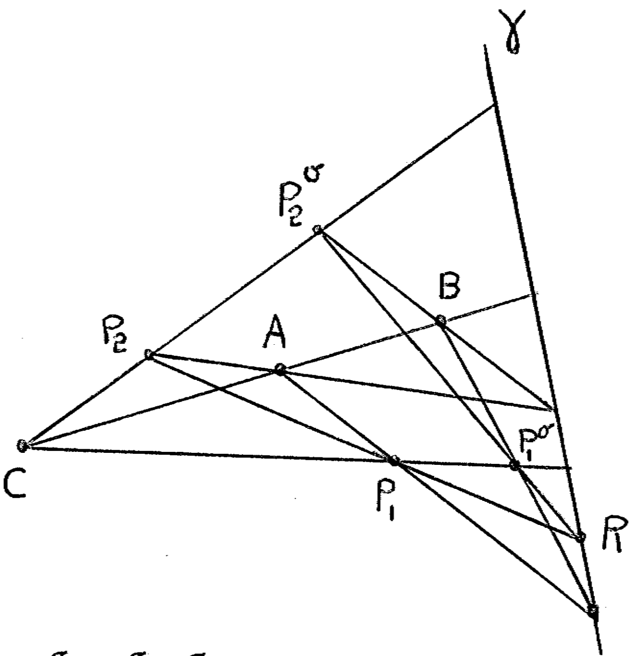
It will now be shown that the mapping σ preserves incidence in the affine plane, i.e. that $P \notin CA_1,\ P \in \ell, \Longrightarrow P^\sigma \in \ell^\sigma$. This will imply that σ maps parallel classes of lines into parallel classes of lines, and hence that a point on CA_1 is mapped into another point on CA_1. Hence σ will be shown to be an incidence-preserving mapping, and in fact to be a (C,γ)-collineation sending $A_1 \longrightarrow B_1$. Thus as A_1 and B_1 were arbitrary as described above, the plane will be shown to be (C,γ)-transitive.

Let P_1 and P_2 be two distinct points not in $\{\gamma \cup C\}$. Let $R = P_1P_2 \cap \gamma$.

If $\equiv C, P_1, P_2$ then by definition of σ both P_1^σ and P_2^σ are on CR, i.e. $\equiv C, P_1^\sigma, P_2^\sigma, R$, and thus

$$\equiv P_1, P_2, R \Rightarrow \equiv P_1^\sigma, P_2^\sigma, R.$$





If $\not\equiv C, P_1, P_2$, construct P_1^σ and P_2^σ and apply Desargues (C,γ) theorem; as $AP_1 \cap BP_1^\sigma \varepsilon \gamma$ and $AP_2 \cap BP_1^\sigma \varepsilon \gamma$, it follows that $P_1^\sigma P_2^\sigma \cap P_1P_2 \varepsilon \gamma$, i.e. that

$$\equiv P_1^\sigma, P_2^\sigma, R.$$

Hence in general

$$\equiv P_1, P_2, R \Longrightarrow \equiv P_1^\sigma, P_2^\sigma, R^\sigma.$$

Thus suppose that A,B,D are arbitrary distinct collinear points not = C nor on γ.

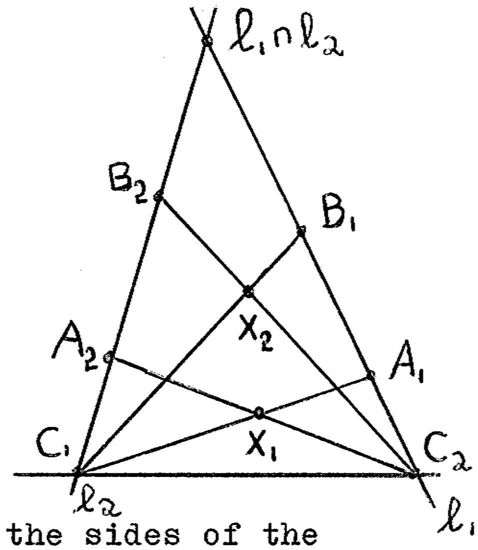
Let $ABD \cap \gamma = R$.

Thus $\equiv A,B,R$ and $\equiv B,D,R$. Hence by the above work, $\equiv A^\sigma, B^\sigma, R$ and $\equiv B^\sigma, D^\sigma, R$, so $\equiv A^\sigma, B^\sigma, D^\sigma$. Hence σ preserves incidence and hence is a collineation; it follows, as remarked earlier, that the plane is (C,γ)-transitive.

<u>Lemma 1.10</u> (See Ostrom (6), lemma 6.) Let π be a projective plane and let σ_1 and σ_2 be two involutory homologies of π with centres C_1 and C_2 respectively and axes ℓ_1 and ℓ_2 respectively. If $C_1 \varepsilon \ell_2$ and $C_2 \varepsilon \ell_1$, then $\sigma_1\sigma_2$ is an involutory homology with centre $\ell_1 \cap \ell_2$ and axis C_1C_2.

<u>Proof</u>: As the points C_1, C_2, and $\ell_1 \cap \ell_2$ are fixed by

both σ_1 and σ_2, they are fixed by $\sigma_1\sigma_2$. Similarly the lines ℓ_1, ℓ_2, and $C_1 \cap C_2$ are fixed by σ_1, σ_2, and $\sigma_1\sigma_2$. Let A_1 and B_1 be two points of ℓ_1 interchanged by σ_2 (as $\sigma_2{}^2 = 1$, points of π are either fixed by σ_2 or are interchanged in pairs). Since σ_1 fixes all points on ℓ_1, $\sigma_1\sigma_2$ also interchanges A_1 and B_1. Similarly, if σ_1 interchanges A_2 and B_2 on ℓ_2, then $\sigma_1\sigma_2$ interchanges these also. Thus points on ℓ_1 and ℓ_2 (with the exception of C_1, C_2, and $\ell_1 \cap \ell_2$) are interchanged in pairs by $\sigma_1\sigma_2$.



Let X_1 be any point not on the sides of the triangle $C_1C_2(\ell_1 \cap \ell_2)$. Let $C_1X_1 \cap \ell_1 = A_1$ and $C_2X_1 \cap \ell_2 = A_2$. Let $A_1 \rightleftarrows B_1$ and $A_2 \rightleftarrows B_2$ under $\sigma_1\sigma_2$. Then if $C_1B_1 \cap C_2B_2 = X_2$, evidently $X_1 \rightleftarrows X_2$ under $\sigma_1\sigma_2$. Thus all points of π are either fixed or interchanged in pairs by $\sigma_1\sigma_2$, so $(\sigma_1\sigma_2)^2 = 1$.

Let $X_1X_2 \cap C_1C_2 = R$.

$$\text{Then} \quad (X_1X_2 \cap C_1C_2)^{\sigma_1\sigma_2} = (X_1X_2)^{\sigma_1\sigma_2} \cap (C_1C_2)^{\sigma_1\sigma_2}$$
$$= X_1X_2 \cap C_1C_2 = R$$

as $\sigma_1\sigma_2$ fixes the line X_1X_2 (as it interchanges X_1 and X_2) and the line C_1C_2 (as both σ_1 and σ_2 do). Thus all points on C_1C_2, and dually all lines through $\ell_1 \cap \ell_2$, are fixed by $\sigma_1\sigma_2$. Hence $\sigma_1\sigma_2$ is an involutary homology with centre $\ell_1 \cap \ell_2$ and axis C_1C_2.

<u>Lemma 1.11</u> (See Piper (10), result 5.) Let π be a finite projective plane and let ℓ be a line of π. Let ℓ possess a point Q with the property that $P \varepsilon \ell$ $(P \neq Q)$ implies that there exists a non-trivial (P, ℓ)-elation. Then there exists a non-trivial (Q, ℓ)-elation.

<u>Proof:</u> Let π have order n and let the points of ℓ be labelled $P_1, \cdots, P_n, Q$. Let m be an arbitrary line through Q $(m \neq \ell)$. Let α_i be a non-trivial (P_i, ℓ)-elation, i = 1 to n.

Then

$$m^{\alpha_i} \neq m, \quad i = 1 \text{ to } n \ (\text{as } m \cap \ell \neq P_i, \ i = 1 \text{ to } n).$$

Hence m has n images under the set $\{\alpha_i\}$, but no more than (n-1) of these can be distinct, as m and ℓ are not possible images and there are (n+1) lines through Q. Hence there exist j and k $(1 \leq j \leq n,\ 1 \leq k \leq n)$ such that

$$m^{\alpha_j} = m^{\alpha_k}, \qquad j \neq k.$$

Thus $\quad m^{\alpha_j\alpha_k^{-1}} = m \quad$ and $\quad \alpha_j\alpha_k^{-1} \neq 1 \quad$ as $j \neq k$.

But by lemma 1.5, $\alpha_j\alpha_k^{-1}$ is an elation with axis ℓ, and as it fixes m, its centre must be Q. Hence $\alpha_j\alpha_k^{-1}$ is a non-trivial (Q, ℓ)-elation.

CHAPTER II

THE CO-ORDINATIZATION OF THE PROJECTIVE PLANE

The following treatment is patterned after that of Pickert (8). However, the ternary ring introduced by Hall (5) is also discussed, and its relation to that of Pickert is treated in some detail.

THE ASSIGNING OF CO-ORDINATES

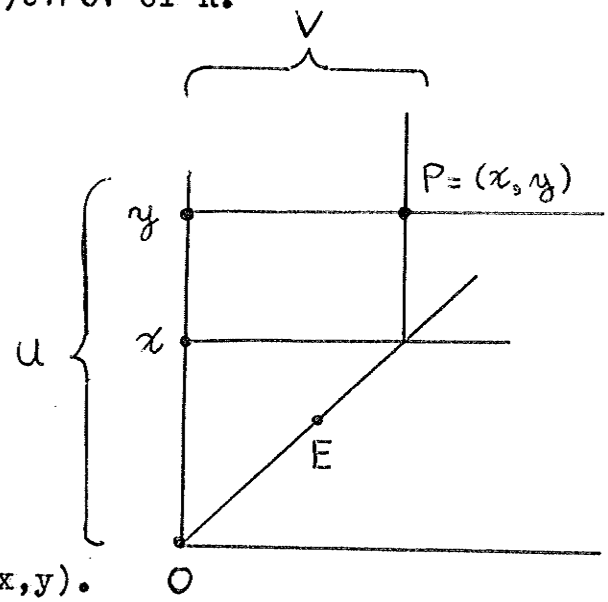
Let π be an arbitrary projective plane, and let UVOE be an arbitrarily chosen non-degenerate quadrangle of π. The line UV, henceforth called the line at infinity, together with its points, is now deleted from π, and the resulting affine plane is denoted as $\bar{\pi}$. The points of $\bar{\pi}$ are called affine points. Let

$$R = \{P \mid P \varepsilon OV,\ P \varepsilon \bar{\pi}\}.$$

If π is a finite plane of order n, then R possesses n distinct elements, which henceforth shall be denoted by $\{o, 1, a, b, \cdots\}$. The special elements o and 1 are identified with the points O and $UE \cap OV$ respectively. Because $\bar{\pi}$ can be extended in one and only one way (apart from isomorphism) to a projective plane, diagrams can without confusion be drawn in the affine plane. Braces will indicate pencils of lines passing through the same point on the line at infinity.

The points of π are now co-ordinatized as follows. To each point P of $\bar{\pi}$ is assigned an ordered pair of elements of R. The members of this pair are called the "co-ordinates" of P, and are assigned as follows: P has co-ordinates (x,y), where y is the element $UP \cap OV$ of R and x is the element $(PV \cap OE)U \cap OV$ of R.

It is customary to identify a point of $\bar{\pi}$ with its co-ordinate pair, as there is a one-to-one correspondence between the points of the affine plane and the elements of RxR. Thus if $P \varepsilon \bar{\pi}$ has co-ordinates (x,y), one writes P = (x,y).



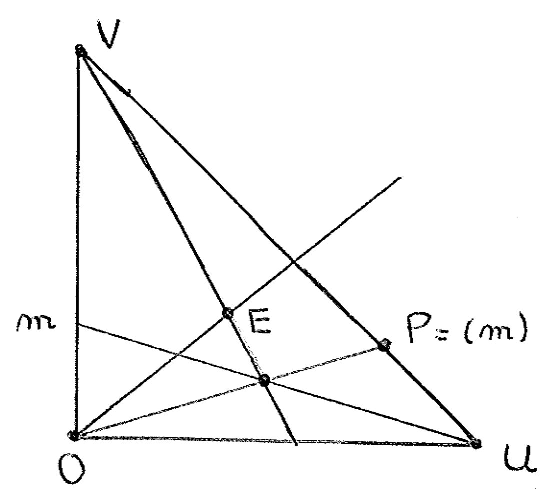
The "points at infinity", i.e. those on the line UV, are assigned singleton co-ordinates as follows:

(1) V is given the co-ordinate (∞)

(2) $P \neq V$ is given the co-ordinate (m) where $OP \cap VE = (1,m)$.

It is easily verified that the singleton co-ordinate (m) of (2) is well-defined and that $P_1 = (m)$, $P_2 = (m)$ if and only if $P_1 = P_2$.

In co-ordinatizing lines of the affine plane, a distinction is made between the pencil of lines through V and the remaining lines of the affine plane. If $\ell \varepsilon \bar{\pi}$ and $V \varepsilon \ell$, then ℓ



is assigned the singleton co-ordinate $[x]$, where $\ell \cap OE = (x,x)$ defines the element $x \varepsilon R$. As $\ell \cap OE$ is well-defined, x also is.

If $\ell \varepsilon \bar{\pi}$ and $V \notin \ell$, ℓ is assigned the ordered pair $[m,b]$ as its co-ordinates, where m is defined by $\ell \cap UV = (m)$ and b is defined by $\ell \cap OV = (o,b)$. The co-ordinate m of a line $[m,b]$ is called the "slope" of the line; affine lines passing through V are said to have "infinite slope".

The line UV is assigned the singleton co-ordinate $[\infty]$. This completes the co-ordinatization of the points and lines of π.

The following special cases are of interest, and are easily verified:

(1) $O = (o,o)$, $E = (1,1)$

If $P \varepsilon \bar{\pi}$:

(2) $P \varepsilon OE \Leftrightarrow P = (x,x)$ for some $x \varepsilon R$

(3) $P \varepsilon OU \Leftrightarrow P = (x,o)$ for some $x \varepsilon R$

(4) $P \varepsilon OV \Leftrightarrow P = (o,y)$ where y is the element of R identified with P.

(5) $P \varepsilon EV \Leftrightarrow P = (1,y)$ for some $y \varepsilon R$

(6) $P \varepsilon EU \Leftrightarrow P = (x,1)$ for some $x \varepsilon R$

(7) $OV = [o]$, $EV = [1]$

(8) $V \notin \ell$, $O \varepsilon \ell \Leftrightarrow \ell = [m,o]$ for some $m \varepsilon R$

(9) $U \varepsilon \ell$, $\ell \neq (\infty) \Leftrightarrow \ell = [o,b]$ for some $b \varepsilon R$

(10) $OU = [o,o]$.

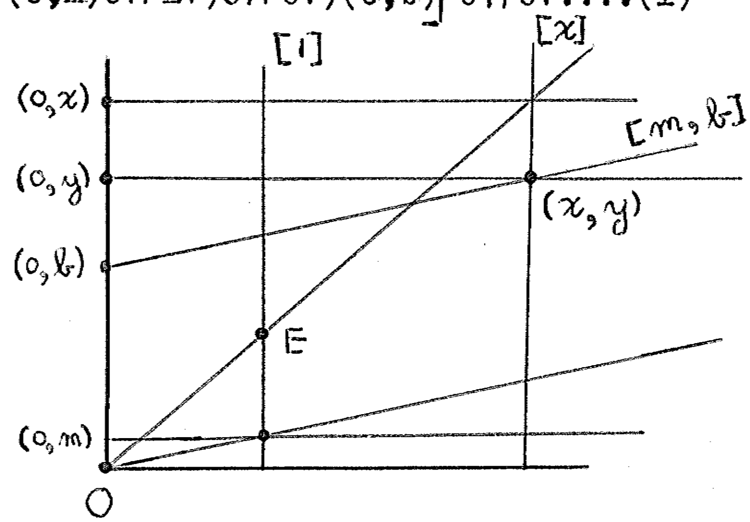
THE TERNARY RING OF π

Closely associated with the co-ordinate set R of a projective plane π is the ternary ring of π. The ternary ring is defined to be the ordered pair (R,T) where R is the set defined previously and T is a ternary function mapping RxRxR onto R and defined as follows: if (m,x,b) is an arbitrary ordered triple of RxRxR, then $y = T(m,x,b) \Longleftrightarrow (x,y) \varepsilon\ m,b$ where we have identified points and lines with their co-ordinates.

Lemma 2.1 T is a well-defined mapping from RxRxR onto R.

Proof: It must be shown that given $(m,x,b) \varepsilon RxRxR$, $T(m,x,b)$ is uniquely determined. Let P be an affine point on $[m,b]$ with first co-ordinate x. Then $PV \cap OE = (x,x)$, and so $P \varepsilon [x]$. Hence $P = [x] \cap [m,b]$ and as two lines intersect in a unique point, P is uniquely determined. Thus the point (x,y) that lies on $[m,b]$ is uniquely determined, and hence y is. In fact it can easily be verified that

$$(o,y) = \left[((o,x)U \cap OE)V \cap (((o,m)U \cap EV)O \cap UV)(o,b)\right] U \cap OV \quad \ldots.(1)$$



As y is uniquely determined, the ternary operation T is well-defined. It is onto because for any $y \varepsilon R$, any affine line $[m,b]$ has incident on it an affine point with second co-ordinate y (this follows from the axioms of incidence).

The function T will be called the "Pickert ternary function" and the algebra (R, T) will be called the "Pickert ternary ring", as this is Pickert's version of Hall's ternary ring (see Pickert (9)).

Two binary operations mapping RxR onto R are now defined in terms of the ternary function T. These are addition (symbolized +) and multiplication (symbolized $\cdot$), and they are defined as follows:

(1) For any $x, b \varepsilon R$,

$$x+b = T(1,x,b)$$

(2) For any $m, x \varepsilon R$,

$$m \cdot x = T(m,x,o).$$

<u>Lemma 2.2</u>

(1) Addition amongst elements of R is a loop.

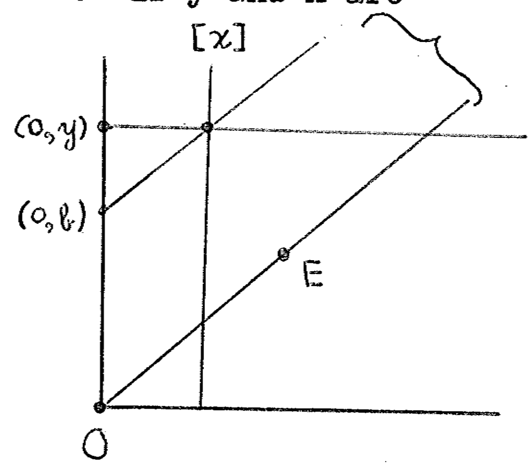
(2) Multiplication amongst elements of $R-\{o\}$ is a loop.

<u>Proof:</u> (1) By the definition of addition and the expression (in the proof of lemma 2.1) for (o,y) in terms of m,x, and b, one obtains that

$$y = x+b \Longleftrightarrow (o,y) = ([x] \cap [1,b])U \cap OV.$$

By lemma 2.1, f,x, and b are specified, (x+b) is uniquely determined. Further, if x and b are specified, $[x]$ is seen to be the line joining the points V and

$(o,y)U \cap (o,b)(1)$; by the incidence axioms, $[x]$, and therefore x, is uniquely defined. If y and x are specified, (o,b) is seen to be the point of intersection of $(x,y)(1)$ and OV; thus (o,b), and hence b, are uniquely determined. Hence addition is a loop.



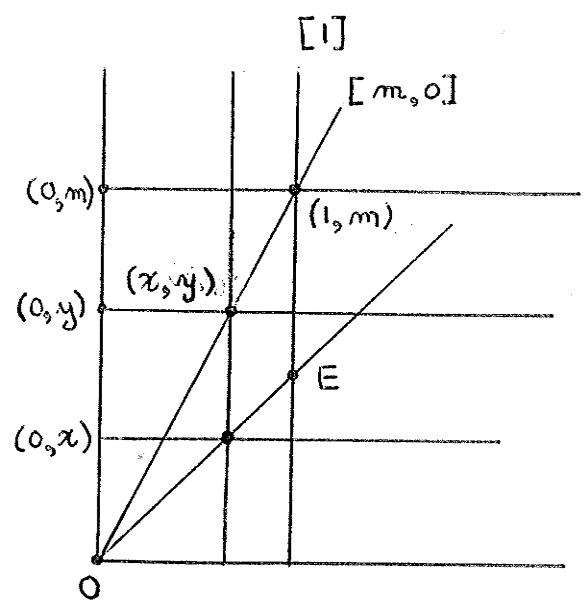
(2) By the definition of multiplication, it is easily seen that

$$y = mx \Leftrightarrow (o,y) = \left[((o,x)U \cap OE)V \cap ((o,m)U \cap EV)O\right]U \cap OV.$$

By lemma 2.1, y is uniquely determined if m and x are specified. If y and x are specified in $R-\{o\}$, it is seen that

$$(o,m) = OV \cap (EV \cap O(x,y))U$$

and hence by the incidence axioms, (o,m) is uniquely determined (note that the line $O(x,y)$ is well-defined as $x \neq 0 \neq y$).



If y and m are specified, it is seen that

$$[x] = ((o,y)U \cap (1,m)O)V$$

and so by the incidence axioms, $[x]$ and thus x are uniquely determined.

Hence multiplication over $R-\{o\}$ is a loop.

<u>Lemma 2.3</u> For all $a, b \varepsilon R$

(i) $ab = o \Longleftrightarrow a = o$ or $b = o$

(ii) $o+a = a+o = a$

(iii) $1 \cdot a = a \cdot 1 = a.$

<u>Proof</u> (i) First suppose that $ab = o$ and that $a \neq o$. Now $ab = T(a,b,o)$, so

$$o = T(a,b,o).$$

Hence $(b,o) \varepsilon [a,o]$. Now $(b,o) \varepsilon OU$ while $[a,o]$ is the line joining (a) and O. As $a \neq o$, $[a,o] \neq OU$. Hence

$$(b,o) = [a,o] \cap OU = (o,o).$$

Hence $b = o$.

Conversely, consider the product $o \cdot a$. Let $y = o \cdot a$; then $y = T(o,a,o)$.

Consequently by equation (1) in the proof of lemma 2.1,

$$(o,y) = [((o,a)U \cap OE)V \cap (((o,o)U \cap EV)O \cap UV)(o,o)]U \cap OV$$
$$= [(a,a)V \cap OU]U \cap OV$$
$$= OU \cap OV$$

i.e. $(o,y) = (o,o)$.

Thus $y = o$ and $o \cdot a = o$.

Similarly, consider the product $a \cdot o$ and let $z = a \cdot o$; then $z = T(a,o,o)$.

Thus as above,

$$(o,z) = [((o,o)U \cap OE)V \cap (((o,a)U \cap EV)O \cap UV)(o,o)]U \cap OV$$
$$= [OV \cap (a)O]U \cap OV$$
$$= OU \cap OV$$

i.e. $(o,z) = (o,o)$.

Thus $z = o$ and $a \cdot o = o$.

(ii) Let $y = o+a$. Then $y = T(1,o,a)$.

Hence by equation (1) in the proof of lemma 2.1,

$$\begin{aligned}(o,y) &= \left[((o,o)U \cap OE)V \cap (((o,1)U \cap EV)O \cap UV)(o,a)\right] U \cap OV \\ &= \left[OV \cap (1)(o,a)\right] U \cap OV \\ &= (o,a)U \cap OV\end{aligned}$$

i.e. $(o,y) = (o,a)$.

Thus $y = a$ and $o+a = a$.

Similarly, set $z = a+o$; then $z = T(1,a,o)$.

Thus

$$\begin{aligned}(o,z) &= \left[((o,a)U \cap OE)V \cap (((o,1)U \cap EV)O \cap UV)(o,o)\right] U \cap OV \\ &= \left[(a,a)V \cap OE\right] U \cap OV \\ &= (a,a)U \cap OV\end{aligned}$$

i.e. $(o,z) = (o,a)$.

Thus $z = a$ and so $a+o = a$.

(iii) Let $y = 1 \cdot a$. Then $y = T(1,a,o)$, and by the last argument in (ii), it immediately follows that $y = a$, i.e. that $a = 1 \cdot a$.

Similarly, let $z = a \cdot 1$. Then $z = T(a,1,o)$.

Thus as above

$$\begin{aligned}(o,z) &= \left[((o,1)U \cap OE)V \cap (((o,a)U \cap EV)O \cap UV)(o,o)\right] U \cap OV \\ &= \left[EV \cap ((1,a)O \cap UV)(o,o)\right] U \cap OV \\ &= (a,a)U \cap OV\end{aligned}$$

i.e. $(o,z) = (o,a)$.

Thus $z = a$ and $a \cdot 1 = a$.

THE HALL TERNARY RING

Marshall Hall (Hall (5), chapter 20) co-ordinatizes the projective plane in essentially the same way as Pickert does, but defines a ternary function H mapping $R \times R \times R \longrightarrow R$ in a somewhat different manner. If $(m,x,b) \varepsilon R \times R \times R$, then the element $H(m,x,b)$ of R is defined as follows:

$$y = H(m,x,b) \Longleftrightarrow (m,y) \varepsilon [x,b] .$$

Thus for any three elements $m,x,b \varepsilon R$, it follows that $T(m,x,b) = H(x,m,b)$.

Hall defines the binary operation of addition, mapping $R \times R \longrightarrow R$, as follows:

$$y = x+b \Longleftrightarrow (x,y) \varepsilon [1,b] ;$$

$$\text{i.e.} \quad \Longleftrightarrow \quad y = H(x,1,b).$$

Thus addition as defined by Hall is the same function as addition as defined by Pickert.

Hall defines multiplication, a binary function mapping $R \times R \longrightarrow R$ which we shall denote by $\underset{H}{\cdot}$, as follows:

$$y = x \underset{H}{\cdot} m \Longleftrightarrow (x,y) \varepsilon [m,o] .$$

$$\text{i.e. } y = H(x,m,o) = T(m,x,o) = m \underset{T}{\cdot} x,$$

where $\underset{T}{\cdot}$ denotes the Pickert operation of multiplication. Thus for arbitrary $m,x \varepsilon R$,

$$m \underset{T}{\cdot} x = x \underset{H}{\cdot} m ,$$

and as multiplication is in general non-commutative, the

Pickert and Hall multiplications are in general distinct functions.

ALGEBRAIC CONSEQUENCES OF (C, γ)-TRANSITIVITY IN π

If UVOE is a non-degenerate quadrangle as above, it follows from lemma 1.9 that π is an alternative plane if and only if it is a translation plane with respect to the non-concurrent lines UV, OV, and OU. By lemma 1.7 , this will occur if and only if the plane is (U,UV)-transitive, (V,UV)-transitive, (V,OV)-transitive, (O,OV)-transitive, (O,OU)-transitive and (U,OU)-transitive. The algebraic properties of the ternary ring that are associated with the various types of transitivity mentioned above are now developed.

First two splitting laws (linearity conditions) that ternary rings obey under certain circumstances are mentioned. They are as follows:

$\underline{L_1}$: If, for all $m,x,b \in R$, the identity

$$T(m,x,b) = m \cdot x + b$$

i.e. $$T(m,x,b) = T(1,T(m,x,o),b)$$

holds, then R is said to obey the "first splitting law", denoted by L_1.

$\underline{L_2}$: If, for all $m,x,b \in R$ the identity

$$T(m,x,mb) = m \cdot (x+b),$$

i.e. $$T(m,x,mb) = T(m,T(1,x,b),o)$$

holds, then R is said to obey the "second splitting law", denoted by L_2.

<u>Theorem 2.1</u> A projective plane π is (V,UV)-transitive if and only if L_1 holds and if addition is associative in the ternary ring of π.

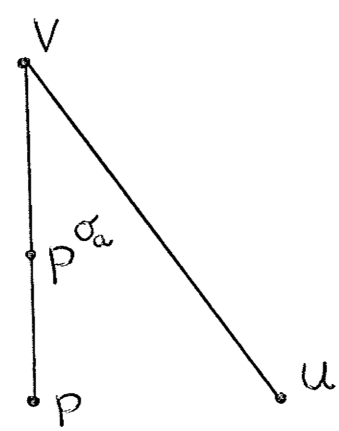
<u>Proof:</u> First assume that π is (V,UV)-transitive. Then for arbitrary $a \varepsilon R$ there exists a collineation σ_a with axis UV and centre V such that $(o,o)^{\sigma_a} = (o,a)$. As points on UV and lines through V are fixed by σ_a, it follows that for arbitrary $m \varepsilon R$,

$$[m]^{\sigma_a} = [m]$$

$$(m)^{\sigma_a} = (m)$$

$$(UV)^{\sigma_a} = UV$$

and $(\infty)^{\sigma_a} = (\infty)$.



If $P = (x,y)$ is an arbitrary affine point of π, then $P \varepsilon [x]$. Consequently as $\equiv P, P^{\sigma_a}, V$, it follows that $P^{\sigma_a} \varepsilon [x]$. In particular if $x = o$, then $(o,y)^{\sigma_a} \varepsilon [o]$. Hence the collineation σ_a induces a permutation on the affine points of $[o]$, and thus on the elements of R. This permutation will be symbolized by writing

$$(o,y)^{\sigma_a} = (o,y^{\sigma_a}) \quad ;$$

thus $y \longrightarrow y^{\sigma_a}$ is a permutation of R. Note in particular that from the definition of σ_a, $o^{\sigma_a} = a$. It follows that

$$(x,y)^{\sigma_a} = (x,y^{\sigma_a}) \quad ,$$

for $\equiv (o,y),(x,y),U \Rightarrow \equiv (o,y^{\sigma_a}),(x,y)^{\sigma_a},U$
and all affine points of a given line through U have the same y-co-ordinate.

The mapping τ of elements of R is now defined by

$$[m,b]^{\sigma_a} = [m,b^{\tau}] \quad \text{for all } m,b\varepsilon R.$$

(Note that as $(m)\varepsilon[m,b]$ and as $(m)^{\sigma_a} = (m)$, the image of $[m,b]$ under σ_a will also have slope m). However, $(x,y)\varepsilon[m,b]$ if and only if $(x,y)^{\sigma_a}\varepsilon[m,b]^{\sigma_a}$; i.e.

$$y = T(m,x,b) \Longleftrightarrow y^{\sigma_a} = T(m,x,b^{\tau}) ;$$

thus
$$(T(m,x,b))^{\sigma_a} = T(m,x,b^{\tau}) \qquad \text{..... (1)}$$

for all $m,x,b\varepsilon R$. In particular, since $T(m,o,b) = b$ for all $m,b\varepsilon R$, setting $x = o$ in equation (1) gives $b^{\sigma_a} = b^{\tau}$ for all $b\varepsilon R$; thus $\sigma_a = \tau$ and equation (1) becomes

$$(T(m,x,b))^{\sigma_a} = T(m,x,b^{\sigma_a}) \text{ for all } m,x,b,a\varepsilon R.$$

Setting $m = 1$, and using the fact that $T(1,x,b) = x+b$, one obtains that

$$(x+b)^{\sigma_a} = x+b^{\sigma_a} \qquad \text{..... (2)}$$

Setting $b = o$

$$(x+o)^{\sigma_a} = x+o^{\sigma_a}$$

i.e. $$x^{\sigma_a} = x+a \qquad \text{for all } x\varepsilon R.$$

Hence from equation (2) it follows that

$$(x+b)+a = x+(b+a).$$

But as a,x, and b are arbitrary in R, it follows that addition in R is associative.

Also, to each $x\varepsilon R$ there exists a unique additive inverse; for suppose that $x+q = o$. Then $T(1,x,q) = o$, i.e. $(x,o)\varepsilon(1,q)$. It follows that

$$(o,q) = OV \cap (OE \cap UV)((UX \cap OE)V \cap OU)$$

which by the axioms of incidence is a well-defined affine point of π. As $x+o = x$ for all $x\varepsilon R$ (lemma 2.3, (ii)) and as $(R,+)$ is a loop (lemma 2.2, (1)), it follows that $(R,+)$ is a group.

To derive the first splitting law, note that as $(T(m,x,b))^{\sigma_a} = T(m,x,b^{\sigma_a})$, it follows that

$$T(m,x,b)+a = T(m,x,b+a) \quad \text{for all } m,x,b,a\varepsilon R.$$

Setting $b = o$,

$$T(m,x,o)+a = T(m,x,a)$$

i.e. $$mx+a = T(m,x,a)$$

and thus L_1 holds.

Conversely, suppose that $(R,+)$ is a group and that L_1 holds, and consider the mapping σ_a of points and lines of π defined, for any given $a\varepsilon R$, as follows:

$$\begin{array}{ll} (x,y)^{\sigma_a} = (x,y+a) & [m,b]^{\sigma_a} = [m,b+a] \\ (m)^{\sigma_a} = (m) & [c]^{\sigma_a} = [c] \\ (\infty)^{\sigma_a} = (\infty) & [\infty]^{\sigma_a} = [\infty] \end{array}$$

Obviously σ_a fixes all points on $[\infty]$ and all lines through V; thus to show that it is a (V,UV)-collineation it suffices to show that σ_a preserves incidence. The verification that this occurs is trivial except for the case in which it is shown that

$(x,y)\varepsilon[m,b] \Longleftrightarrow (x,y)^{\sigma_a}\varepsilon[m,b]^{\sigma_a}$.

But by L_1

$$\begin{aligned}(x,y)\varepsilon[m,b] &\Longleftrightarrow y = mx+b\\ &\Longleftrightarrow y+a = (mx+b)+a\\ &\qquad\qquad = (mx+(b+a));\end{aligned}$$

hence $\quad (x,y)\varepsilon[m,b] \Longleftrightarrow y+a = T(m,x,b+a)$

i.e. $\quad (x,y)\varepsilon[m,b] \Longleftrightarrow (x,y)^{\sigma_a}\varepsilon[m,b]^{\sigma_a}$.

Hence σ_a preserves incidence and is thus a (V,UV)-collineation. As "a" was arbitrary in R, it follows that π is (V,UV)-transitive.

<u>Theorem 2.2</u> A projective plane π is (U,UV)-transitive if and only if (R,+) is a group and L_2 holds.

<u>Proof</u>: First assume that π is (U,UV)-transitive. Then for arbitrary $b\varepsilon R$, there is a (U,UV)-elation σ_b such that $(o,o)^{\sigma_b} = (b,o)$. Because σ_b fixes the line $[o,o]$, it induces a permutation on the affine points of $[o,o]$, and thus on the elements of R, which will be denoted by $(x,o)^{\sigma_b} = (x^{\sigma_b},o)$; thus $x \longrightarrow x^{\sigma_b}$, where x^{σ_b} is defined as above, is the permutation induced on R by σ_b. In particular $o^{\sigma_b} = b$.

From incidence considerations it immediately follows that

$$[o,a]^{\sigma_b} = [o,a] \qquad \text{for all } a\varepsilon R;$$
$$(\infty)^{\sigma_b} = (\infty)$$

$$(m)^{\sigma_b} = (m)$$

and $$[\infty]^{\sigma_b} = [\infty] .$$

Further, as for arbitrary $x \varepsilon R$ $(x,o) \varepsilon [x]$, it follows that $(x,o)^{\sigma_b} \varepsilon [x]^{\sigma_b}$; i.e.

$$(x^{\sigma_b}, o) \varepsilon [x]^{\sigma_b}.$$

But $(x^{\sigma_b}, o) \varepsilon [x^{\sigma_b}]$, and so

$$[x]^{\sigma_b} = [x^{\sigma_b}].$$

Hence for an arbitrary affine point (x,y), since $\equiv (x,y),(x,y)^{\sigma_b},U$ and since $(x,y)^{\sigma_b} \varepsilon [x]^{\sigma_b}$, it follows that $(x,y)^{\sigma_b} = (x^{\sigma_b},y)$.

Similarly, as $(m)^{\sigma_b} = (m)$, an affine line $[m,c]$ will be mapped as follows:

$$[m,c]^{\sigma_b} = [m,c^{\varphi_b}]$$

where this defines the permutation φ_b of elements of R.

As σ_b is a collineation,

$$(x,y) \varepsilon [m,c] \Longleftrightarrow (x,y)^{\sigma_b} \varepsilon [m,c]^{\sigma_b} ;$$

i.e. $y = T(m,x,c) \Longleftrightarrow y = T(m,x^{\sigma_b},c^{\varphi_b})$.

Thus for all $m,x,b,c \varepsilon R$

$$T(m,x,c) = T(m,x^{\sigma_b},c^{\varphi_b}) \qquad \ldots\ldots (1).$$

Setting $x = o$,

$$c = T(m,b,c^{\varphi_b}).$$

Hence equation (1) becomes

$$T(m,x, T(m,b,c^{\varphi_b})) = T(m,x^{\sigma_b},c^{\varphi_b}) \qquad \ldots\ldots (2).$$

Setting $m = 1$ and recalling the definition of addition,

$$x+(b+c^{\varphi_b}) = x^{\sigma_b}+c^{\varphi_b} \qquad \ldots\ldots (3)$$

Choosing c such that $c^{\varphi_b} = o$ (this is possible as φ_b is a permutation on R), equation (3) becomes

$$x+b = x^{\sigma_b} \quad \text{for all } x,b\varepsilon R.$$

Using this, equation (3) becomes, in general,

$$x+(b+c^{\varphi_b}) = (x+b)+c^{\varphi_b} \quad \text{for all } x,bc\varepsilon R.$$

Hence addition is associative and (by the reasoning used in theorem 2.1), (R,+) is a group.

Choosing c so that $c^{\varphi_b} = o$, equation (2) becomes

$$\begin{aligned} T(m,x,mb) &= T(m,x+b,o) \\ &= m(x+b) \end{aligned}$$

and hence L_2 holds.

Conversely, assume that L_2 holds and that (R,+) is a group. For arbitrary $c\varepsilon R$, define a mapping σ_c as follows:

$$\begin{array}{llll} (\infty)^{\sigma_c} = (\infty) & & [\infty]^{\sigma_c} = [\infty] \\ (m)^{\sigma_c} = (m) & & [x]^{\sigma_c} = [x+c] \\ (x,y)^{\sigma_c} = (x+c,y) & & [m,b] = [m,T(m,\alpha,b)] \end{array}$$

where α is defined by $c+\alpha = o$.

The verification that σ_c preserves incidence, and hence is a collineation, is trivial except for the verification that

$$(x,y)\varepsilon[m,b] \Longleftrightarrow (x,y)^{\sigma_c}\varepsilon[m,b]^{\sigma_c} \qquad \ldots\ldots (4).$$

But $\quad (x,y)\varepsilon[m,b] \Longleftrightarrow y = T(m,x,b)$

while $\quad (x,y)^{\sigma_c}\varepsilon[m,b]^{\sigma_c} \Longleftrightarrow y = T(m,x+c,T(m,\alpha,b))$.

If $\bar{b}$ is defined by $m\bar{b} = b$ (and $\bar{b}$ is well-defined as

$(R,\cdot)$ is a loop), it follows that

$$\begin{aligned} T(m,x+c,\ T(m,\alpha,b)) &= T(m,x+c,\ T(m,\alpha,m\bar{b})) \\ &= T(m,x+c,m\ T(1,\alpha,\bar{b})) \\ &= mT(1,x+c,\alpha+\bar{b}) \text{ (by successive applications of } L_2) \\ &= m((x+c)+(\alpha+\bar{b})) \\ &= m((x+(c+\alpha))+\bar{b}) \\ &= m(x+b) \text{ (associativity of addition)} \\ &= T(m,x,m\bar{b}) \end{aligned}$$

i.e. $T(m,x+c,T(m,\alpha,b)) = T(m,x,b)$.

Hence condition (4) holds and σ_c is a (U,UV)-collineation (as it fixes all lines through U and all points on UV). As c was arbitrary in R, it follows that π is (U,UV)-transitive.

<u>Theorem 2.3</u> A projective plane π is a translation plane with respect to the line UV if and only if:

(i) $(R,+)$ is an abelian group,

(ii) L_1 and L_2 are valid.

<u>Proof</u>: By lemma 1.7, π is a translation plane with respect to UV if and only if π is (V,UV)- and (U,UV)-transitive.

If π is (V,UV)- and (U,UV)-transitive, by the last two theorems, L_1 and L_2 both hold and $(R,+)$ is a group. Also, on the assumption that π is a translation plane with respect to UV, by theorem 1.1, the group of all elations with axis UV is abelian. For arbitrary $a,b \in R$, there exist (V,UV) elations σ_a and σ_b such that $(o,o)^{\sigma_a} = (o,a)$ and $(o,o)^{\sigma_b} = (o,b)$. Then, as in the proof of theorem 2.1,

$$(o,o)^{\sigma_a \sigma_b} = (o,a)^{\sigma_b} = (o,a+b).$$

Similarly $(o,o)^{\sigma_b \sigma_a} = (o,b+a)$.

But $\sigma_a \sigma_b = \sigma_b \sigma_a$; hence for all $a,b \in R$

$$a+b = b+a$$

and $(R,+)$ is abelian.

Conversely, if L_1 and L_2 are valid and $(R,+)$ is a group, by the two previous theorems π is (U,UV)-transitive and (V,UV)-transitive; hence it is a translation plane with respect to UV.

<u>Corollary</u>: If π is a translation plane with respect to UV, then the left distributive law is valid in C; i.e. for all $a,b,c \in R$, $a(b+c) = ab+ac$.

<u>Proof</u>: If π is a translation plane with respect to UV, then both L_1 and L_2 hold. Hence

$$T(a,b,ac) = ab+ac \qquad \text{by } L_1 ;$$

but

$$T(a,b,ac) = aT(1,b,c)$$
$$= a(b+c) \qquad \text{by } L_2 ;$$

hence

$$ab+ac = a(b+c) \text{ as claimed.}$$

Note that under the Hall definition of multiplication, a right distributive law is obtained when π is a translation plane with respect to UV; i.e. for all $a,b,c\varepsilon R$, $ba+ca = (b+c)a$.

<u>Theorem 2.4</u> If a projective plane π is (U,UV)- and (V,OV)-transitive, then the right distributive law holds; i.e. for all $a,b,c\varepsilon R$, $ba+ca = (b+c)a$.

<u>Proof:</u> As π is (V,OV)-transitive, for arbitrary $m\varepsilon R$ there exists a (V,OV)-elation σ_m such that $(o)^{\sigma_m} = (m)$. Then as $[\infty]$ is fixed by σ_m, σ_m permutes the points of $[\infty] - \{(\infty)\}$ amongst themselves, and hence induces a permutation $a \longrightarrow a^{\sigma_m}$ of the elements of R defined by $(a)^{\sigma_m} = (a^{\sigma_m})$. Hence in particular $o^{\sigma_m} = m$. Incidence considerations immediately give that

$$[\infty]^{\sigma_m} = [\infty] \qquad (o,b)^{\sigma_m} = (o,b)$$
$$[x]^{\sigma_m} = [x] \qquad (\infty)^{\sigma_m} = (\infty).$$

As $(a)^{\sigma_m}\varepsilon[a,b]^{\sigma_m}$ and $(o,b)^{\sigma_m}\varepsilon[a,b]^{\sigma_m}$, it follows that $[a,b]^{\sigma_m} = [a^{\sigma_m},b]$ and in particular $[o,b]^{\sigma_m} = [m,b]$.

For an arbitrary affine point (x,y), since $(x,y)\varepsilon[x]$, it follows that

$$(x,y)^{\sigma_m}\varepsilon[x]^{\sigma_m} = [x].$$

As π is (U,UV)-transitive, by theorem 2.1 L_1 holds and from this it follows that $(x,y)\varepsilon[o,y]$; hence

$$(x,y)^{\sigma_m}\varepsilon[o,y]^{\sigma_m} = [m,y].$$

Thus $(x,y)^{\sigma_m} = [x]\cap[m,y]$, and from L_1 it immediately follows that

$$(x,y)^{\sigma_m} = (x,mx+y). \qquad \ldots\ldots (1)$$

As $(x,y)\varepsilon[c,b] \Longleftrightarrow (x,y)^{\sigma_m}\varepsilon[c,b]^{\sigma_m}$, it follows from L_1 that

$$y = cx+b \Longleftrightarrow mx+y = c^{\sigma_m}x+b,$$

i.e. that $\qquad mx+(cx+b) = c^{\sigma_m}x+b$

for all m,c,x, and $b\varepsilon R$. As $(R,+)$ is a group (since π is (U,UV)-transitive), this can be rewritten as

$$(mx+cx)+b = c^{\sigma_m}x+b,$$

i.e.

$$mx+cx = c^{\sigma_m}x \qquad \ldots\ldots (2)$$

for all $m,x,c\varepsilon R$. Setting $x = 1$ in equation (1) gives $(1,y)^{\sigma_m} = (1,m+y)$ for all $m,y\varepsilon R$.

But by L_1, $(1,c)\varepsilon[c,o]$; hence

$$(1,c)^{\sigma_m}\varepsilon[c,o]^{\sigma_m},$$

i.e.

$$(1,m+c)\varepsilon[c^{\sigma_m},o].$$

Hence by L_1, $m+c = c^{\sigma_m}$. Substitution in equation (1) gives

$$mx+cx = (m+c)x \qquad \text{for all } m,c,x\varepsilon R,$$

and hence the right distributive law holds.

<u>Theorem 2.5</u> If π is a translation plane with respect to the lines UV and OV, then for arbitrary $c\varepsilon R-\{o\}$ there exists $c^{-1}\varepsilon R$ such that for arbitrary $b\varepsilon R$, $(bc)c^{-1} = b$.

<u>Proof</u>: As π is (O,OV)-transitive, for each $c\varepsilon R-\{o,-1\}$

there exists an (O,OV)-elation σ_c such that $(o)^{\sigma_c} = (-1-c,o)$. Since, for arbitrary $b \varepsilon R$, σ_c permutes the lines through $(o,b+bc)$ amongst themselves, it follows that

$$[o,b+bc]^{\sigma_c} = [\bar{b},b+bc]$$

for some element $\bar{b}$ which will be in general a function of b. Since $(o)\varepsilon[o,b+bc]$ it follows that

$$(o)^{\sigma_c}\varepsilon[o,b+bc]^{\sigma_c},$$

i.e. $$(-1-c,o)\varepsilon[\bar{b},b+bc].$$

As π is a translation plane with respect to UV, by theorem 2.3 L_1 is valid and hence

$$o = \bar{b}(-1-c)+(b+bc).$$

Using the easily verified fact that $(-a)b = -(ab) = a(-b)$, and the fact that by the hypotheses and theorems 2.3 and 2.4 both distributive laws are valid, it follows that

$$o = (-\bar{b}+b)(1+c).$$

As $c \neq -1$, it follows from lemma 2.3 that $-\bar{b}+b = o$, i.e. that $\bar{b} = b$. Consequently

$$[o,b+bc]^{\sigma_c} = [b,b+bc] \qquad \text{for arbitrary } b\varepsilon R.$$

Also, as $(o,o)\varepsilon[b+bc,o]$ for arbitrary $b\varepsilon R$, it follows that $[b+bc,o]^{\sigma_c} = [b+bc,o]$ for all $b\varepsilon R$. But by L_1, for all $b\varepsilon R$, $(1,b+bc)\varepsilon[b+bc,o]$ and $(1,b+bc)\varepsilon[o,b+bc]$. Hence

$$(1,b+bc)^{\sigma_c} = [b+bc,o]^{\sigma_c} \cap [o,b+bc]^{\sigma_c}$$

$$= [b+bc,o] \cap [b,b+bc].$$

If $c \neq o$ this is an affine point. On this assumption, if $(1,b+bc)^{\sigma_c} = (h,k)$, by L_1 one obtains

$$k = (b+bc)h$$

and $$k = bh+(b+bc).$$

Using the distributive laws, these equations give

$$bh+(bc)h = bh+b+bc$$

i.e. $$(bc)h = b+bc \qquad \ldots\ldots (1) \text{ for all } b\varepsilon R.$$

However, for any $b\varepsilon R$, $(1,b+bc)\varepsilon[1]$, so $(1,b+bc)^{\sigma_c}\varepsilon[1]^{\sigma_c}$, and thus $[1]^{\sigma_c} = h$. Hence h is a function of c alone; by setting $b = 1$ in equation (1) one obtains

$$ch = 1+c$$

which specifies h uniquely as a function of c. Set $h = u+1$ (this uniquely determines u). Substitution in equation (1) gives

$$(bc)(u+1) = b+bc$$

i.e. $$(bc)u = b \quad \text{(using the left distributive law)}$$

for all $b\varepsilon R$. As u is a function of c alone, it follows that u is the c^{-1} of the hypotheses, if $c \neq -1$. If $c = -1$, it is evident that $(b(-1))(-1)=b$ for all $b\varepsilon R$. Hence for all $c\varepsilon R - \{o\}$, there exists $c^{-1}\varepsilon R - \{o\}$ such that $(bc)c^{-1} = b$ for arbitrary $b\varepsilon R$.

<u>Corollary I</u> For all $c \varepsilon R$, $cc^{-1} = 1$.

<u>Proof:</u> Set $b = 1$ in $(bc)c^{-1} = b$.

<u>Corollary II</u> For all $c \varepsilon R$, $c^{-1}c = 1$.

<u>Proof:</u> Setting $b = c^{-1}$ in the above, one obtains $(c^{-1}c)c^{-1} = c^{-1}$. But $1 \cdot c^{-1} = c^{-1}$ so by the loop property of $(R - \{o\} , \cdot)$, $c^{-1}c = 1$.

<u>Theorem 2.6</u> If π is a translation plane with respect to UV and OV, then the following algebraic laws hold:

(i) $(R ,+)$ is an abelian group.

(ii) L_1 and L_2 are valid.

(iii) $(R- \{o\} , \cdot)$ is a loop with a right inverse that obeys the inverse condition $(bc)c^{-1} = b$ for all $c \varepsilon R- \{o\}$ where $c^{-1} \varepsilon R- \{o\}$ is so chosen that $cc^{-1} = 1$.

(iv) Both distributive laws hold.

<u>Proof:</u> This follows immediately from theorems 2.3, 214, and 2.5.

<u>Theorem 2.7</u> If a projective plane π obeys the algebraic laws enunciated in theorem 2.6, it is a translation plane with respect to all lines through V.

<u>Proof:</u> By theorem 2.3, π will be a translation plane with respect to UV. Hence to show that π is a translation plane with respect to OV, it suffices by lemma 1.8 to show that there is a collineation of π mapping UV into

another line through V.

Consider the mapping φ of π defined by

$(\infty)^{\varphi} = (\infty)$

$(m)^{\varphi} = (1,m)$

$(c,d)^{\varphi} = ((1+c^{-1})^{-1},\ d(1+c)^{-1})$ for $c \neq o,-1$

$(o,d)^{\varphi} = (o,d)$

$(-1,d)^{\varphi} = (-d)$

$(UV)^{\varphi} = [1]$ $\qquad$ $[1]^{\varphi} = UV$

$[c]^{\varphi} = [(1+c^{-1})^{-1}],\ c \neq o,\ -1$ $\qquad$ $[m,b]^{\varphi} = [m-b,b]$

$[o]^{\varphi} = [o]$

Evidently φ fixes V. To show that φ is a collineation of π, it must be verified that φ preserves incidence. This is trivial for all cases except for showing that

$$(c,d)\varepsilon[m,b] \Longleftrightarrow (c,d)^{\varphi}\varepsilon[m,b]^{\varphi} \quad (c \neq o,-1).$$

By L_1, $(c,d)\varepsilon[m,b]$ if and only if $d = mc+b$.
Similarly $(c,d)^{\varphi}\varepsilon[m,b]^{\varphi}$ if and only if

$$((1+c^{-1})^{-1}, d(1+c)^{-1})\varepsilon[m-b,b] ,$$

i.e. if and only if

$$d(1+c)^{-1} = (m-b)(1+c^{-1})^{-1}+b.$$

Hence $(c,d)\varepsilon[m,b] \Longleftrightarrow (c,d)^{\varphi}\varepsilon[m,b]^{\varphi}(c \neq o,-1)$
if and only if

$$(mc+b)(1+c)^{-1} = (m-b)(1+c^{-1})^{-1}+b \qquad \ldots\ldots (1)$$

is an identity for all $m,b,c\varepsilon R$ $(c \neq o,-1)$.
However, for all $m,b,c\varepsilon R$ $(c \neq o,-1)$

$$m = m$$

and thus $m = \left[m(1+c^{-1})^{-1}\right](1+c^{-1})$

$$= m(1+c^{-1})^{-1}+\left[m(1+c^{-1})^{-1}\right]c^{-1}.$$

Thus $mc = \left[m(1+c^{-1})^{-1}\right]c+m(1+c^{-1})^{-1}$

$$= \left[m(1+c^{-1})^{-1}\right](c+1)$$

$$= \left[m(1+c^{-1})^{-1}\right](1+c).$$

Hence $mc(1+c)^{-1} = (\left[m(1+c^{-1})^{-1}\right](1+c))(1+c)^{-1}$

i.e. $mc(1+c)^{-1} = m(1+c^{-1})^{-1}$ ..... (2)

and equation (2) is an identity for all $m,c\varepsilon R$ ($c \neq o,-1$).

Similarly $o = -b+b$

$$= (-b)\left[(1+c^{-1})^{-1}(1+c^{-1})\right]+b$$

$$= \left[(-b)(1+c^{-1})^{-1}\right](1+c^{-1})+b$$

$$= (-b)(1+c^{-1})^{-1}+\left[(-b)(1+c^{-1})^{-1}\right]c^{-1}+b.$$

Multiplying on the right by c,

$$o = \left[(-b)(1+c^{-1})^{-1}\right]c+(-b)(1+c^{-1})^{-1}+bc.$$

Thus $b = \left[(-b)(1+c^{-1})^{-1}\right]c+(-b)(1+c^{-1})^{-1}+bc+b$

$$= \left[(-b)(1+c^{-1})^{-1}\right](c+1)+b(c+1).$$

Hence $b(1+c)^{-1} = (-b)(1+c^{-1})^{-1}+b$ ..... (3)

is an identity for all $b,c\varepsilon R$ ($c \neq o,-1$).

But upon expanding (1) one obtains

$$(mc)(1+c^{-1})+b(1+c)^{-1} = m(1+c^{-1})^{-1}+(-b)(1+c^{-1})^{-1}+b$$

and from (2) and (3) it is seen that this is an identity for all $b,c,m\varepsilon R$ ($c \neq o,-1$).

Hence φ is indeed a collineation and π is a translation plane with respect to all lines through V.

—

Note that if Hall multiplication is used in the co-ordinatization of π, then π is a translation plane with respect to all lines through V if and only if the algebraic laws cited in theorem 2.6 hold, with the exception that the existence of a right inverse is replaced by the existence of a left inverse; i.e. for any $c \neq o$, $c \varepsilon R$, there exists c_L^{-1} such that $c_L^{-1}(cb) = b$ for any $b \varepsilon R$.

Theorem 2.8 A projective plane π is an alternative plane if and only if it is co-ordinatized by an alternative field in which L_1 is valid.

Proof: The plane π will be an alternative plane if and only if π is a translation plane with respect to UV, OV, and OU, by lemma 1.9 . Hence, using the results of theorems 2.6 and 2.7, it suffices to show:

(i) If π is a translation plane with respect to all lines through V, and if there exists (O,OU)-transitivity, then to each $c \varepsilon R - \{o\}$ there exists a unique $c_L^{-1} \varepsilon R - \{o\}$ such that $c_L^{-1}(cb) = b$ for all $b \varepsilon R$, and in fact c_L^{-1} is the c^{-1} of theorem 2.5. This will prove that an alternative plane is co-ordinatized by an alternative field.

(ii) A plane co-ordinatized by an alternative field in which L_1 is valid possesses a collineation moving V. Then by the fact that V is a translation plane with respect to all lines through V, it follows by lemma 1.6 that π is a translation plane with respect to three non-concurrent lines, and hence by lemma 1.9, π is an alternative plane.

To prove (i), suppose π is alternative. Then π is (0,0U)-transitive and there exists an (0,0U)-elation σ such that $(\infty)^{\sigma} = (o,-1)$. Evidently $(a,o)^{\sigma} = (a,o)$ for all $a \varepsilon R$, and $[m,o]^{\sigma} = [m,o]$ for all $m \varepsilon R$. Now $[a] = (\infty)(a,o)$, and so

$$[a]^{\sigma} = (\infty)^{\sigma}(a,o)^{\sigma} = (o,-1)(a,o).$$

If $a \neq o$, $[a]^{\sigma}$ is evidently of the form $[m,b]$ and by L_1 it is found that

$$[a]^{\sigma} = [a^{-1},-1] \qquad (a \neq o)$$

where a^{-1} is as defined in theorem 2.5.

Since for all $r \varepsilon R$ $(o,o) \varepsilon [r,o]$, it follows that $[r,o]^{\sigma} = [r,o]$ for all $r \varepsilon R$. Thus for $a \neq o \neq b$, consider how the point $(a,1-ba)$ maps under σ. By L_1 and the distributive laws it is found that $(a,1-ba) \varepsilon [a^{-1}-b,o]$. Also $(a,1-ba) \varepsilon [a]$; hence

$$\begin{aligned}(a,1-ba)^{\sigma} &= [a^{-1}-b,o]^{\sigma} \cap [a]^{\sigma} \\ &= [a^{-1}-b,o] \cap [a^{-1},-1]. \qquad \ldots\ldots (1)\end{aligned}$$

As $b \neq o$, $(a,1-ba)^{\sigma}$ is an affine point of π of the form (h,k). Applying L_1 and equation (1), one obtains

$$h = b^{-1}, \; k = a^{-1}b^{-1}-1.$$

Consequently $(a,1-ba)^{\sigma} = (b^{-1},a^{-1}b^{-1}-1) \qquad \ldots\ldots (2)$

for $a \neq o \neq b$.

Next consider how the point (1,1-ab) maps under σ for $a \neq o \neq b$. By L_1, $(1,1-ba) \varepsilon [1-ba,o]$.

Consequently

$$(1,1-ba) = [1] \cap [1-ba,o]$$

Hence
$$(1,1-ba)^{\sigma} = [1]^{\sigma} \cap [1-ba,o]^{\sigma}$$
$$= [1,-1] \cap [1-ba,o].$$

As $a \neq o \neq b$, $(1,1-ba)^{\sigma}$ is an affine point of the form (h,k). By L_1, the distributive laws, and the existence of the right alternative law, it is found that

$$h = (ba)^{-1}, \quad k = (ba)^{-1}-1.$$

Hence
$$(1,1-ba)^{\sigma} = ((ba)^{-1},(ba)^{-1}-1).$$

As σ is an (O,OU)-elation, lines through U are permuted amongst themselves by σ. Hence for $a \neq o \neq b$,

$$[o,1-ba]^{\sigma} = [o,k] \qquad (\text{assuming } [o,1-ba] \neq UV).$$

But $(1,1-ba) \varepsilon [o,1-ba]$; hence

$$((ba)^{-1},(ba)^{-1}-1) \varepsilon [o,1-ba]^{\sigma}$$

and evidently $[o,1-ba]^{\sigma}$ is an affine line. Hence by L_1,

$$(ba)^{-1}-1 = k.$$

Consequently $[o,1-ba]^{\sigma} = [o, (ba)^{-1}-1]$. ..... (3)

Now $(a,1-ba) \varepsilon [o,1-ba]$ and hence $(a,1-ba)^{\sigma} \varepsilon [o,1-ba]^{\sigma}$; consequently from equations (2) and (3)

$$(b^{-1},a^{-1}b^{-1}-1) \varepsilon [o,(ba)^{-1}-1] \qquad (a \neq o \neq b).$$

Thus
$$a^{-1}b^{-1}-1 = (ba)^{-1}-1,$$

i.e.
$$a^{-1}b^{-1} = (ba)^{-1} \quad , \quad a \neq o \neq b.$$

However, from theorem 2.5 and the hypotheses, $b^{-1} = (b^{-1}a^{-1})(a^{-1})^{-1}$, and as $(a^{-1})(a^{-1})^{-1} = 1$ and $a^{-1}a = 1$, by the loop properties of $(R-\{o\},\cdot)$, $a = (a^{-1})^{-1}$; hence $b^{-1} = (b^{-1}a^{-1})a$.

Thus
$$\begin{aligned} b = (b^{-1})^{-1} &= [(b^{-1}a^{-1})a]^{-1} \\ &= a^{-1}(b^{-1}a^{-1})^{-1} \\ &= a^{-1}((a^{-1})^{-1}(b^{-1})^{-1}) \\ &= a^{-1}\,(ab) \qquad \text{(by several applications of } (ba)^{-1} = a^{-1}b^{-1}) \end{aligned}$$

for $a \neq o \neq b$. If $b = o$ then $b = a^{-1}(ab)$ is trivially true. Hence for any $a \varepsilon R-\{o\}$, a^{-1} has the property that $b = a^{-1}(ab)$ for any $b \varepsilon R$. Hence R is an alternative field.

To prove (ii), consider the mapping φ of π defined as follows:

$$\begin{array}{ll} (a,b)\varphi = (b,a) & [c]^{\varphi} = [o,c] \\ (m)^{\varphi} = (m^{-1}), m \neq o & [m,b]^{\varphi} = [m^{-1},-m^{-1}b], \ m \neq o \\ (o)^{\varphi} = (\infty) & [o,b]^{\varphi} = [b] \\ (\infty)^{\varphi} = (o) & [\infty]^{\varphi} = [\infty]. \end{array}$$

Evidently this mapping moves V; to show that φ is a collineation it must be verified that φ is one-to-one onto and preserves incidence. This is trivial, the most complicated case being the following:

$(a,b)\varepsilon[m,c](m \neq o)$ holds if and only if $b = ma+c$; $(b,a)\varepsilon[m^{-1},-m^{-1}c]$ holds if and only if

$a = m^{-1}b - m^{-1}c$. But $b = ma+c$ if and only if $a = m^{-1}b - m^{-1}c$, since $a = m^{-1}(ma+c) - m^{-1}c$ is an identity as $m^{-1}(ma) = a$. Thus

$$(a,b)\varepsilon[m,c] \Longleftrightarrow (a,b)^{\varphi}\varepsilon[m,b]^{\varphi}.$$

Hence φ is a collineation and it follows that π is an alternative plane.

CHAPTER III

THE THEORY OF FINITE ALTERNATIVE FIELDS

In Chapter II it was shown that an alternative plane can be co-ordinatized by an alternative field. In this chapter it will be proved that any finite alternative field is a commutative field. It is well-known (Pickert (9), page 136) that the ternary ring of a projective plane is a field if and only if the plane is Pappian; it is also well-known (Ibid. page 144) that all Pappian planes are Desarguesian. Hence it follows that all finite alternative planes are Desarguesian.

DEFINITION OF AN ALTERNATIVE FIELD

Recall that an alternative field is a triple $(A,+,\cdot)$ (where A is a set with special elements 0 and I, and + and $\cdot$ are binary operations defined on A) obeying the following axioms:

1. Addition is an abelian group with neutral element 0.
2. The left and right distributive laws hold; i.e. for all $a,b,c \varepsilon A$,

$$a(b+c) = ab+ac$$

$$(b+c)a = ba+ca$$

3. If $x,y,z \varepsilon A-\{0\}$, and if the values of any two of x,y,z are known, then the equation $xy=z$ uniquely specifies the value of the

third. (I.e. multiplication, excluding 0, is a loop.)

4. To each $a \varepsilon A - \{0\}$ there corresponds a unique element $a^{-1} \varepsilon A - \{0\}$ such that $a^{-1}a = aa^{-1} = 1$, and for all $b \varepsilon A$,

$$(ba)a^{-1} = b$$

$$\text{and } a^{-1}(ab) = b$$

5. $1 \cdot a = a \cdot 1 = a$ for all $a \varepsilon A$.

Note that multiplication need not be either associative or commutative.

<u>Lemma 3.1</u> For all $a \varepsilon A$ and $b \varepsilon A$:

(i) $a \cdot 0 = 0 \cdot a = 0$

(ii) $(-1)(a) = (a)(-1) = -a$

(iii) $-(-a) = a$

(iv) $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$

where "$-a$" denotes the additive inverse of "a".

<u>Proof</u>: (i) By axiom 2 and the fact that 0 is the neutral element for addition

$$a(1) = a(1+0) = a(1)+a(0).$$

Hence as addition is a group,

$$a \cdot 0 = 0 .$$

Similarly $0 \cdot a = 0$

(ii) From axiom 2,

$$(1+-1) \cdot a = 1 \cdot a+(-1) \cdot a .$$

Thus $\qquad 0 \cdot a = a+(-1) \cdot a$

i.e. $\qquad 0 = a+(-1)a$

Thus by definition of $-a$,

$$(-1)a = -a$$

A similar argument yields $a(-1) = -a$

(iii) By definition of $-(-a)$,

$$-a+-(-a) = 0$$

But by definition of $-a$,

$$-a+a = 0$$

Hence $-(-a) = a$ as A is a group under addition.

(iv) Assume $ab = 0$ and that $a \neq 0$. Then by axiom 4 $a^{-1} \varepsilon A-\{0\}$ exists such that

$$b = a^{-1}(ab) = a^{-1} \cdot 0 = 0 \text{ (by (i))}$$

Thus $b = 0$.

<u>Theorem 3.1</u> For all $a, b \varepsilon A$,

(i) $(ba)a^{-1} = b \Rightarrow (ba)a = ba^2$

(ii) $a^{-1}(ab) = b \Rightarrow a(ab) = a^2 b$

<u>Proof</u>: (i) If $a = 0$, then

$$(ba)a = 0 = ba^2$$

and if $a = -1$, then

$$(ba)a = -(-b) = b \qquad \text{(lemma 3.1)}$$

while $ba^2 = b[(-1)(-1)] = b$ (lemma 3.1)

so $ba^2 = (ba)a$ for $a = 0, -1$

Now assume that $a \neq 0, -1$ and for arbitrary $c \varepsilon A$, consider

$$(ca)(a^{-1}-(a+1)^{-1})$$

(both a^{-1} and $(a+1)^{-1}$ are defined as $a \neq 0, -1$)

By axiom 2,

$$(ca)(a^{-1}-(a+1)^{-1}) = (ca)a^{-1}-(ca)(a+1)^{-1}$$
$$= c-(ca)(a+1)^{-1}.$$

Hence

$$\begin{aligned}\left[(ca)(a^{-1}-(a+1)^{-1})\right] (a+1) &= \left[c-(ca)(a+1)^{-1}\right](a+1)\\ &= c(a+1)-\left[(ca)(a+1)^{-1}\right](a+1)\\ &= c(a+1)-ca\\ &= ca+c-ca\\ &= c.\end{aligned}$$

Solving for ca, we obtain

$$ca = \left[c(a+1)^{-1}\right]\left[a^{-1}-(a+1)^{-1}\right]^{-1} \qquad \ldots\ldots (1)$$

This holds for arbitrary $c\varepsilon A$. Hence in particular it is true if $c = a+1$. Substituting this in equation (1) we obtain

$$(a+1)a = \left[a^{-1}-(a+1)^{-1}\right]^{-1};$$

substituting this in equation (1) gives

$$ca = \left[c(a+1)^{-1}\right]\left[(a+1)a\right] \qquad \ldots\ldots (2)$$

As c is arbitrary, set $c = b(a+1)$ and substitute into equation (2). This gives

$$\left[b(a+1)\right]a = \left[\{b(a+1)\}\ (a+1)^{-1}\right]\left[(a+1)a\right]$$

or $\qquad (ba+b)a = ba^2+ba$

i.e. $\qquad (ba)a+ba = ba^2+ba.$

As addition is a group, this implies

$$(ba)a = ba^2. \qquad \ldots\ldots (3)$$

As c was arbitrary in A, so is b, and thus equation (3) holds for all $b,a\varepsilon A$.

A completely analogous argument verifies (ii).

ASSOCIATORS AND COMMUTATORS

Let a,b,c be three arbitrary elements of A. The **associator** $[a,b,c]$ of the ordered triple (a,b,c) is defined to be the element $(ab)c-a(bc)$. The **commutator** $[a,b]$ of the ordered pair (a,b) is defined to be the element $ab-ba$. Thus the associator is a function mapping $A\times A\times A \to A$, and the commutator is a function mapping $A\times A \to A$.

Lemma 3.2 The associator function is linear in each argument.

Proof: For arbitrary $a,\bar{a},b,c \in A$, consider the associator $[a+\bar{a},b,c]$. By definition

$$\begin{aligned}[a+\bar{a},b,c] &= ((a+\bar{a})b)c-(a+\bar{a})(bc)\\ &= (ab+\bar{a}b)c-a(bc)-\bar{a}(bc)\\ &= (ab)c-a(bc)+(\bar{a}b)c-\bar{a}(bc)\\ &= [a,b,c]+[\bar{a},b,c].\end{aligned}$$

Thus the associator is linear in its first argument. Similar reasoning yields that it is linear in its second and third arguments as well.

Lemma 3.3 If two arguments of an associator are the same, the associator is zero.

Proof: Let a and b be arbitrary elements of A.

Then $[a,a,b] = (a^2)b-a(ab) = 0$ (theorem 3.1)

Similarly $[b,a,a] = 0$

Thus $\quad 0 = [a,b+a,b+a]$

$$= [a,b,b]+[a,b,a]+[a,a,b]+[a,a,a]$$

(by lemma 3.2);

Thus $\quad 0 = [a,b,a]$

and the lemma holds.

<u>Corollary</u>: For all $a,b\varepsilon A$, $a(ba) = (ab)a$; for $0 = [a,b,a] = (ab)a-a(ba)$.

<u>Lemma 3.4</u>: Interchanging two arguments of an associator changes its sign.

<u>Proof</u>: Let a,b,c be arbitrary in A. By lemmas 3.2 and 3.3,

$$\begin{aligned} 0 &= [a+b,a+b,c] \\ &= [a+b,b+a,c] \\ &= [a,b,c]+[a,a,c]+[b,b,c]+[b,a,c] \\ &= [a,b,c]+[b,a,c]. \end{aligned}$$

Hence

$$[a,b,c] = -[b,a,c].$$

Similarly, by expanding $[a,b+c,\ b+c]$ one obtains

$$[a,c,b] = -[a,b,c]$$

and by expanding $[a+c,b,a+c]$ one obtains

$$[c,b,a] = -[a,b,c]$$

<u>Lemma 3.5</u>: For all $a,b,c\varepsilon A$,

$$[a,b,c,] - [a,c,b] + [c,a,b] = [ab,c]-a[b,c]+[a,c]b$$

<u>Proof</u>: Expanding the right-hand side of the above, we obtain

$$\begin{aligned} &[ab,c]-a[b,c]+[a,c]b \\ &= (ab)c-c(ab)-a(bc)+a(cb)+(ac)b-(ca)b \end{aligned}$$

$$= [a,b,c]-[a,c,b]+[c,a,b] = \text{left-hand side.}$$

<u>Lemma 3.6</u> For all $a,b,c,d\varepsilon A$,

$$[ab,c,d]-[a,bc,d]+[a,b,cd] = a[b,c,d]+[a,b,c]d$$

<u>Proof:</u> Upon expanding,

$$[ab,c,d]-[a,bc,d]+[a,b,cd]$$

$$= ((ab)c)d-(ab)(cd)-(a(bc))d+a((bc)d)+(ab)(cd)-a(b(cd))$$

$$= a((bc)d-b(cd))+((ab)c-a(bc))d$$

$$= a[b,c,d]+[a,b,c]d.$$

<u>Theorem 3.2</u> Let A be an alternative field with commutative multiplication. Then if $1+1+1\neq 0$, multiplication in A is associative.

<u>Proof:</u> Let a,b,c be arbitrary in A. By lemma 3.5,

$$[ab,c] = a[b,c]+[a,c]b+[a,b,c]-[a,c,b]+[c,a,b]$$

Applying lemma 3.4, this becomes

$$[ab,c] = a[b,c]+[a,c]b+3[a,b,c]$$

(where $3 = 1+1+1$)

As A is commutative, all commutators are zero; hence

$$3[a,b,c] = 0$$

This implies, as $3\neq 0$, that

$$[a,b,c] = 0\ ;$$

that is, $(ab)c = a(bc)$

As a,b,c are arbitrary, A is associative.

<u>The "f" Function:</u> Define a function $f: A\times A\times A\times A\longrightarrow A$ as follows: for arbitrary $w,x,y,z\varepsilon A$,

$$f(w,x,y,z) = [wx,y,z]-[x,y,z]w-x[y,z,w]$$

Several properties of the "f" function follow.

Lemma 3.7 The function f is linear in each argument.

Proof: Let $w, \bar{w}, x, y$, and z be arbitrary in A, and consider

$$\begin{aligned}
&f(w+\bar{w},x,y,z)\\
=\ &[(w+\bar{w})x,y,z]-[x,y,z](w+\bar{w})-x[y,z,w+\bar{w}]\\
=\ &[wx+\bar{w}x,y,z]-[x,y,z]w+[x,y,z]\bar{w}-x[y,z,w]-x[y,z,\bar{w}]\\
&\quad\text{(by lemma 3.2)}\\
=\ &[wx,y,z]-[x,y,z]w-x[y,z,w]+[\bar{w}x,y,z]-[x,y,z]\bar{w}-x[y,z,\bar{w}]\\
=\ &f(w,x,y,z)+f(\bar{w},x,y,z).
\end{aligned}$$

Thus f is linear in its first argument. The verification that it is linear in the other three arguments is similar.

Theorem 3.3 The f function is alternative; that is, interchanging any two of the arguments of $f(w,x,y,z)$ changes the sign of $f(w,x,y,z)$.

Proof: Define a function $S: A\times A\times A\times A \longrightarrow A$ as follows: for arbitrary $w,x,y,z \varepsilon A$,

$$S(w,x,y,z) = f(w,x,y,z)-f(x,y,z,w)+f(y,z,w,x).$$

Upon expansion we obtain

$$\begin{aligned}
S(w,x,y,z) = &[wx,y,z]-[x,y,z]w-x[y,z,w]\\
&-[xy,z,w]+[y,z,w]x+y[z,w,x]\\
&+[yz,w,x]-[z,w,x]y-z[w,x,y] \qquad \ldots\ldots (1)
\end{aligned}$$

However, by application of lemma 3.4 and lemma 3.5, one obtains

$$\begin{aligned}
&[wx,y,z]-[xy,z,w]+[yz,w,x]\\
=\ &w[x,y,z]+[w,x,y]z
\end{aligned}$$

Hence equation (1) becomes

$$\begin{aligned} S(w,x,y,z) = {} & w[x,y,z]+[w,x,y]z \\ & -[x,y,z]w-x[y,z,w]+[y,z,w]x \\ & +\ y[z,w,x]-[z,w,x]y-z[w,x,y]. \end{aligned}$$

Recalling the definition of the commutator, this becomes

$$\begin{aligned} S(w,x,y,z) = {} & [y,[z,w,x]]-[x,[y,z,w]] \\ & -[z,[w,x,y]]+[w,[x,y,z]]. \end{aligned}$$

Cyclic permutation of the arguments of S gives

$$S(w,x,y,z) = -S(x,y,z,w).$$

Hence by definition of S,

$$\begin{aligned} & f(x,y,z,w)-f(y,z,w,x)+f(z,w,x,y) \\ = {} & -f(w,x,y,z)+f(x,y,z,w)-f(y,z,w,x). \end{aligned}$$

Thus $$f(z,w,x,y) = -f(w,x,y,z). \qquad \text{.....}\ (2)$$

Also,

$$\begin{aligned} f(w,x,y,z) &= [wx,y,z]-[x,y,z]w-x[y,z,w] \\ &= -[wx,z,y]+[x,z,y]w+x[z,y,w] \end{aligned}$$

(using lemma 3.4);

$$f(w,x,y,z) = -f(w,x,z,y). \qquad \text{.....}\ (3)$$

It is easily seen that equations (2) and (3) together imply that interchanging any two of the arguments of f changes the sign of f; for example,

$$\begin{aligned} f(w,x,y,z) &= -f(x,y,z,w) \\ &= f(y,z,w,x) \\ &= -f(y,z,x,w) \\ &= f(w,y,z,x)\ ; \end{aligned}$$

i.e. $f(w,x,y,z) = -f(w,y,x,z)$ by repeated use of equations (2) and (3).

<u>Corollary I</u> If two arguments of f are equal, then $f = 0$.

<u>Corollary II</u> (i) Since $f(x,x,y,z) = 0$, it follows that $[x^2,y,z] = [x,y,z]x + x[y,z,x]$.

(ii) Since $f(z,x,y,z) = 0$, it follows that $[zx,y,z] = [x,y,z]z + x[y,z,z]$

i.e. $[zx,y,z] = [x,y,z]z$.

(iii) Since $f(w,x,y,x) = 0$, it follows that $[wx,y,x] = x[y,x,w] = x[w,y,x]$ (by lemma 3.4).

<u>Theorem 3.4</u> For arbitrary $a,b,c \in A$:

(i) $(ab)(ca) = a((bc)a)$

(ii) $((ab)a)c = a(b(ac))$

(iii) $(a(bc))a = (ab)(ca)$

(iv) $c(a(ba)) = ((ca)b)a$

<u>Proof</u>: (i) $(ab)(ca) = a(b(ca)) + [a,b,ca]$

$= a(b(ca)) - [ca,b,a]$

$= a(b(ca)) - a[c,b,a]$ (from theorem 3.3, Corollary II, (iii)).

$= a(b(ca) + [b,c,a])$

$= a(b(ca) + (bc)a - b(ca))$

i.e. $(ab)(ca) = a((bc)a)$

(ii) $((ab)a)c = [ab,a,c] + (ab)(ac)$

$= [b,a,c]\,a + (ab)(ac)$ (from Corollary II, (iii) above)

$$= [b,a,ac]+(ab)(ac)$$
$$= (ab)(ac)-[a,b,ac]$$
$$= (ab)(ac)-(ab)(ac)+a(b(ac))$$

i.e. $\quad ((ab)a)c = a(b(ac))$

(iii) $\quad (a(bc))a = ((ab)c-[a,b,c])a$
$$= ((ab)c)a-[a,b,c]a$$
$$= ((ab)c)a-[ab,c,a] \quad \text{(corollary II (ii) above)}$$
$$= ((ab)c)a-((ab)c)a+(ab)(ca)$$

i.e. $\quad (a(bc))a = (ab)(ca)$

(iv) $\quad c(a(ba)) = (ca)(ba)-[c,a,ba]$
$$= (ca)(ba)-[ba,c,a]$$
$$= (ca)(ba)-a[b,c,a] \quad \text{(corollary II (iii)}$$
$$= (ca)(ba)+[ca,b,a]$$
$$= (ca)(ba)+((ca)b)a-(ca)(ba)$$

i.e. $\quad c(a(ba)) = ((ca)b)a$.

These four identities are sometimes called the Moufang identities , after Ruth Moufang (Hall (5), page 424) who first enunciated them.

<u>SOME ELEMENTARY PROPERTIES OF FIELDS</u>

Some basic properties of finite fields are now stated. Proofs of these results can be found in van der Waerden.[1]

(1) A finite field F can be regarded as a vector space (of finite dimension, say n) over the additive

---

[1] Van der Waerden, Modern Algebra, Vol. I, Ungar Publishing Company, 1953.

group generated by the element 1. As all finite fields have prime characteristic p, the order of a finite field F will be p^n.

(2) If F is a finite field of order p^n, then $F-\{0\}$, which will be denoted by F^*, is a multiplicative group of order p^n-1.

(3) If K is a subfield of a finite field F, and if F has order p^n, then K has order p^m where m divides n.

(4) The intersection of two subfields of a field F is itself a subfield of F.

<u>DEFINITION OF THE CENTRALIZER</u>

For an arbitrary element $x\varepsilon F$, define the centralizer $C_F(x)$ of x in F as follows:

$$C_F(x) = \{f\varepsilon F \mid xf = fx\} .$$

<u>Lemma 3.8</u> Let F be a finite field. For arbitrary $x\varepsilon F$, $C_F(x)$ is a subfield of F.

<u>Proof</u>: Trivially $0\varepsilon C_F(x)$ and $1\varepsilon C_F(x)$, for any $x\varepsilon F$.

To show that $C_F(x)$ is a subfield of F it suffices to verify closure of addition and multiplication; the associativity of addition and multiplication and the commutativity of addition in $C_F(x)$ then follow from the corresponding facts about F.

Let y and z be arbitrary elements of $C_F(x)$.

Then $\quad xy = yx \;,\quad yz = zx.$

Thus $\quad (y+z)x = yx+zx$

$\quad = xy+xz$

i.e. $\quad (y+z)x = x(y+z)$

and thus $\qquad y+z\varepsilon C_F(x)$.

Hence $C_F(x)$ is closed under addition.

Similarly,

$$(yz)x = y(zx) = y(xz)$$
$$= (yx)z = (xy)z$$

i.e. $\qquad (yz)x = x(yz)$

and thus $\qquad yz\varepsilon C_F(x)$.

Hence $C_F(x)$ is closed under multiplication.

For a given $z\varepsilon C_F^*(x)$, the mapping

$$\varphi_z : y \longrightarrow yz \qquad (z,y\varepsilon C_F(x))$$

is a one-to-one mapping of $C_F(x)$ onto $C_F(x)$.

Since $1\varepsilon C_F(x)$, there exists $\bar{z}\varepsilon C_F(x)$ such that $Z\bar{Z} = 1$;

hence $z^{-1}\varepsilon C_F^*(x)$ if $z\varepsilon C_F^*(x)$.

Similarly $(-z)\varepsilon C_F(x)$ if $z\varepsilon C_F(x)$.

This completes the verification that $C_F(x)$ is a field.

Theorem 3.5

Wedderburn's Theorem. Every finite field is a commutative field.

Proof: Let F be a finite field of order p^n, and let x be arbitrary in F. Let

$$|C_F(x)| = p^{i_x}$$

and let $\qquad |Z(F)| = p^m$.

Then for all $x\varepsilon F$, i_x divides n and m divides i_x.

For arbitrary $x\varepsilon F^*$, define C_x, the conjugate class of the multiplicative group F^*, as

$$C_x = \{g^{-1}xg \mid g\varepsilon F^*\}.$$

Then F^* can be partitioned into disjoint conjugate classes, as it is easily verified that being in a given conjugate class is an equivalence relation. Hence the order of F^* can be written as the sum of the orders of the conjugate classes of F^*; this equality is called the class equation of F^*.

Now

$$|C_z| = 1 \iff z \varepsilon Z^*(F).$$

Hence there are (p^m-1) singleton conjugate classes of F^*.

Also, $$|C_x| = [F^*: C_F^*(x)];$$

for let $C_F(x)g_1$ and $C_F(x)g_2$ be two distinct cosets of $C_F^*(x)$ in F^*, and let

$$\lambda_1 \varepsilon C_F^*(x)g_1, \ \lambda_2 \varepsilon C_F^*(x)g_2.$$

Then

$$\lambda_1^{-1}x\lambda_1 = (fg_1)^{-1}x(fg_1), \quad f\varepsilon C_F^*(x)$$
$$= g_1^{-1}f^{-1}xfg_1$$

i.e. $$\lambda_1^{-1}x\lambda_1 = g_1^{-1}xg_1 .$$

Thus conjugation of x by any element from a given coset $C_F^*(x)g_1$ yields the same conjugate $g_1^{-1}xg_1$.

However, $\lambda_1^{-1}x\lambda_1 \neq \lambda_2^{-1}x\lambda_2$; for if this were not the case, then

$$g_1^{-1}xg_1 = g_2^{-1}xg_1$$

i.e. $$(g_1g_2^{-1})^{-1}x(g_1g_2^{-1}) = x$$

and thus $$g_1g_2^{-1}\varepsilon C_F(x),$$

contradicting the hypothesis that $C_F^*(x)g_1$ and $C_F^*(x)g_2$ were distinct cosets.

Hence $$|C_x| = [F^*:C_F^*(x)] = \frac{p^n-1}{p^{1x}-1}$$

Thus the class equation for F is

$$p^n-1 = p^m-1+\sum \frac{p^n-1}{p^{i_x}-1} \qquad \ldots\ldots (1)$$

where the summation is over distinct conjugate classes of order > 1.

As m divides n and m divides i_x for all x, we can write

$$p^m = q$$

$$n = mr$$

$$i_x = mj_x, \qquad \text{for all } x\varepsilon F^*.$$

Then equation (1) becomes

$$q^r-1 = q-1+\sum \frac{q^r-1}{q^{j_x}-1} \qquad \ldots\ldots (2)$$

Define $\Phi_r(q)$ by

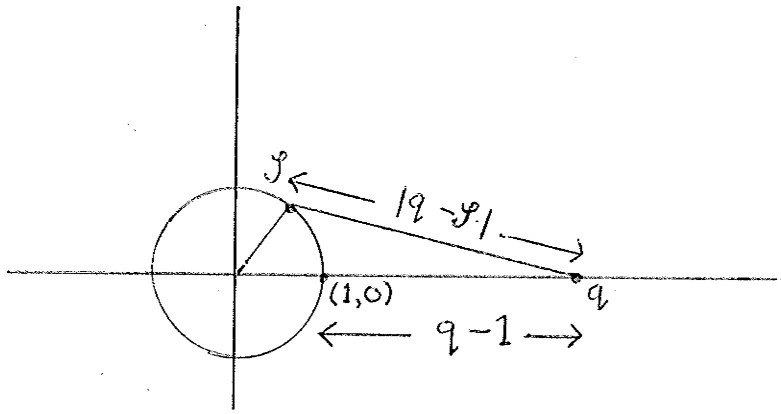
$$\Phi_r(q) = \prod_i (q-\mathcal{S}_i),$$

where the product is taken over all the rth primitive roots $\mathcal{S}_i$ of 1. Then $\Phi_r(q)$ divides q^r-1. Also, since $j_x < r$ for all $x\varepsilon F^*$(if we assume that $Z^*(F) \neq F^*$), $(q^{j_x}-1)$ contains no factors of the form $q-\mathcal{S}$, where $\mathcal{S}$ is an rth root of unity. Consequently $\Phi_r(q)$ divides $\sum \frac{q^r-1}{q^{j_x}-1}$.
Hence from equation (2), it follows that

$$\Phi_r(q) \text{ divides } (q-1) \qquad \ldots\ldots (3)$$

Set up an Argand diagram of the complex plane, and consider the distribution of the rth primitive roots of unity about the unit circle. As q is a positive integer, it is seen that

$$|q-\mathcal{S}| > q-1 \quad \text{for each root } \mathcal{S}.$$



However, result (3) implies that

$$\pi(q-\mathcal{J}) \text{ divides } (q-1),$$

from which it follows that $r = 1$. Thus $n = m$, i.e. $Z(F) = F$, and as $Z(F)$ is commutative by definition, F is commutative.

__Theorem 3.6__ Every finite alternative field K is a commutative field.

__Proof:__ The proof can be broken into four main assertions:

(1) If a and b are arbitrary in K, then $D = \{a,b,1\}$ generates a finite subfield F of K.

(2) By theorem 3.5, F is a commutative field, and so $ab = ba$.

(3) As a and b were arbitrary in K, K is commutative.

(4) A commutative alternative field is associative, and hence K is a commutative field.

Assertion (2) follows from (1), and (3) follows from (2), immediately. Hence it suffices to prove assertions (1) and (4).

To prove (1), some notation is first introduced. If A, B, and C are subsets of K, then $[A,B,C]$ is defined by

$$[A,B,C] = \{[a,b,c] \mid a\varepsilon A,\ b\varepsilon B,\ c\varepsilon C.\}$$

By the statement "$[A,B,C] = 0$" we shall mean that

$$[a,b,c] = 0\ , \text{ for all } a\varepsilon A,\ b\varepsilon B,\ c\varepsilon C.$$

Define a subset X of K by

$$X = \{x \mid [D,D,x] = 0,\ x\varepsilon K\}$$ (where D is $\{a,b,1\}$ as above).

Then $D \subseteq X$; for let $[d_1,d_2,d_3] \varepsilon [D,D,D]$. If $d_i = d_j$, $i \neq j$ $(i,j = 1,2,3)$ then by lemma 3.3, $[d_1,d_2,d_3] = 0$. If d_1,d_2,d_3 are distinct, then as $D = \{a,b,1\}$, one of d_1,d_2,d_3 is 1, and hence $[d_1,d_2,d_3] = 0$ as any associator with 1 as one of its elements is zero. Hence $[D,D,D] = 0$ and thus $D \subseteq X$.

Secondly, $DX \subseteq X$; for let $[d_1,d_2,d_3x]$ be arbitrary in $[D,D,DX]$. If $d_1 = d_2$, then $[d_1,d_2,d_3x] = 0$ by lemma 3.3. If d_1 or $d_2 = 1$, then $[d_1,d_2,d_3x] = 0$ as above. Hence without loss of generality assume that $d_1 = a$, $d_2 = b$.

If $d_3 = 1$, then $[d_1,d_2,d_3x] = 0$ by definition of X. If $d_3 = a$, then

$$\begin{aligned}[d_1,d_2,d_3x] &= [a,b,ax] \\ &= -[ax,b,a] \\ &= -[x,b,a]a \quad \text{(theorem 3.3, Corollary II, part (ii)),} \\ &= [a,b,x]a\end{aligned}$$

i.e. $\quad [d_1,d_2,d_3x] = 0$

as $$[a,b,x] \varepsilon [D,D,X] = 0$$

If $d_3 = b$ the proof is similar. Hence in general $[D,D,DX] = 0$ and so $DX \subseteq X$.

Define a subset Y of K by

$$Y = \{y \mid y \varepsilon X,\ yX \subseteq X,\ [D,X,y] = 0.\}$$

Then $D \subseteq Y$. To verify this, suppose that $[d_1,x,d_2]$ is arbitrary in $[D,X,D]$. Then

$$[d_1,x,d_2] = -[d_1,d_2,x] = 0$$

and thus $[D,X,D] = 0$. As $D \subseteq X$ and $DX \subseteq X$, it follows that $D \subseteq Y$.

Define a subset R of K by

$$R = \{r \mid r \varepsilon Y,\ [X,Y,r] = 0.\}$$

Then $D \subseteq R$, as can be verified by the methods employed above. It follows that

$$D \subseteq R \subseteq Y \subseteq X.$$

In order to verify (1), it suffices to show that R is a field. By definition of X,Y, and R, it follows that $0 \varepsilon R$ and $1 \varepsilon R$.

Addition is closed in R; for if $r_1 \varepsilon R$, $r_2 \varepsilon R$, then $r_1 + r_2 \varepsilon R$ by the linear property of associators and the definitions of X, Y, and R.

Multiplication is closed in R, i.e. $RR = R$; for if r_1 and r_2 are arbitrary in R, then as $R \subseteq Y$ and $R \subseteq X$, $r_1 \varepsilon Y$ and $r_2 \varepsilon X$; thus

$$r_1 r_2 \varepsilon yX \subseteq X\ ,$$

and so $r_1 r_2 \varepsilon X$; in general $RR \subseteq X$. Further, as $[X,Y,R] = 0$, we have

$$(r_1r_2)X = r_1(r_2X).$$

As $r_2 \varepsilon Y$, $r_2X \subseteq X$ and so

$$(r_1r_2)X \subseteq r_1X \subseteq X \qquad \text{(as } r_1 \varepsilon Y).$$

Also, $r_1r_2 \varepsilon X$, so in order to show that $r_1r_2 \varepsilon Y$, it remains to verify that $[D,X,r_1r_2] = 0$. However,

$$[D,X,r_1r_2] = 0 \quad \text{if and only if}$$

$$[X,D,r_1r_2] = 0 \quad \text{(by lemma 3.3)}$$

and this will certainly be true if

$$[X,Y,r_1r_2] = 0 \quad \text{as } D \subseteq Y.$$

For arbitrary $x \varepsilon X$, $y \varepsilon Y$, consider

$$f(y,x,r_1,r_2) = [yx,r_1,r_2] - [x,r_1,r_2]y - x[y,r_1,r_2].$$

As $[X,Y,R] = 0$ and as $R \subseteq Y \subseteq X$, the last two associators are zero; also $yx \varepsilon X$, so by similar reasoning, $[yx,r_1,r_2] = 0$. Hence

$$f(y,x,r_1,r_2) = 0.$$

By theorem 3.3, this implies that

$$\begin{aligned} 0 &= f(r_1,r_2,y,x) \\ &= [r_1r_2,y,x] - [r_2,y,x]r_1 - r_2[y,x,r_1] \end{aligned}$$

and by the alternative property of associators and the argument used above, one obtains

$$0 = [r_1r_2,y,x] = -[x,y,r_1r_2].$$

Hence $\qquad [X,Y,RR] = 0$ so $RR \subseteq Y$.

By the definition of R it immediately follows that $RR = R$, and so R is closed under multiplication.

Addition is associative and commutative in R, as it is in K. Also,

$$[R,R,R] \subseteq [X,Y,R] = 0$$

so multiplication in R is associative.

Finally, $r \varepsilon R^* \Longrightarrow r^{-1} \varepsilon R^*$

and $\qquad -r \varepsilon R \Longrightarrow -r \varepsilon R$

by the methods used to establish this in lemma 3.8. Hence R is a field, and as $D \subseteq R$, D generates a subfield of K.

This completes the proof of (1).

To prove (4), first note that by theorem 3.2, if $1+1+1 \neq 0$ in K, then K is associative. Hence all that need be considered now is the case in which $1+1+1 = 0$ (i.e. $3 = 0$).

Let u, v, and a be arbitrary in K. Consider the element $(uv)a^3$. As $\langle 1,uv,a \rangle$ is a field, and hence associative, it follows that

$$\begin{aligned}
(uv)a^3 &= (uv)((a^2)a) \\
&= ((uv)(a^2))a \\
&= (a^2(uv))a \\
&= a^2((uv)a) \\
&= a(a((uv)a)) \\
&= a((au)(va)) \qquad \text{(by theorem 3.4 (i))} \\
&= ((ua)(av))a \\
&= u(a((av)a)) \qquad \text{(by theorem 3.4 (iv))}
\end{aligned}$$

i.e. $\qquad (uv)a^3 = u(va^3) \qquad \ldots\ldots (1)$

(as $\langle 1,v,a \rangle$ is a field).

Choose a,b,c arbitrary in K^*. Define d by

$$(ab)c = (a(bc))d.$$

As any two elements of K, plus the identity, generate a field, for arbitrary $x,y \varepsilon K$:

$$x^3 y^3 = (xy)^3.$$

Hence

$$\begin{aligned}(a^3 b^3)c^3 &= (ab)^3 c^3 = ((ab)c)^3 \\ &= ((a(bc))d)^3 \\ &= (a(bc))^3 d^3 \\ &= (a^3 (bc)^3)d^3\end{aligned}$$

i.e. $\quad (a^3 b^3)c^3 = (a^3(b^3 c^3))d^3.$

By equation (1), expressions involving cubes as the third term are associative; hence

$$(a^3 b^3)c^3 = ((a^3 b^3)c^3)d^3$$

and thus $\quad d^3 = 1,$

i.e. $\quad d^3 - 1 = 0.$

As $1+1+1 = 0$, $\ d^3 - 1 = (d-1)^3$, so

$$(d-1)^3 = 0,$$

i.e. $\quad d-1 = 0 \qquad$ or $d = 1.$

Hence by the definition of d, for arbitrary $a,b,c \varepsilon K$,

$a(bc) = (ab)c$; $\quad$ i.e. K is associative.

Hence K is a commutative field, and therefore every finite alternative field is a commutative field.

CHAPTER IV

GROUP THEORETICAL AND COMBINATORIAL THEOREMS

The Elementary Theory of Permutation Groups

In this section a brief outline of the basic ideas of the theory of permutation groups will be given, with particular reference to how the theory relates to collineation groups of projective planes. In addition, several special results that will be needed later are proved. For a detailed treatment of this subject reference should be made to Wielandt (14).

Let S be a finite set. The number of elements in a subset T of S will be denoted by $|T|$ and will be called the order of T. A permutation of S is a one-to-one mapping of S onto itself. If g is a permutation of S and if $s \varepsilon S$, then the image of s under the permutation g will be written as s^g. If g and h are two permutations of S, their product gh is defined as the mapping sending $s \longrightarrow (s^g)^h$. Then gh is a permutation if g and h are, and multiplication of permutations is associative.

A permutation group G on a set S is a group each of whose elements is a permutation of S. The identity permutation 1 fixes every element of S while the inverse g^{-1} of a permutation g is defined by writing

$$s^{g^{-1}} = t \Longleftrightarrow t^g = s \quad \text{for all } s,t\varepsilon S.$$

Obviously g^{-1} is a permutation.

One subgroup of G deserves special mention. If $T \subseteq S$, then G_T is defined by

$$G_T = \{ g\varepsilon G \;\; t^g = t \quad \text{for all } t\varepsilon T \}.$$

Obviously G_T is a subgroup of G and thus also a permutation group of S. If in particular T is the singleton set $\{t\}$, then G_t is called the stabilizer of t.

The order of G will be denoted by $|G|$ and will always be assumed to be finite.

For arbitrary $s\varepsilon S$, the "orbit" of s, denoted Orb s, is defined as follows:

$$\text{Orb } s = \{ s^g \,|\, g\varepsilon G \}.$$

Orbits are sometimes called "transitive classes" of S under G. The set of orbits of S under G forms a partition of S into disjoint sets. In general Orb $(s) \subseteq S$; however, if for any $s\varepsilon S$ Orb $(s) = S$, then G is said to be "transitive" on S. Evidently G will be transitive on S if and only if for arbitrary $\alpha,\beta\varepsilon S$, there exists $g\varepsilon G$ such that $\alpha^g = \beta$.

More generally, an <u>action</u> of an abstract group G on a given set S is defined as a function mapping SxG onto S such that $s^1 = s$ for all $s\varepsilon S$ and such that $(s^{g_1})^{g_1} = s^{g_1 g_2}$ for all $s\varepsilon S$ and $g_1, g_2\varepsilon G$. A given group G may have an action defined on more than one set, and the structure of G considered as a permutation group on one set may differ from the structure of G considered as a permutation group on another. As an example, a collineation of a projective plane has an action on two distinct sets, the set of points of the plane and the set of lines of the plane. If a group G has an action on a set S, it can be regarded as a permutation group of S.

Of basic importance is the "fundamental" theorem of permutation groups:

<u>Lemma 4.1</u> Let a group G have an action on a set S and let α be an arbitrary point of S. Then $|G_\alpha|\,|\mathrm{Orb}\ (\alpha)| = |G|$.

<u>Proof</u>: For arbitrary $g_1, g_2 \varepsilon G$, it is seen that

$$\alpha^{g_1} = \alpha^{g_2} \Leftrightarrow \alpha^{g_1 g_2^{-1}} = \alpha$$

i.e. $$\Leftrightarrow g_1 g_2^{-1} \varepsilon G_\alpha$$

i.e. $\alpha^{g_1} = \alpha^{g_2} \Leftrightarrow g_1$ and g_2 are in the same right coset of G_α in G. Hence the number of images of α under G equals the number of right cosets of G_α in G, i.e.

$$|\mathrm{Orb}\ (\alpha)| = [G:G_\alpha] = \frac{|G|}{|G_\alpha|}.$$

Hence $$|\mathrm{Orb}\ (\alpha)|\,|G_\alpha| = |G|.$$

<u>Lemma 4.2</u> Let a group G have an action on a set S and let T_1 and T_2 be two orbits of S under G. If $|T_1|$ and $|T_2|$ are relatively prime and if $\delta_1 \varepsilon T_1$, then G_{δ_1} is transitive on T_2.

<u>Proof:</u> Let $\delta_1 \varepsilon T_1$ and $\delta_2 \varepsilon T_2$. Then Orb $(\delta_1) = T_1$ and Orb $(\delta_2) = T_2$. Hence by lemma 4.1,

$$|T_1|\,|G_{\delta_1}| = |G|$$

and $$|T_2|\,|G_{\delta_2}| = |G|.$$

Thus $$|T_1|\,|G_{\delta_1}| = |T_2|\,|G_{\delta_2}|. \qquad \ldots\ldots (1)$$

As $|T_1|$ and $|T_2|$ are relatively prime, this implies that integers k_1 and k_2 exist such that

$$|G_{\delta_1}| = k_2|T_2|$$

and $$|G_{\delta_2}| = k_1|T_1|.$$

Substitution into equation (1) gives

$$|T_1|k_2|T_2| = |T_2|k_1|T_1|$$

i.e. $$k_1 = k_2 = k \text{ (say)}.$$

But considering G_{δ_1} as a permutation group on T_2 and using lemma 4.1, if the orbit of δ_2 under G_{δ_1} is denoted by Orb $G_{\delta_1}(\delta_2)$, it follows that

$$|\text{Orb } G_{\delta_1}(\delta_2)|\,|(G_{\delta_1})_{\delta_2}| = |G_{\delta_1}|. \qquad \ldots\ldots (2)$$

Similarly $$|\text{Orb } G_{\delta_2}(\delta_1)|\,|(G_{\delta_2})_{\delta_1}| = |G_{\delta_2}|. \qquad \ldots\ldots (3)$$

Noting that $(G_{\delta_1})_{\delta_2} = (G_{\delta_2})_{\delta_1}$ and dividing equation (2) by equation (3), one obtains

$$\frac{|\text{Orb } G_{\delta_1}(\delta_2)|}{|\text{Orb } G_{\delta_2}(\delta_1)|} = \frac{|G_{\delta_1}|}{|G_{\delta_2}|} = \frac{k|T_2|}{k|T_1|} = \frac{|T_2|}{|T_1|}$$

i.e. $$|T_1|\,|\text{Orb } G_{\delta_1}(\delta_2)| = |T_2|\,|\text{Orb } G_{\delta_2}(\delta_1)|.$$

Thus as $|T_1|$ and $|T_2|$ are relatively prime, there exists an integer n such that

$$n|T_2| = |\mathrm{Orb}\ G_{\delta_1}(\delta_2)|$$

i.e. $$|T_2| \mid |\mathrm{Orb}\ G_{\delta_1}(\delta_2)|.$$

As $\mathrm{Orb}\ G_{\delta_1}(\delta_2) \subseteq T_2$, $n = 1$ and thus $\mathrm{Orb}\ G_{\delta_1}(\delta_2) = T_2$.

Hence by definition G_{δ_1} is transitive on T_2.

<u>Lemma 4.3</u> Let a group G have an action on a set S and let H be a subgroup of G. Let

$$T = \{ s\varepsilon S | s^h = s \text{ for all } h\varepsilon H \}.$$

Then $N_G(H)$, the normalizer of H in G, will permute the members of S amongst themselves.

<u>Proof</u>: Let n be arbitrary in $N_G(H)$, let t be arbitrary in T, and let h_1 be arbitrary in H.

Then $$nh_1n^{-1} = h_2 \varepsilon H.$$

Thus $$t^{nh_1n^{-1}} = t^{h_2} = t \quad \text{by definition of } T.$$

Hence $$(t^n)^{h_1} = t^n .$$

As h_1 was arbitrary in H, $t^n \varepsilon T$; as n was arbitrary in $N_G(H)$, $N_G(H)$ permutes members of T amongst themselves.

<u>Lemma 4.4</u> (see Gleason (4)) Let a group G have an action on a set S, and let $T \subseteq S$ be such that for any $t\varepsilon T$, there exists $g\varepsilon G$ of given prime order p such that g fixes t but no other element of S. Then T is contained in an orbit of S under G.

<u>Proof</u>: Choose $t\varepsilon T$ and $g\varepsilon G$ as specified in the hypotheses, and let D be the orbit of S under G to which t belongs. Then $\langle g \rangle$, the group generated by g, is a permutation group of order p on D and partitions it into disjoint

orbits. The orbit of t has order one and the orbits of all other members of D, since none is fixed by g, will have order p. Hence

$$|D| = 1+np \qquad \ldots\ldots (1)$$

for some integer n.

If $T \nsubseteq D$, then there exists $\bar{t} \varepsilon T \cap (S-D)$ and $\bar{g} \varepsilon G$ such that $\bar{t}^{\bar{g}} = \bar{t}$ but all other elements of S are moved by $\bar{g}$. Thus in particular all elements of D are moved by $\bar{g}$, so the permutation group $\langle \bar{g} \rangle$ partitions D into disjoint orbits each of order p. Hence $|D|$ is divisible by p, which contradicts equation (1). Hence the assumption that such a $\bar{t}$ exists is false and $T \subseteq D$.

<u>Definitions</u>

(1) A permutation group G transitive on a set S is said to be <u>regular</u> on S if $|G| = |S|$.

(2) A permutation group G is said to be a <u>Frobenius group</u> on a set S if:

a) G is transitive but not regular on S,

b) only the identity of G fixes two distinct elements of S.

(3) The <u>kernel</u> K of a Frobenius group F on a set S is defined as follows:

$$K = \{k \varepsilon F \mid s^k \neq s \quad \text{for all } s \varepsilon S\} \cup \{1\}.$$

(4) Let G be a permutation group transitive on a set S. Then G is said to be imprimitive if S can be partitioned into a collection $\{T_i\}$ of disjoint sets,

each of the same order t where $1 < t < |S|$, such that each element of G maps any T_i either onto itself or onto another of the sets. G is said to be primitive on S if it is not imprimitive on S.

(5) A permutation group G on a set S is said to be doubly transitive on S if for arbitrary $\alpha \varepsilon S$, G is transitive on S and G_α is transitive on $S-\{\alpha\}$.

Definition A fixed-point-free automorphism α of a finite group G is an automorphism of G such that $g^\alpha = g \Longleftrightarrow g = 1$ for all $g \varepsilon G$.

Lemma 4.5 If a finite group G has a fixed-point-free automorphism α of order 2, then G is abelian.

Proof: First note that the mapping $x \longrightarrow x^{-1}x^\alpha$, $x \varepsilon G$, is one-to-one; for if $x^{-1}x^\alpha = y^{-1}y^\alpha$ for $x,y \varepsilon G$ then $yx^{-1} = y^\alpha(x^\alpha)^{-1} = (yx^{-1})^\alpha$ and α fixes yx^{-1}. Thus $yx^{-1} = 1$, i.e. $y = x$ and the mapping is one-to-one as claimed. Hence as G is finite it is onto, so $y_1, y_2 \varepsilon G \Longrightarrow$ there exist $x_1, x_2 \varepsilon G$ such that $y_1 = x_1^{-1}x_1^\alpha$ and $y_2 = x_2^{-1}x_2^\alpha$, and x_1 and x_2 are unique. But $y_1 = x_1^{-1}x_1^\alpha \Longrightarrow y_1^\alpha = (x_1^{-1})^\alpha x_1^{\alpha^2} = (x_1^\alpha)^{-1}x_1 = y_1^{-1}$; consequently

$$(y_1y_2)^\alpha = y_1^\alpha y_2^\alpha = y_1^{-1}y_2^{-1}.$$

But $$(y_1y_2)^\alpha = (y_1y_2)^{-1} = y_2^{-1}y_1^{-1};$$

hence $y_1^{-1}y_2^{-1} = y_2^{-1}y_1^{-1}$ and taking inverses gives

$$y_1y_2 = y_2y_1.$$

As y_1 and y_2 were arbitrary in G, G is abelian.

Lemma 4.6 (see Wagner (12)). Let F be a Frobenius group of order 2n on a set S of order n, where n is odd. Then:

(1) If α and β are distinct elements of S, there exists $f \varepsilon F$ such that $f^2 = 1$ and $\alpha^f = \beta$.

(2) The kernel K of F is a characteristic subgroup of F and is regular on S.

(3) If H is a subgroup of F possessing r distinct elements of order 2, where $r > 1$, then $|H| = 2r$.

Proof: Any element f of order 2 in F interchanges elements of S in pairs, except for those elements that it fixes. As $|S|$ is odd, this implies that f fixes at least one element of S. As F is a Frobenius group, f fixes no more than one element of S; hence f fixes exactly one element of S. Thus to each element of order 2 in F there corresponds exactly one point of S fixed by it.

Conversely, for arbitrary $\alpha \varepsilon S$, by lemma 4.1

$$|\mathrm{Orb}\ (\alpha)|\ |F_\alpha| = |F|.$$

As F is transitive on S, $|\mathrm{Orb}(\alpha)| = n$; also $|F| = 2n$; hence $|F_\alpha| = 2$. Thus there is, for each element $\alpha \varepsilon S$, exactly one element of F of order 2 fixing α. Hence there is a one-to-one correspondence between points of

S and elements of F of order 2. The element of order 2 in F that fixes $\alpha \varepsilon S$ will be denoted f_α.

Assertion (1) is now proved. Let α and β be distinct points of S and let $\gamma \varepsilon S-\{\alpha\}$. Then $\alpha^{f_\gamma} \neq \alpha$ (as otherwise f_γ would fix both α and γ, which contradicts F being Frobenius). Now suppose that for some $\delta \varepsilon S$, $\alpha^{f_\gamma} = \alpha^{f_\delta}$. Then $\alpha^{f_\gamma f_\delta} = \alpha$, and

$$(\alpha^{f_\gamma})^{f_\gamma f_\delta} = \alpha^{f_\gamma^2 \, f_\delta} = \alpha^{f_\delta} = \alpha^{f_\gamma},$$

so $f_\gamma f_\delta$ fixes the distinct points α and α^{f_γ}. Thus $f_\gamma f_\delta = 1$, i.e. $f_\gamma = f_\delta$, and by the one-to-one correspondence established above, $\gamma = \delta$. Hence $\alpha^{f_\gamma} = \alpha^{f_\delta} \Longrightarrow \gamma = \delta$, and so as γ ranges over the (n-1) elements of $S-\{\alpha\}$, α^{f_γ} also ranges over these (n-1) elements; hence there must exist $\gamma \varepsilon S-\{\alpha\}$ such that $\alpha^{f_\gamma} = \beta$, and as ${f_\gamma}^2 = 1$, assertion (1) holds.

To prove assertion (2), note that from the proof of (1) K consists of all elements of F that are not of order 2; hence $|K| = 2n-n = n$. No two elements of order 2 in F interchange the same two elements of S; for suppose that $x,y \varepsilon F$ (and x and y are of order 2) and that α and β are distinct elements of S such that $\alpha^x = \beta$, $\alpha^y = \beta$. Then $\beta^x = \alpha$ and $\beta^y = \alpha$, and so $\beta^{xy} = \alpha^y = \beta$. Similarly $\alpha^{xy} = \alpha$, so xy fixes β and α: hence as F is Frobenius, $xy = 1$, i.e. $x = y$.

Let $x_1, \cdots, x_n$ be the n elements of order 2 in F and consider the set $x_1x_1, x_1x_2, \cdots, x_1x_n$. These are n distinct elements of F and none but $x_1x_1 = 1$ fixes an element of S; for if x_1x_p fixed α, then both x_1 and x_p would interchange α and α^{x1}, in contradiction to the previous paragraph. Hence $K = \{x_1x_1, \cdots, x_1x_n\}$. But similarly $K = \{x_1x_1, x_2x_1, \cdots, x_nx_1\}$; thus if $k_1, k_2 \varepsilon K$ then $k_1 = x_px_1$ and $k_2 = x_1x_q$ for $1 \leq p \leq n$, $1 \leq q \leq n$ and $k_1k_2 = x_px_q \varepsilon K$ by the characterization of K. Hence K is closed under multiplication, and is thus a group. Evidently K is normal in F, and as it consists of all elements not of order 2 (plus the identity), it is characteristic in F. As no element of K (other than 1) fixes an element of S and $|K| = |S|$, it follows that K is regular on S.

To prove assertion (3), let f_γ be an element of order 2 in H (as H is a subgroup of F, all elements of order 2 in H will be of this form). Let T be the orbit of S under H containing γ, and let $|T| = c$. As f_γ fixes $\gamma \varepsilon T$ and interchanges other elements of T in pairs, c is odd. Now $|H_\gamma| \geq 2$ as H_γ contains both 1 and γ; however $|H_\gamma| \leq |F_\gamma| = 2$. Hence $|H_\gamma| = 2$. But by lemma 4.1,

$$|\text{Orb } \gamma||H_\gamma| = |H|$$

and thus $$|H| = 2c.$$

Now consider the action of H on T. Only the identity of H fixes more than one point of T, as H is a subgroup of a Frobenius group; also, H is transitive but not regular on T, and $|H| = 2c$ while $|T| = c$, where c is odd. Hence the same hypotheses hold on H and T as hold on F and S. Consequently there is a one-to-one correspondence between elements of T and elements of order 2 of H. Thus there are c elements of order 2 in H, i.e. $r = c$, and thus $|H| = 2r$.

Lemma 4.7 (see Wagner (12)) Let G be a doubly transitive permutation group on a set S consisting of (n+1) elements, where n is odd. Let $\alpha \varepsilon S$ be such that G_α contains a subgroup F_α of even order which is a Frobenius group on $S-\{\alpha\}$. Then G_α is primitive on $S-\{\alpha\}$.

Proof: For an arbitrary element $\beta \varepsilon S$, since G is transitive on S there exists $g \varepsilon G$ such that $\alpha^g = \beta$. Then $g^{-1}F_\alpha g$, which will be denoted as F_β, is a subgroup of $g^{-1}G_\alpha g = G_\beta$, and is a Frobenius group on $S- \{\beta\}$ (since F_β is isomorphic to F_α and thus plays the same role vis-a-vis β as F_α plays towards α).

Let K_β be the kernel of F_β. Then by lemma 4.6 part (2) K_β is a characteristic subgroup of F_β and is regular on $S-\{\beta\}$. Hence $|K_\beta| = |S-\{\beta\}| = n$. As $|F_\beta|$ is even, F_β contains an element b of order 2; as $|K_\beta|$ is odd, $b \notin K_\beta$ and hence by definition of the kernel, b fixes an element of $S-\{\beta\}$.

Let $\bar{F}_\beta$ be the group generated by K_β and b. As

K_β is normal in F_β (being characteristic), a typical element f of $\bar{F}_\beta$ is of the form $f = b^r k$ where $k \varepsilon K_\beta$ and $r = o$ or 1. Hence $|\bar{F}_\beta| = 2|K_\beta| = 2n$. Also, $\bar{F}_\beta$ is transitive on $S-\{\beta\}$, as it contains K_β, but is not regular, as it contains $b \neq 1$ fixing an element of $S-\{\beta\}$. Only the identity of $\bar{F}_\beta$ fixes two distinct elements of $S-\{\beta\}$ as $\bar{F}_\beta$ is a subgroup of the Frobenius group F_β; hence $\bar{F}_\beta$ is a Frobenius group on $S-\{\beta\}$.

Now assume that G_α is not primitive on $S-\{\alpha\}$. Then $S-\{\alpha\}$ can be partitioned into sets of imprimitivity $T_1, T_2, \cdots, T_s$, each of order t where $1 < t < n$. Then $st = n$, and as n is odd, so are s and t. Let $T_1 = \{\delta_i | i = 1 \text{ to } t\}$ and let $\gamma \varepsilon T_s$. As $\bar{F}_\gamma$ is a Frobenius group on a set $S-\{\gamma\}$ of odd order n, as $\alpha \neq \gamma$ and $\beta_i \neq \gamma$, $i = 1$ to t, and as $\bar{F}_\gamma = 2n$, the hypotheses of part (1) of lemma 4.5 hold and so there exists a set of elements of $\bar{F}_\gamma$, namely $\{c_i | i = 1 \text{ to } t\}$, such that $c_i^2 = 1$ and $\alpha^{c_i} = \beta_i$, $i = 1$ to t.

Let $T_1 \cup \{\alpha\} = V$. Then $V^{c_i} = V$ for $i = 1$ to t. To prove this, note first that $\alpha^{c_i} = \beta_i \varepsilon V$ for $i = 1$ to t. Now suppose that there exist j and k, $1 \leq j \leq t$ and $1 \leq k \leq t$, such that $\beta_k{}^{c_j} = \delta$ and $\delta \notin V$. But as $\bar{F}_\delta$ is a Frobenius group of order $2n$ on the set $S-\{\delta\}$ of order n (n odd), and as $\alpha, \beta_j \neq \delta$ (since $\delta \notin V$), by lemma 4.6, part (1), there exists $d \varepsilon \bar{F}_\delta$ such that $d^2 = 1$ and $\alpha^d = \beta_j$. Thus $\alpha^{c_jd} = \beta_j^{\,d} = \alpha$, and hence $c_jd \varepsilon G_\alpha$. But $\beta_j^{\,c_jd} = \alpha^d = \beta_j$, so as G_α is imprimitive on $S-\{\alpha\}$ by assumption and c_jd fixes $\beta_j \varepsilon T_1$, c_jd should map T_1 onto T_1. However, $\beta_k \varepsilon T_1$ and $\beta_k^{\,c_jd} = \delta^d = \delta$; hence as $\delta \not\varepsilon T_1$, c_jd does not map T_1 onto T_1. This contradiction implies that the assumed j and k do not exist and hence $V^{c_i} = V$, $i = 1$ to t, as claimed.

Let H be the subgroup of $\bar{F}_\gamma$ generated by the $\{c_i\}$. Also, H maps V onto itself by the above remarks, and from the way in which the $\{c_i\}$ were defined, H is transitive on V. Also, as $\bar{F}_\gamma$ is a Frobenius group on $S-\{\gamma\}$, each non-identity element of H either fixes no point of $S-\{\gamma\}$ or has order 2 and fixes precisely one point of $S-\{\gamma\}$ (as recall $|S-\{\gamma\}| = n$ and $|\bar{F}_\gamma| = 2n$). But $|V| = t+1$ and as t is odd, t+1 is even. Thus no element of order 2 in H can fix any point of V. Hence $|H_{\beta_i}| = 1$ and $|H_\alpha| = 1$. Thus by the fundamental theorem, $|H| = t+1$. But by lemma 4.6, part (3), as H possesses at least t elements of order 2, namely the $\{c_i\}$, it follows that $|H| \geq 2t$. Thus

$$t+1 \geq 2t, \qquad \text{i.e.} \quad 1 \geq t$$

which contradicts the assumption that $t > 1$. Hence the assumption that G_α is imprimitive on $S-\{\alpha\}$ is false;

i.e. G_α is primitive on $S-\{\alpha\}$.

Lemma 4.8 Let G be a permutation group primitive on a set S and let N be a non-trivial normal subgroup of G. Then N is transitive on S.

Proof: As N is a permutation group on S it partitions S into disjoint orbits. Let α be arbitrary in S and let g be arbitrary in G. Let $\alpha^g = \beta$. If the orbit of α under N is denoted $\mathrm{Orb}_N\alpha$, then $(\mathrm{Orb}_N\alpha)^g = \mathrm{Orb}_N\beta$; for let $\gamma\varepsilon\mathrm{Orb}_N\alpha$. Then there exists $n\varepsilon N$ such that $\alpha = \gamma^n$. Thus $\alpha^g = \gamma^{ng}$. But as N is normal, there exists $\bar{n}\varepsilon N$ such that $ng = g\bar{n}$. Hence

$$\beta = \alpha^g = \gamma^{ng} = (\gamma^g)^{\bar{n}}$$

and thus $\gamma^g\varepsilon\mathrm{Orb}_N\beta$. Hence $(\mathrm{Orb}_N\alpha)^g \subseteq \mathrm{Orb}_N\beta$, and by reversing the argument, $(\mathrm{Orb}_N\beta) \subseteq (\mathrm{Orb}_N\alpha)^g$. Thus $|\mathrm{Orb}_N\beta| = |(\mathrm{Orb}_N\alpha)^g| = |\mathrm{Orb}_N\alpha|$. Evidently each $g\varepsilon G$ maps each orbit either onto itself or onto another orbit. As orbits are disjoint, they form sets of imprimitivity of G of order >1 (as $|N|>1$). Hence as G is imprimitive, $\mathrm{Orb}_N\alpha = S$ and hence N is transitive on S.

Theorem 4.1 Let G_α, F_α, and K_α be as in lemma 4.7, and in addition assume that F_α is normal in G_α. Then K_α is an elementary abelian group and thus n is a power of a prime.

Proof: As K_α is characteristic in F_α, it is normal in

G_α. As $|F_\alpha|$ is even and $|K_\alpha| = n$ and thus is odd, F_α contains an element f of order 2 not in K_α. By definition of K_α there exists $\beta\varepsilon S-\{\alpha\}$ such that $\beta^f = \beta$. Then $k \longrightarrow f^{-1}kf$ for all $k\varepsilon K_\alpha$ is a fixed-point-free automorphism of K_α; for if not then there exists $k\varepsilon K_\alpha$, $k \neq 1$, such that $fk = kf$ (as $f^{-1} = f$). Then $\beta^{fk} = \beta^{kf}$ and so $\beta^k = (\beta^k)^f$. Thus f fixes the distinct points β and β^k of $S-\{\alpha\}$ in contradiction to the fact that F_α is a Frobenius group on $S-\{\alpha\}$. Hence K_α has a fixed-point-free automorphism of order 2, so by lemma 4.5 K_α is abelian.

Now K_α has no proper non-trivial characteristic subgroups; for let N be such a group. Then $|N| < |K_\alpha| = n$. Then as K_α is normal in G_α, N is normal in G_α. But as G_α is primitive on $S-\{\alpha\}$, by lemma 4.8 N is transitive on $S-\{\alpha\}$. This contradicts the fact that $|N| < n$, and so K_α has no proper characteristic subgroups.

Assume that p is a prime > 1 dividing $|K_\alpha|$. Then $|K_\alpha| = p^r$; for if not, K_α would have a p-Sylow subgroup P properly contained in it. As K_α is abelian, P would be characteristic in K_α, contradicting the result of the previous paragraph.

Lastly, all non-identity elements of K_α have order p; for as K_α is abelian, the set $K_\alpha{}^p = \{k^p | k\varepsilon K_\alpha\}$ is a proper characteristic subgroup of K_α, and hence is the identity. Hence $k^p = 1$ for all $k \varepsilon K_\alpha$, and thus K_α is elementary abelian of order $n = p^r$ for some prime p.

The following lemmas and theorems are due to Gleason (4). Proofs are also given in Pickert (8), pages 26-28.

<u>Lemma 4.9</u> Let ℓ be a line and C be a point (incident with ℓ) of a finite projective plane π of order n. Denote the group of all elations with centre C and axis ℓ as $G_{C,\ell}$ and the group of all elations with axis ℓ as G_ℓ. Then:

(1) $|G_{C,\ell}|$ divides n

(2) $|G_\ell|$ divides n^2

(3) $|G_\ell| = n^2 \Longleftrightarrow \pi$ is a translation plane with respect to ℓ.

<u>Proof:</u> (1) Let m be an arbitrary line through C ($m \neq \ell$). Then as each element of $G_{C,\ell}$ fixes m, $G_{C,\ell}$ acts as a permutation group on the n points of $S = m-\{c\}$ (where m is thought of as a point set). By lemma 1.4, if $Q \varepsilon S$ and $g \varepsilon G_{C,\ell}$, then Q and Q^g uniquely determine the element g. Hence $|\text{Orb } Q| = G_{C,\ell}$. By lemma 4.1, $|\text{Orb } Q|$ divides $|S|$ and hence $|G_{C,\ell}|$ divides n.

(2) The n^2 points of $\mathcal{P}-\{\ell\} = T$ (where ℓ is taken as a point set) are permuted amongst themselves

by elements of G_ℓ , and hence G_ℓ acts as a permutation group on T. By the argument used in (1), if $Q\varepsilon T$ then $|\mathrm{Orb}\ Q| = |G_\ell|$. By lemma 4.1, $|\mathrm{Orb}\ Q|$ divides $|T|$ and hence $|G_\ell|$ divides n^2.

(3) Suppose that $|G_\ell| = n^2$. Then $|\mathrm{Orb}\ Q| = n^2$ for an arbitrary point $Q\varepsilon T$. Hence as $|T| = n^2$, if Q and R are any two points of T there exists $g\varepsilon G$ such that $Q^g = R$. But this clearly implies that π is (C,ℓ)-transitive for all $C\varepsilon\ell$; i.e. that π is a translation plane with respect to ℓ .

Conversely, if π is a translation plane with respect to ℓ and if Q and R are arbitrary in T, then there exists an elation g in G_ℓ such that $Q^g = R$. Thus $|\mathrm{Orb}\ Q| = n^2$, but as $|\mathrm{Orb}\ Q| = |G_\ell|$ it follows that $|G_\ell| = n^2$.

<u>Lemma 4.10</u> Let ℓ be a line of a projective plane π of order n. If for each point $C\varepsilon\ell$ the elation group $G_{C,\ell}$ has order $m>1$, then π is a translation plane with respect to ℓ.

<u>Proof</u>: Let $|G_\ell| = r$. By part (2) of the preceding lemma, $rk = n^2$ for some integer $k>0$. By lemma 1.5 Corollary II, $G_\ell = \bigcup_{C\varepsilon\ell} G_{C,\ell}$, and evidently $|G_{C_1,\ell}\cap G_{C_2,\ell}| = 1$ if $C_1 \neq C_2$, so

$$|G_\ell| = (n+1)(|G_{C,\ell}| -1)+1$$

i.e.

$$r = (n+1)(m-1)+1.$$

As $m > 1$, $r > n$ and hence $k < n$.

Since $kr = n^2$, it follows that

$$n^2 - k = (r-1)k = (n+1)(m-1)k$$

i.e. $$k = n^2 - (m-1)(n+1)k$$

or $$k-1 = n^2 - 1 - (m-1)(n+1)k$$
$$= (n+1)((n-1)-(m-1)k).$$

Thus $(n+1)$ divides $(k-1)$. As $k < n$, this implies that $k-1 = 0$, i.e. $k = 1$. Hence $r = n^2$ and by part (3) of the preceding lemma, π is a translation plane with respect to ℓ.

Lemma 4.11 Let π be a projective plane possessing a line ℓ with the following properties: for each $C \varepsilon \ell$; (1) there exists a non-trivial (C,ℓ)-elation,

(2) there exists a line m, $C \varepsilon m$ and $m \neq \ell$, such that there exists a non-trivial (C,m)-elation.

Then π is a translation plane with respect to ℓ.

Proof: By theorem 1.1 and hypothesis (1), every non-trivial elation with axis ℓ has the same prime order p. For a fixed point $C \varepsilon \ell$ denote $\bigcup_{C \varepsilon m} G_{C,m}$, the set of all elations with centre C, by G_C. By the dual of Corollary II of lemma 1.5, G_C is a group. By the hypotheses and the dual of theorem 1.1, G_C will be an elementary abelian p-group for each $C \varepsilon \ell$.

Let H be the group generated by all non-trivial (C,m)-elations, of the type described in hypothesis (2), for each $C \varepsilon \ell$. Then each element of H fixes the line ℓ, and so H acts as a permutation group on the points of ℓ. Also, for each $C \varepsilon \ell$ there exists an element of H of order p that fixes C but no other point of ℓ (namely the non-trivial (C,m)-elation for that C); hence by lemma 4.4 H is transitive on the points of ℓ. Thus if C_1 and C_2 are arbitrary distinct points of ℓ there exists $h \varepsilon H$ such that $C_1{}^h = C_2$. By lemma 1.6, $G_{C_2,\ell} = h^{-1}(G_{C_1,\ell})h$. Thus $|G_{C_2,\ell}| = |G_{C_1,\ell}| > 1$ and as C_1 and C_2 were arbitrary on ℓ, it follows by lemma 4.10 that π is a translation plane with respect to ℓ.

<u>Definition</u> Let π be a projective plane. Then the collineation group generated by all elations of π is called the <u>little projective group</u> of π.

<u>Theorem 4.2</u> Let π be a finite projective plane and let G be a collineation group of π such that for every line ℓ and point C such that $C \varepsilon \ell$, G possesses a non-trivial (C,ℓ)-elation. Then π is Desarguesian and G contains the little projective group of π as a subgroup.

Proof: From the hypotheses, every line of π satisfies the conditions imposed on the line ℓ in lemma 4.11. Hence from lemma 4.11 π is a translation plane with respect to every line of π, i.e. π is an alternative plane. As π is finite, from the conclusions of Chapter III it follows that π is Desarguesian. Evidently the elations in G generate all possible elations of π so G contains the little projective group of π.

The following result is due to Andre (1).

Theorem 4.3 Let γ be a line of a projective plane π and let γ be the axis of two non-trivial homologies σ_1 and σ_2 with distinct centres C_1 and C_2 respectively. Let G be the group generated by σ_1 and σ_2. Then:

(1) All elements of G are central collineations with axis γ.

(2) G has an action on the points of $\pi - \{\gamma\}$ and the set of centres of the homologies in G is contained in one orbit of G.

(3) There is an elation in G mapping C_1 into C_2.

Proof: Result (1) follows immediately from the fact that every element of G fixes γ pointwise.

Let $C_1C_2 = \ell$ and let F be the group of elations of G with centre $\ell \cap \gamma$. It is easily verified that F is a normal subgroup of G. Let $|F| = t$.

Regarding G as a permutation group on the points of $\pi - \{\gamma\}$, let $\{T_i \mid i = 1 \text{ to } N\}$ be the orbits of $\pi - \{\gamma\}$ under G. Regarding F as a permutation group on $\pi - \{\gamma\}$, it is seen that F fixes each T_i and hence can be regarded as a permutation group on T_i. F thus splits each T_i into orbits, each of which has length t since an element $f \epsilon F$ is uniquely determined by P and P^f for any point $P \epsilon \pi - \{\gamma\}$.

Let t_i be the number of orbits of T_i under F. Then $tt_i = |T_i|$ and as there are N orbits of the n^2 points of $\pi - \{\gamma\}$ under G, it follows that

$$n^2 = \sum_{i=1}^{N} tt_i \qquad \ldots\ldots (1)$$

Let P_1 and P_2 be two points in the same orbit of $\pi - \{\gamma\}$ under G. Then Orb P_1 = Orb P_2 and by the fundamental theorem it immediately follows that $|G_{P_1}| = |G_{P_2}|$. But G_{P_1}, the set of elements that fix P_1, is just the set of homologies with centre P_1 (plus the identity). Thus the number of homologies with centre P_1 equals the number of homologies with centre P_2, and hence without ambiguity the number of homologies (including the identity) whose centre is a given point in T_i can be denoted s_i.

Let $|G| = k$. As G can be partitioned into $F \cup (G-F)$, where G-F is the set of all homologies in G (excepting the identity), we can write

$$|G| = |F| + |G-F|$$

i.e. $$k = t + \sum_{i=1}^{N} tt_i(s_i - 1) \qquad \ldots\ldots (2)$$

where $tt_i(s_i-1)$ is evidently the number of homologies in G with centres in T_i.

Let $C \varepsilon T_i$. Then applying the fundamental theorem,

$$|\text{Orb } C|\,|G_C| = |G|$$

i.e. $$tt_i s_i = k \qquad \ldots\ldots (3)$$

Substituting this in equation (2) gives

$$k = t + \sum_{i=1}^{N} k - \sum_{i=1}^{N} tt_i .$$

Combining this with equation (1) gives

$$k = t + Nk - n^2$$

i.e. $$k(N-1) = n^2 - t$$

so by equation (3),

$$tt_i s_i (N-1) = n^2 - t$$

i.e. $$(N-1)(t_i s_i) = n^2 t^{-1} - 1.$$

Summing over the N orbits, this becomes

$$\frac{N-1}{n^2 t^{-1} - 1} \sum_{i=1}^{N} t_i = \sum_{i=1}^{N} \frac{1}{s_i} .$$

Using equation (1) this becomes

$$\left(\frac{N-1}{n^2 t^{-1} - 1}\right)\left(\frac{n^2}{t}\right) = \sum_{i=1}^{N} \frac{1}{s_i}$$

i.e. $$\frac{N-1}{1 - \frac{t}{n^2}} = \sum_{i=1}^{N} \frac{1}{s_i} \qquad \ldots\ldots (4)$$

Now the left-hand side, and hence the right-hand side, of equation (4) is greater than (N-1),

i.e. $$\sum_{i=1}^{N} \frac{1}{s_i} > N-1. \qquad \text{.....} \ (5)$$

Suppose that $s_i \geq 2$ for $i = 1$ to m and that $s_i = 1$ for $i = (m+1)$ to N. Then $m \geq 1$ as the number of homologies with centre C_1 is ≥ 2 as σ_1 and the identity are two such. Thus $\frac{1}{s_i} \leq \frac{1}{2}$ for $i = 1$ to m and so

$$\sum_{i=1}^{m} \frac{1}{s_i} \leq \sum_{i=1}^{m} \frac{1}{2} = \frac{m}{2} \qquad \text{.....} \ (6)$$

As $s_i = 1$ for $i = (m+1)$ to N, it follows that

$$\sum_{i=m+1}^{N} \frac{1}{s_i} = N-m.$$

Consequently

$$\sum_{i=1}^{m} \frac{1}{s_i} = \sum_{i=1}^{N} \frac{1}{s_i} - \sum_{i=m+1}^{N} \frac{1}{s_i}$$

$$> (N-1) - (N-m) \qquad \text{(using result (5))}$$

i.e. $$\frac{m}{2} > m-1 \qquad \text{(using result (6)).}$$

Thus $m > 2m-2$, and so $2 > m$. But as $m \geq 1$, it follows that $m = 1$. Hence only one orbit of $\pi - \{\gamma\}$ under G, namely T_1, is such that a point P of that orbit is the centre of more than one homology. Hence the centres of the non-trivial homologies are all contained in one orbit T_1 of $\pi - \{\gamma\}$ under G and the second claim is true.

Setting $i = 1$ in equation (3) and substituting in equation (2), we obtain

$$tt_1 s_1 = t+t \sum_{i=1}^{n} t_i(si^{-1}).$$

As $s_i = 1$ for $i > 1$, this becomes

$$t_1 s_1 = 1+t_1 s_1 - t_1$$

i.e. $\qquad t_1 = 1.$

Hence recalling the definition of t_1, the orbit T_1 has only one suborbit under F; i.e. F is transitive on T_1. Hence as C_1 and $C_2 \varepsilon T_1$, there is an elation in F sending C_1 into C_2. Hence result (3) holds.

Theorem 4.4 Let π be a finite projective plane and let G be a collineation group of π.

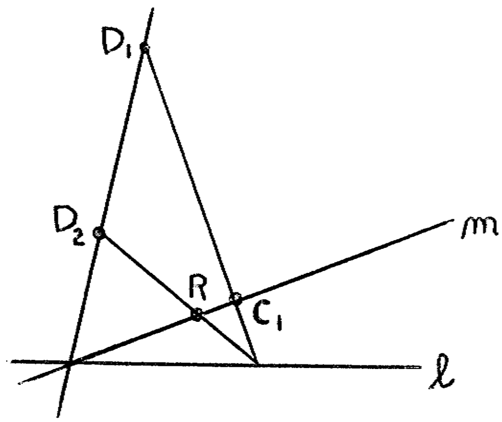
Then:

(1) If ℓ and m are distinct lines of π such that for every point $C \varepsilon m$ ($C \neq \ell \cap m$) there exists a non-trivial (C, ℓ)-homology in G, then π is $(\ell \cap m, \ell)$-transitive.

(2) If ℓ is a line such that $C \notin \ell \Longrightarrow$ there exists a non-trivial (C, ℓ)-homology, then π is a translation plane with respect to ℓ.

(3) If for every point C and line ℓ of π, $C \notin \ell$, there exists a non-trivial (C, ℓ)-homology in G then π is Desarguesian and G contains the little projective group of π.

Proof: (1) Let C_1 and C_2 be arbitrary distinct points of $m - \{\ell \cap m\}$ and let them be centres of non-trivial homologies σ_1 and σ_2(respectively) of G. By theorem 4.3 G contains an elation φ such that $C_1^{\varphi} = C_2$. Let D_1 and D_2 be arbitrary points of $\pi - \{\ell\}$ such that $\equiv D_1, D_2, \ell \cap m$. Then let



$$(D_1C_1 \cap \ell)D_2 \cap m = R.$$

There is an elation mapping $C_1 \longrightarrow R$ and under this $D_1 \longrightarrow D_2$. Hence π is $(\ell, \ell \cap m)$-transitive.

(2) From (1) it immediately follows that π is (P, ℓ)-transitive for every $P \varepsilon \ell$, and hence π is a translation plane with respect to ℓ.

(3) From (2) it immediately follows that π is a translation plane with respect to all lines of π, and hence is a finite alternative plane. Hence by the result of chapter 3, π is Desarguesian and G contains all possible elations of π and hence the little projective group.

Lemma 4.12 Let φ be a collineation of a finite projective plane π of order n. Let N_{φ} be the number of points fixed by φ and $\bar{N}_{\varphi}$ the number of lines fixed by φ. Then $N_{\varphi} = \bar{N}_{\varphi}$.

Proof: Define

$$K = \left\{(P, \ell) \;\middle|\; P \text{ a point}, \ell \text{ a line}, P \varepsilon \ell, P \varepsilon \ell^{\varphi}\right\}.$$

Two expressions for the order of K are now calculated. Each point P fixed by φ has (n+1) lines through it, and for each such line ℓ, $P \varepsilon \ell$ and $P \varepsilon \ell^{\varphi}$. Each point Q not fixed by φ (there are $(n^2+n+1)-N_{\varphi}$ of these) has exactly one line ℓ through it, namely $QQ\varphi^{-1}$, such that $Q \varepsilon \ell$ and $Q \varepsilon \ell^{\varphi}$. Hence

$$|K| = N_{\varphi}(n+1)+(n^2+n+1-N_{\varphi}).$$

The dual argument gives

$$|K| = \bar{N}_{\varphi}(n+1)+(n^2+n+1-\bar{N}_{\varphi})$$

and it immediately follows that $N_{\varphi} = \bar{N}_{\varphi}$.

Lemma 4.13 Let G be a permutation group on a set S, and let k be the number of orbits of S under G. Then $k|G| = \sum rf_r$ where f_r is the number of elements of G that fix r elements of S, and summation is over r.

Proof: Let $|S| = n$. Set up a matrix $M = (m_{ij})$ with rows indexed by elements of G and columns indexed by elements of S. Then M has $|G|$ rows and n columns. Assign elements of M as follows:

$$m_{ij} = 1 \iff \alpha_j^{g_i} = \alpha_j$$

$$m_{ij} = 0 \iff \alpha_j^{g_i} \neq \alpha_j.$$

Let N be the total number of "1"s appearing in M. For $r = 0,1,2,\cdots$ the number of rows of M containing r "1"s is f_r; hence as N is the sum over all rows of M of the number of "1"s in each row, it follows that

$$N = \sum_r r f_r \qquad \ldots\ldots (1)$$

However, the number of "1"s appearing in a column of M indexed by $\alpha \varepsilon S$ is the number of elements of G fixing α, i.e. is $|G_\alpha|$. Thus

$\sum_{\alpha \varepsilon S} |G_\alpha| = N$ (as N is the sum over all columns of the number of "1"s in each column).

Let the k orbits of S under G be $\{T_i \mid i = 1 \text{ to } k\}$

Then

$$\sum_{\alpha \varepsilon S} |G_\alpha| = \sum_{i=1}^{k} \left(\sum_{\alpha \varepsilon T_i} |G_\alpha| \right).$$

But by the fundamental theorem

$$\alpha_1 \varepsilon T_i, \alpha_2 \varepsilon T_i \Longrightarrow |G_{\alpha_1}| = |G_{\alpha_2}|$$

and hence $\sum_{\alpha \varepsilon T_i} |G_\alpha| = |\text{Orb } \alpha|\,|G_\alpha| = |G|$.

Thus $N = \sum_{\alpha \varepsilon S} |G_\alpha| = \sum_{i=1}^{k} |G| = k|G|$

so by equation (1),

$$\sum_r r f_r = k\,|G|.$$

<u>Theorem 4.5</u> Let G be a collineation group of a finite projective plane π. Then the number k of orbits of points of π under G equals the number $\bar{k}$

of orbits of lines of π under G.

Proof: By lemma 4.13,

$$k|G| = \sum_r rf_r$$

where f_r is the number of elements in G that fix r points of π. Similarly

$$\bar{k}\,|G| = \sum_r r\bar{f}_r$$

where $\bar{f}_r$ is the number of elements in G that fix r lines of π. But by lemma 4.12, if $g \varepsilon G$ then g fixes r points of π if and only if g fixes r lines of π. Thus for all r, $f_r = \bar{f}_r$. Consequently $\sum_r rf_r = \sum_r r\bar{f}_r$ and so $k|G| = \bar{k}|G|$; hence $k = \bar{k}$.

Definition: Let $\pi = \{\mathcal{P}, \mathcal{L}, \varepsilon\}$ be a projective plane with point set $\mathcal{P}$ and line set $\mathcal{L}$. Then a function φ mapping $\mathcal{P}$ onto $\mathcal{L}$ and $\mathcal{L}$ onto $\mathcal{P}$ such that $P \varepsilon \ell \Longleftrightarrow \ell^{\varphi} \varepsilon P^{\varphi}$ is called a correlation of π.

As φ is one-to-one onto, its inverse exists and is a correlation. Evidently φ^2 is a collineation of π.

If φ is correlation such that $\varphi^2 = 1$, then φ is called a polarity of π. A point P is an absolute point of φ if $P \varepsilon P^{\varphi}$.

Theorem 4.6 (see Baer (2)) Every polarity φ of a finite projective plane π of order n possesses absolute points.

<u>Proof</u>: Define an m-cycle as an ordered m-tuplet of points $(P_1,\cdots,P_m)$, not all necessarily distinct, such that $P_i \varepsilon P_{i+1}^{\varphi}$ for i = 1 to (m-1) and $P_m \varepsilon P_1{}^{\varphi}$. Let Z_m be the number of ordered m-cycles of φ. Evidently the one point of a 1-cycle is an absolute point.

Let p be a prime; then $(Z_p - Z_1)$ is divisible by p. To prove this note that there are two types of p-cycles. The first is of the form $(P,\cdots,P)$ where the same point P is repeated p times. Evidently such a P is an absolute point and thus there are Z_1 such p-cycles. The second type is the set of p-cycles in which two or more distinct points occur in the cycle; there are $(Z_p - Z_1)$ p-cycles of this type.

Let $(P_1,\cdots,P_p)$ be a p-cycle of the second type and suppose that there exists an integer r, $o < r < p$, such that $P_i = P_{i+r}$, i = 1 to p, (subscripts are taken modulo p). As the set of integers modulo a prime p forms a field, there exists an integer t such that $rt \equiv 1 \pmod p$. But for an arbitrary integer $k \geq o$ it is evident by applying $P_i = P_{i+r}$ k times that $P_i = P_{i+kr}$, i = 1 to p; thus in particular $P_i = P_{i+rt}$, i = 1 to p. As indices are modulo p, this says that $P_i = P_{i+1}$ for i = 1 to p, i.e. that the given p-cycle is a p-cycle of the first type. This contradicts the assumption so no integer r as described exists. Hence p-cycles of the second type come in classes of p, where a typical class is

$$\left\{ (P_{1+r}, \cdots, P_{p+r}) \mid r = o \text{ to } p-1 \right\}$$

and each member of the class is distinct by the above argument. Hence $Z_p - Z_1$ is divisible by p.

There are now two cases, namely n even and n odd.

<u>Case (1).</u> If n is even, let (P_1, P_2) be a 2-cycle. Then $P_1 \varepsilon P_2^{\varphi}$ and $P_2 \varepsilon P_1^{\varphi}$; but as $\varphi^2 = 1$, $P_1 \varepsilon P_2^{\varphi} \Longrightarrow P_1^{\varphi} \varepsilon P_2^{\varphi^2} = P_2$, so (P_1, P_2) is a 2-cycle if and only if $P_1 \varepsilon P_2^{\varphi}$, i.e. if and only if P_1 is any of the $(n+1)$ points on P_2^{φ}. Hence as there are (n^2+n+1) points of π, there are $(n^2+n+1)(n+1)$ distinct ordered 2-cycles. As n is even, $(n^2+n+1)(n+1) = Z_2$ is odd so $Z_2 \equiv Z_1 \bmod 2$. But as 2 is a prime from the above $Z_2 \equiv Z_1 \bmod 2$, so $Z_1 \equiv 1 \bmod 2$. Hence $Z_1 \neq o$ so there exist one-cycles and hence absolute points.

<u>Case (2)</u> Suppose that n is odd. Then for $m > 3$ consider an ordered set of $(m-1)$ points, namely $\{P_1, \cdots, P_{m-1}\}$. If $P_i \varepsilon P_{i+1}^{\varphi}$ for $i = 1$ to $m-2$, such an ordered set is called an $(m-1)$-chain. There are $(n^2+n+1)(n+1)^{m-2}$ distinct ordered $(m-1)$-chains, as P_{m-1} can be chosen in (n^2+n+1) ways, P_{m-2} can be chosen to be any of the $(n+1)$ points on P_{m-1}^{φ}, P_{m-3} can be any of the $(n+1)$ points on P_{m-2}^{φ}, and so on.

A distinction is made between two types of $(m-1)$-chains. The first type is that in which $P_{m-1} = P_1$

and the second type is all other (m-1)-chains. To each (m-1)-chain of the first type there corresponds (n+1) distinct m-cycles, as the m-cycle can be completed by choosing P_m to be any of the (n+1) points of $P_1{}^{\varphi}$. Then $P_m \varepsilon P_1{}^{\varphi}$, so $P_1{}^{\varphi^2} \varepsilon P_m{}^{\varphi}$, i.e. $P_{m-1} \varepsilon P_m{}^{\varphi}$ and we indeed have an m-cycle. To each (m-1)-chain of the second type there corresponds one m-cycle, namely that for which $P_m = P_1{}^{\varphi} \cap P_{m-1}{}^{\varphi}$. This exhausts the m-cycles of φ.

However, the number of (m-1)-chains of the first type is Z_{m-2}, for the (m-1)-chains of the form $\{P_1, \cdots, P_{m-2}, P_1\}$ can be put in one-to-one correspondence with the set of (m-2)-cycles $(P_1, \cdots, P_{m-2})$ (since $P_{m-2}{}^{\varphi} \varepsilon P_1$). Hence the number of m-cycles can be written by noting that there are (n+1) m-cycles for each (m-1)-chain of the first type and $((n^2+n+1)(n+1)^{m-2} - Z_{m-2})$ other m-cycles, i.e. one for each (m-1)-chain of the second type. Thus

$$Z_m = (n+1)Z_{m-2} + (n^2+n+1)(n+1)^{m-2} - Z_{m-2}$$

i.e. $$Z_m = nZ_{m-2} + (n^2+n+1)(n+1)^{m-2} \qquad \cdots\cdots (1)$$

Now for any integer $k \geq o$,

$$Z_{2k+1} = (n+1)^{2k+1} + n^k(Z_1 - n - 1) \qquad \cdots\cdots (2)$$

To prove this induct on k. If $k = o$ it is evidently true. Suppose that it holds for (2k-1).

Then by equation (1),

$$Z_{2k+1} = nZ_{2k-1}+(n^2+n+1)(n+1)^{2k-1}$$

$$= n\left[(n+1)^{2k-1}+n^{k-1}(Z_1-n-1)\right]+(n^2+n+1)(n+1)^{2k-1}$$

(by the induction hypothesis)

$$= n(n+1)^{2k-1}+n^k(Z_1-n-1)+(n^2+n+1)(n+1)^{2k-1}$$

$$= (n+1)(n+1)^{2k-1}+n^k(Z_1-n-1)+n(n+1)(n+1)^{2k-1}$$

i.e. $Z_{2k+1} = (n+1)^{2k+1}+n^k(Z_1-n-1)$

and equation (2) evidently holds in general for all k.

As n is odd there exists an odd prime p, expressible as 2k+1 for some k, such that p divides n. In this case equation (2) becomes

$Z_p = (n+1)^p+ps$ for some integer s

$= n^p+pr+1+p$ for integers r and s.

Hence $Z_p \equiv 1 \bmod p$; but as $Z_p \equiv Z_1 \bmod p$, $Z_1 \equiv 1 \bmod p$, so $Z_1 \neq 0$ and hence there exist absolute points.

Definition: An involutory collineation of a projective plane π is a collineation of order 2.

Lemma 4.14 Let π be a projective plane of order n containing a projective subplane $\mathcal{M}$ of order m. Let incidence of points and lines in $\mathcal{M}$ be the same as that in π, and let all points of π be on extended lines of $\mathcal{M}$. Then $n = m^2$.

Proof: Each line of $\mathcal{M}$ has (m+1) points and each line of π has (n+1) points. Hence in extending a line of $\mathcal{M}$ to a line of π it is necessary to add $(n+1)-(m+1) = (n-m)$ points to the line. This must be done for each of the (m^2+m+1) lines of $\mathcal{M}$; hence $(m^2+m+1)(n-m)$ new points are added to $\mathcal{M}$ in this way. As all points of π are on extensions of lines of $\mathcal{M}$, these $(m^2+m+1)(n-m)$ points comprise all the points of $\pi-\mathcal{M}$.

These new points are all distinct; for if m_1 and m_2 are distinct lines of $\mathcal{M}$ and P is a point of $\pi-\mathcal{M}$ lying on both the extension of m_1 and the extension of m_2, then m_1 and m_2 (thought of now as lines of π) intersect both at a point of $\mathcal{M}$ and at $P\varepsilon\pi-\mathcal{M}$, contradicting the axioms of incidence. Thus as π has (n^2+n+1) points and $\mathcal{M}$ has (m^2+m+1) points, it follows that

$$n^2+n+1 = (m^2+m+1)+(m^2+m+1)(n-m)$$

i.e.

$$(n^2-m^2)+(n-m) = (m^2+m+1)(n-m)$$

$$(n-m)(n+m+1) = (m^2+m+1)(n-m).$$

As $n > m$, this implies $n = m^2$.

<u>Theorem 4.7</u> (see Baer (3)) Let σ be an involutory collineation of a finite projective plane of order n. Then either σ is a central collineation or σ fixes pointwise a subplane of π of order $\sqrt{n}$.

<u>Proof</u>: Every point of π lies on a line fixed by σ; for choose an arbitrary point $P\varepsilon\pi$. If P is not

fixed by σ then PP^{σ} is a well-defined line and $(PP^{\sigma})^{\sigma} = P^{\sigma}P^{\sigma^2} = P^{\sigma}P$. Hence PP^{σ} is fixed by σ and $P\varepsilon(PP^{\sigma})$. If P is fixed by σ, choose any line ℓ such that $P\not\in\ell$ and $\ell^{\sigma} \neq \ell$ (such a line exists as $\sigma \neq 1$). Then $\ell \cap \ell^{\sigma} \neq P$ and so $P(\ell \cap \ell^{\sigma})$ is a well-defined line through P fixed by σ (as both P and $\ell \cap \ell^{\sigma}$ are). Thus P lies on a fixed line.

Let K be the set of all points and lines of π fixed by σ. Then two lines of K intersect at a unique point of K and two points of K are joined by a unique line of K. Hence if there are four points of K of which no three are collinear, the points and lines of K comprise a projective plane. As every point of π is on a line of π fixed by σ, i.e. on an extension of a line of K, it follows by lemma 4.13 that K has order $\sqrt{n}$.

If there are not four points of K of which no three are collinear, choose P such that $P^{\sigma} \neq P$ and let $\{\ell_i | i = 1 \text{ to } n+1\}$ be the (n+1) lines through P. Then there exists, for i = 1 to n+1, a point Q_i such that $Q_i \varepsilon \ell_i$ and $Q_i^{\sigma} = Q_i$ (and thus $Q_i \neq P$). As $Q_i \varepsilon K$, i = 1 to n+1, either all (n+1) points $\{Q_i\}$ are collinear or else n of them (say Q_1 to Q_n) are collinear. In the first case σ fixes a line pointwise and hence is a central collineation; in the second case let S be the remaining point on the line $m = Q_1Q_n$. Then $m^\sigma = m$ so $S^\sigma \varepsilon m$; but $Q_i^\sigma = Q_i, i = 1$ to n, so $S^\sigma = S$ and σ fixes m pointwise and is thus a central collineation.

CHAPTER V

LOCALLY DESARGUESIAN PLANES

Let G be the collineation group of a finite projective plane π. In this chapter various assumptions are made concerning the action of G on the points and lines of π. Assumptions are also made concerning the number of elations and homologies in G. These assumptions are shown to imply in some cases that π is a translation plane or its dual, and in other cases that π is Desarguesian.

Two approaches are used; in the first, due to Wagner (13), the collineation group of the projective plane is regarded as a permutation group on the points and lines of the plane. Certain general assumptions about the orbits of the group are shown to imply that the projective plane in question is a translation plane, and a well-known theorem of Ostrom and Wagner (7), namely that if G is a collineation group doubly transitive on the points of π then π is Desarguesian, is shown to follow immediately as a corollary. The second approach, due to Wagner (11) and Piper (10), consists of postulating the existence of a certain number of central collineations and from this deducing information about the structure of the plane. The method is essentially an extension of the work of Gleason (4), and Andre (1).

Flags in Projective Planes

A flag in a projective plane π is an incident point-line pair. If the point is C and the line is ℓ, then the flag is symbolized (C, ℓ); C is called the centre of the flag and ℓ the axis of the flag. A collineation φ is said to map the flag (C_1, ℓ_1) onto the flag (C_2, ℓ_2) if and only if $C_1^{\varphi} = C_2$ and $\ell_1^{\varphi} = \ell_2$. This is symbolized by writing $(C_1, \ell_1)^{\varphi} = (C_2, \ell_2)$. Thus a collineation group G of a projective plane π has an action on the set F of flags of π. Hence the usual concepts of permutation group theory will be applicable to the collineation group G considered as a permutation group on the set F.

In the following work a very general condition on the collineation group of a finite projective plane π is shown to be sufficient to ensure that π is a translation plane. A number of preliminary lemmas must first be proved.

2-Subplanes of Projective Planes

Let π be a finite projective plane and G a collineation group of π. A 2-subgroup of G is defined to be a subgroup of G of order 2^{α} for some non-negative integer α. A non-degenerate projective subplane μ of π will be called a 2-subplane of π with respect to G if there is a 2-subgroup H of G fixing every element of μ and no other element of π.

More generally, let G be a collineation group of a finite projective plane π containing a projective subplane μ, and suppose that G permutes the elements of μ amongst themselves. Then G has an action on μ, and induces a permutation group $\bar{G}$ on the elements of μ. It is easily seen that $\bar{G}$ will be a homomorphic image of G, and that the kernel K of the homomorphism will be the set of all elements of G that fix μ elementwise.

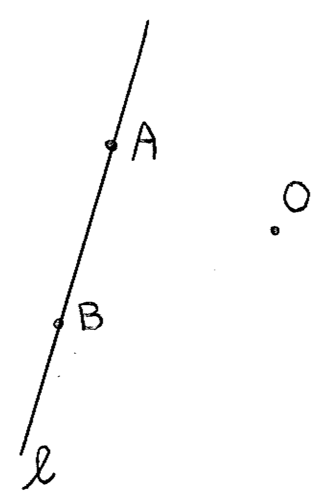
<u>Lemma 5.1</u> Let π be a finite projective plane of order n and let μ be a 2-subplane of π with respect to the collineation group G of π. If μ has order m, then $n = m^{2^g}$ for some non-negative integer g.

<u>Proof</u>: Let H be the 2-subgroup of G that fixes μ, and only μ, elementwise. Then $H = 2^\alpha$ for some integer α. If $\alpha = 0$ then $\pi = \mu$, $g = 0$, and the theorem holds. If $\alpha > 0$ then $|Z(H)| > 1$ (where $Z(H) = \{h \varepsilon H \mid hk = kh$ for all $k \varepsilon H\}$). Consequently there exists an element $\varphi \varepsilon Z(H)$ of order 2. By theorem 4.7, φ is either a central collineation or fixes a subplane π_1 of π of order $\sqrt{n}$. As H fixes only elements of μ, the first alternative is impossible. Hence φ fixes a subplane π_1 elementwise.

As $\varphi \varepsilon Z(H)$, then $N_H(\langle\varphi\rangle) = H$ if $\langle\varphi\rangle$ is the cyclic group generated by φ; hence by lemma 4.3 H permutes the elements of π_1 amongst themselves. Thus

H has an action on π_1. Denote by H_1 the permutation group of π_1 induced by H and let K be the subgroup of H fixing π_1 elementwise. Then H_1 is isomorphic to $\frac{H}{K}$, as noted earlier. It follows that H_1 is a 2-group and a collineation group of π_1 that fixes only the elements of μ. If $H_1 = 1$, then $\pi_1 = \mu$ and $n = m^2$. If $H_1 \neq 1$, then the above argument is iterated with π_1 playing the role of π and H_1 playing the role of H (note that all the requisite hypotheses hold). As n is finite, after iterating the argument a finite number of times (say g), the group corresponding to H_1 (call it H_g) is the identity. Then the plane corresponding to π_1 will be μ, and it follows that $m^{2g} = n$.

<u>Definition</u> A projective plane π will be said to have the homology property if π contains a fixed line and a fixed point O, $O \notin \ell$, such that for any two distinct points A and B on ℓ, there exists an involutory homology of π with axis OA and centre B.



<u>Lemma 5.2</u> Let π be a finite projective plane of order n possessing the homology property. Then $n = p^m$ for some prime p.

Proof: Let ℓ and O be the fixed line and point of π respectively, and let G be the group of collineations generated by all homologies with centre on ℓ and axis through O. Let A be an arbitrary point of ℓ, and define K_A to be the subgroup of G generated by all the involutory homologies of π with centre on ℓ and axis OA. Note that K_A is a proper subgroup of G_A, as G_A includes homologies with centre A.

The group G fixes ℓ and hence has an action on the points of ℓ; thus K_A also has such an action. Also, as π has the homology property, for any point B of $\ell-\{A\}$ there is a (B,OA)-homology of order 2 in K_A. Thus by theorem 4.4, K_A is (A,OA)-transitive, i.e. is transitive on the points of $\ell-\{A\}$. Further, all elements of K_A are, from its definition, central collineations with axis OA; hence by lemma 1.3 only the identity of K_A fixes two points of $\ell-\{A\}$ and K_A is thus a Frobenius group on the points of $\ell-\{A\}$.

By the above reasoning, for any distinct points A_1 and B_1 on ℓ, G_{A_1} is transitive on $\ell-\{A_1\}$ and G_{B_1} is transitive on $\ell-\{B_1\}$; hence G is transitive on the points of ℓ. Since, for an arbitrary $C\varepsilon\ell$, G_C is transitive on $\ell-\{C\}$, it follows that G is doubly transitive on the points of ℓ.

Finally, K_A is normal in G_A; for let α be a generator of K_A and σ a generator of G_A. Then α is a (C,OA)-

homology where $C \in \mathcal{l} - \{A\}$; thus by lemma 1.6, $\sigma^{-1}\alpha\sigma$ is a $(C^{\sigma}, (OA)^{\sigma})$-collineation. As G fixes O and G_A fixes A, $(OA)^{\sigma} = OA$, so $\sigma^{-1}\alpha\sigma$ is an involutory homology with axis OA and hence is in K_A. It follows that K_A is normal in G_A.

As K_A is generated by involutory homologies it has even order; by the definition of G, any generator of G interchanges all but two of the points of $\mathcal{l}$ in pairs, so (n-1) is even, i.e. n is odd (i.e. any finite plane with the homology property has odd order). Hence all the hypotheses of theorem 4.1 are satisfied, with S being the set of points on $\mathcal{l}$, G_{α} being G_A, and F_{α} being K_A. Thus by theorem 4.1 n is a power of some prime. Consequently a finite plane with the homology property has order p^m for some prime p.

<u>Lemma 5.3</u> Let π be a finite projective plane and let G be a collineation group of π fixing a line $\mathcal{l}$ of π. Then the following three conditions are equivalent:

(1) G is transitive on the affine lines of π (where $\mathcal{l}$ is considered to be the "line at infinity").

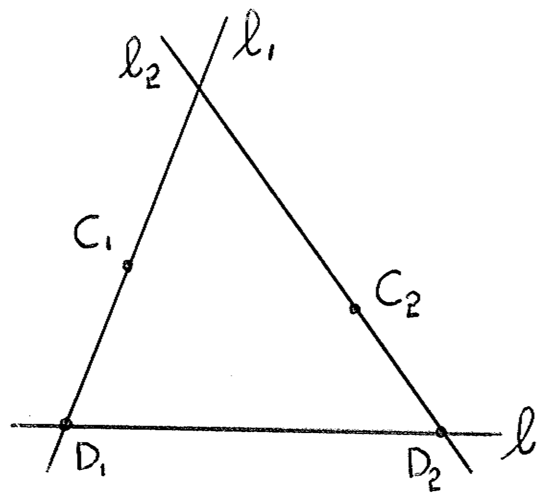
(2) G is transitive on the points of $\mathcal{l}$ and on the affine points of $\pi_{\mathcal{l}}$.

(3) G is transitive on affine flags of $\pi_{\mathcal{l}}$ (i.e. on flags (C,γ) with $C \notin \mathcal{l}$ and $\gamma \neq \mathcal{l}$).

Proof:

(1) $\Longrightarrow$ (2): Considered as a collineation group on the set $\mathcal{L}$ of lines of π, G partitions $\mathcal{L}$ into two disjoint orbits. By theorem 4.5, G will partition the points of π into two disjoint orbits. As G cannot map points of ℓ onto points not on ℓ (since G fixes ℓ), these two orbits must be the points of ℓ and the points of $\pi - \{\ell\}$. Hence (2) follows immediately.

(2) $\Longrightarrow$ (3): Let (C_1, ℓ_1) and (C_2, ℓ_2) be arbitrary affine flags of π. Let $\ell_1 \cap \ell = D_1$ and $\ell_2 \cap \ell = D_2$. By hypothesis the points of $\pi - \{\ell\}$ and the points of are orbits, under the action of G, of orders $(n+1)$ and n^2 respectively. But $(n+1)$ and n^2 are relatively prime, so by two applications of lemma 4.2 there exist



elements σ_1 and σ_2 in G such that $C_1^{\sigma_1} = C_1$, $D_1^{\sigma_1} = D_2$, and $D_2^{\sigma_2} = D_2$, $C_1^{\sigma_2} = C_2$. Thus $(C_1, \ell_1)^{\sigma_1\sigma_2} = (C_2, \ell_2)$; as (C_1, ℓ_1) and (C_2, ℓ_2) were arbitrary affine flags of π, G is transitive on such flags.

(3) $\Longrightarrow$ (1): This is trivially true.

Corollary: Let π be a finite projective plane of order n and let G be a collineation group of π fixing ℓ and transitive on the lines of $\pi - \{\ell\}$. Let $G_{C,\gamma}$ denote the stabilizer in G of the affine flag (C,γ), let G_C denote the stabilizer in G of C, and let G_γ denote the stabilizer in G of γ. Then:

(1) $|G_{C,\gamma}|n^2(n+1) = |G|$

(2) $|G_{C,\gamma}|n^2 = |G_A|$ where G_A is the stabilizer in G of an arbitrary point $A \varepsilon \ell$.

(3) $|G_\gamma| = (n+1)|G_{C,\gamma}|$

(4) $|G_C| = n|G_{C,\gamma}|$

(5) $|G_{A,C}| = |G_{C,\gamma}|$ where $G_{A,C}$ is the subgroup of G fixing both C and a point $A \varepsilon \ell$.

Proof:

(1) There are n^2 affine points in π_ℓ, and $(n+1)$ affine lines through each of these. As each incident point-line pair with elements drawn from these points and lines comprises an affine flag of π, there are $n^2(n+1)$ affine flags in π. As G is transitive on affine flags of π_ℓ by lemma 5.3, $|\mathrm{Orb}\ (C,\gamma)| = n^2(n+1)$. Thus $|G_{C,\gamma}|n^2(n+1) = |G|$ by lemma 4.1.

(2) As by lemma 5.3 G is transitive on the points of ℓ, it follows from lemma 4.1 that $|G_A|(n+1) = |G|$. Combining this with (1) immediately gives $|G_{C,\gamma}|n^2 = |G_A|$.

(3) By hypothesis G is transitive on the (n^2+n) affine lines of π, so by lemma 4.1 $|G_\gamma|(n^2+n) = |G|$. Combining this with (1) immediately gives $|G_\gamma| = n|G_{C,\gamma}|$.

(4) By lemma 5.3 G is transitive on the n^2 affine

points of π_ℓ . Thus by lemma 4.1, $|G_C|n^2 = |G|$. Combining this with (1) immediately gives $|G_C| = (n+1)|G_{C,\gamma}|$.

(5) It is evident that $G_{A,C} = G_{C,AC}$. As G is transitive on affine lines it follows from lemma 4.1 that $|G_{C,AC}| = |G_{C,\gamma}|$. Consequently $|G_{A,C}| = |G_{C,\gamma}|$.

Lemma 5.4 Let π be a finite projective plane and let G be a collineation group of π fixing a line ℓ of π. Then G is transitive on points of $\pi - \{\ell\}$ if and only if, for an arbitrary point $A \varepsilon \ell$, G_A is transitive on affine lines through A.

Proof: Let the action of G on the points of ℓ split these points into s orbits.

First assume that G is transitive on the points of $\pi - \{\ell\}$. Then there are (s+1) distinct orbits of points of π under the action of G. By theorem 4.5 there are (s+1) orbits of lines of π under the action of G. As ℓ is a fixed line, there are s orbits of affine lines of π under G. Let T_1 and T_2 be distinct orbits of points of ℓ under G, and let ℓ_1 and ℓ_2 be affine lines such that $\ell_1 \cap \ell \; \varepsilon T_1$ and $\ell_2 \cap \ell \; \varepsilon T_2$. Then if there exists $g \varepsilon G$ such that $\ell_1{}^g = \ell_2$, it would follow that $(\ell_1 \cap \ell)^g = \ell_2 \cap \ell$, contradicting the assumption that T_1 and T_2 are distinct orbits. Consequently the set of affine lines of π intersecting ℓ in the points of a given orbit of points of must comprise an orbit of lines of ℓ. Thus G is transitive on affine lines through $A\varepsilon\ell$, and consequently G_A is also transitive on these lines (for arbitrary $A\varepsilon\ell$).

Conversely, suppose that for arbitrary $A\varepsilon\ell$, G_A is transitive on affine lines through A. Let T be an orbit of points of ℓ and let $P_1,P_2\varepsilon T$. Then there exists $g\varepsilon G$ such that $P_1{}^g = P_2$. Hence if m_1 is an arbitrary affine line through P_1, $m_1{}^g$ is an affine line through P_2. But G_{P_i} is transitive on affine lines through $P_i (i = 1,2)$, and P_1 and P_2 were arbitrary in T, so it follows that the set of affine lines intersecting ℓ in points of the same orbit T comprise an orbit of the lines of π under G. There are s such orbits, plus a singleton orbit $\{\ell\}$, and hence a total of (s+1) orbits of lines under G. By theorem 4.5, there are (s+1) orbits of points of π under G, of which s are comprised entirely of points of ℓ; it follows that G is transitive on the affine points of π.

<u>Corollary</u> Let π be a finite projective plane and G a collineation group of π fixing the line ℓ and transitive on the lines of $\pi - \{\ell\}$. If A and B are arbitrary points of ℓ and m_1 and m_2 are two affine lines through B, then $|G_{A,B,m_1}| = |G_{A,B,m_2}|$.

<u>Proof</u>: By part (2) of the corollary to lemma 5.3, G_A is transitive on the affine points of π. Thus by lemma 5.4, $G_{A,B}$ is transitive on affine lines through

B. Thus as $|\mathrm{Orb}_{G_{A,B}} m_1| = |\mathrm{Orb}_{G_{A,B}} m_2|$, it follows from lemma 4.1 that $|G_{A,B,m_1}| = |G_{A,B,m_2}|$.

Theorem 5.1 Let π be a finite projective plane of order n and let G be a collineation group of π fixing a line ℓ and transitive on the affine lines of π (where ℓ is regarded as the "line at infinity"). Then if either

(1) n is even

or (2) n is a power of an odd prime,

π is a translation plane with respect to ℓ and G contains the group of elations with axis ℓ.

Proof: By lemma 5.3, G is transitive on the points of ℓ. Hence if C_1 and C_2 are distinct points of ℓ, the elation groups $G_{C_1,\ell}$ and $G_{C_2,\ell}$ will be conjugate in G by lemma 1.6. Hence, by lemma 4.10, in order to show that π is a translation plane with respect to ℓ it suffices to show that G contains a non-trivial elation with axis ℓ.

Let (C,m) be an affine flag of π, and suppose $|G_{C,m}| = k$. By the notation $p^u \| x$ (for a prime p and integers u and x) we shall mean that p^u divides x but p^{u+1} does not divide x. There are two cases:

Case (1): n is even. Suppose $2^u \| n$ and $2^v \| k$. Then $u > 0$. Let M be a Sylow 2-subgroup of G. By the corollary of lemma 5.3, $|G_{C,m}|(n+1)n^2 = |G|$ and hence M has order 2^{2u+v}. As M has a non-trivial centre, choose

$\alpha\varepsilon Z(M)$ of order 2. Let S denote the set of all points of $\pi - \{\ell\}$ fixed by α, and let $|S| = s$. By theorem 4.7, either α is a central collineation or α fixes elementwise a projective subplane μ of π of order $\sqrt{n}$. If α is a central collineation, since n is even α is an elation by theorem 1.2. If α has axis ℓ, we are finished; if α has axis m ($m \neq \ell$), then S consists of the points of m, excepting $m \cap \ell$, and so $s = n$. If α fixes the points of a subplane μ, then α fixes $(n+\sqrt{n}+1)$ points of π, of which $\sqrt{n}+1$ are on ℓ restricted to μ; hence $s = n$ in this case as well.

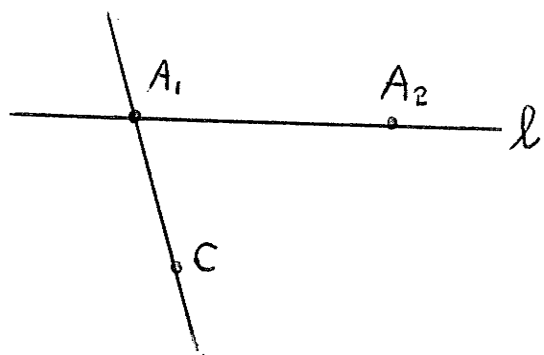
By lemma 4.3, the normalizer in M of the group generated by α permutes the members of S amongst themselves; as $\alpha\varepsilon Z(M)$, M is this normalizer, so M has an action on the points of S. Let T be an orbit of S under M and let P be an arbitrary element of T. Suppose $|T| = t$. Now M_P is a subgroup of G_P, and by the corollary of lemma 5.3, $|G_P| = (n+1)k$. Evidently $2^v \| (n+1)k$ (as $(n+1)$ is odd), i.e. $2^v \| \, |G_P|$, and hence $|M_P|$ divides 2^v. But by lemma 4.1, $|M_P| t = |M| = 2^{2u+v}$, so it follows that 2^{2u} divides t. But as T was an arbitrary orbit in S, it follows that

$$2^{2u} \text{ divides } \sum_{\text{all orbits } T} t,$$

i.e. 2^{2u} divides n. As $u > 0$, this contradicts the hypothesis that $2^u \| n$. Consequently $s = n$ is impossible, α is an elation with axis ℓ, and π is a translation plane with respect to ℓ.

<u>Case (2)</u> $n = p^s$ for an odd prime p and a positive integer s.

Let $|G_{C,m}| = k$ as before, let $p^t \| k$, and let A_1 be an arbitrary point of ℓ. By the corollary to lemma 5.3, $|G_{A_1}| = n^2 |G_{C,m}|$. Thus $p^{t+2s} \| |G_{A_1}|$, so if M is a Sylow p-subgroup of G_{A_1}, $|M| = p^{2s+t}$. Let C be an arbitrary point of $\pi - \{\ell\}$. Then by lemma 4.1, the orbit of C under M will be of order p^u for some integer u; hence $|M_C| p^u = p^{2s+t}$, i.e. $|M_C| = p^{2s+t-u}$. But M_C is a subgroup of $G_{A_1,C}$, and by the corollary to lemma 5.3,



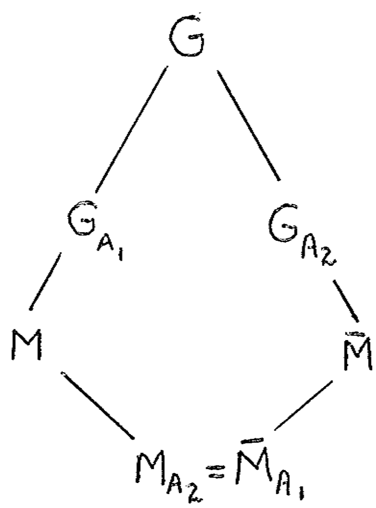
$$|G_{A_1,C}| = |G_{C,m}| = k.$$

Thus p^{2s+t-u} divides k. As $p^t \| k$, it follows that $p^{2s+t-u} \leq p^t$, and as $u \leq 2s$ from the definition of s and u, it follows that $u = 2s$. Hence $|\text{Orb } C| = p^u = p^{2s} = n^2$ and M is transitive on the affine points of π.

Now M has an action on the points of $\ell - \{A_1\}$, and hence partitions these points into orbits. Let $A_2 \varepsilon \ell$ and let A_2 be a member of an orbit of minimal length under M. Thus $B \varepsilon \ell - \{A_1\} \Longrightarrow |M_{A_2}| \geq |M_B|$. As M is transitive on affine points of π, by lemma 5.4 M_{A_2} is transitive on affine lines through A_2.

Evidently M_{A_2} is a p-subgroup of G_{A_2}; consequently there is a Sylow p-subgroup $\bar{M}$ of G_{A_2} such that $M_{A_2} \leq \bar{M}$. As M_{A_2} fixes A_1, it further follows that $M_{A_2} \leq (\bar{M})_{A_1}$.

By the corollary of lemma 5.3, it follows that $|G| = (n+1)|G_{A_1}|$, so M and $\bar{M}$ are Sylow p-subgroups of G.



(See the Hasse diagram giving the group relationships.) Hence there exists $g \varepsilon G$ such that $g^{-1}\bar{M} = M$. Let $A_1{}^g = B$. Then $B \varepsilon \ell$. If $A_1 = B$, then $g \varepsilon G_{A_1}$, $\bar{M} \varepsilon Syl_p(G_{A_1})$, and $(\bar{M})_{A_1} = \bar{M}$. Similarly $M_{A_2} = M$, and $M_{A_2} = (\bar{M})_{A_1} = M = \bar{M}$. If $A_1 \neq B$, it is seen that $g^{-1}(\bar{M})_{A_1} g \leq g^{-1}Mg = M$. But evidently $g^{-1}(\bar{M})_{A_1} g \leq M_B$, so by the maximality of M_{A_2}, $|M_{A_2}| \geq |g^{-1}(\bar{M})_{A_1} g| = |(\bar{M})_{A_1}|$. But $|M_{A_2}| \leq |(\bar{M})_{A_1}|$, and so $M_{A_2} = (\bar{M})_{A_1}$.

Just as M_{A_2} is transitive on affine lines through A_2, so also is $(\bar{M})_{A_1}$ transitive on affine lines through A_1. Hence M_{A_2} is transitive on affine lines through A_1.

Let $\{A_i | i = 2, \cdots, q\}$ be the set of points of $\ell - \{A_1\}$ fixed by M_{A_2}. Thus $M_{A_2} \leq M_{A_i}$, $i = 2, \cdots, q$; thus by the maximality of M_{A_2}, $M_{A_2} = M_{A_i}$, $i = 2$ to q, so as M_{A_i} is transitive on affine lines through A_i, $i = 2$ to q, and as M_{A_2} has been shown to be transitive on affine lines through A_1, it follows that M_{A_2} is transitive on the affine lines through A_i, $i = 1$ to q.

As p-groups have non-trivial centres, we can find $\alpha \varepsilon Z(M_{A_2})$ such that α is of order p. Then α fixes at least two points of π, namely A_1 and A_2; hence by theorem 4.5, α fixes at least two lines of π, one of which is ℓ. Let one of the other lines be denoted by m. Then either $\ell \cap m = A_j$ for some $j \varepsilon \{1, \cdots, q\}$, or $\ell \cap m \neq A_j$ for any $j \varepsilon \{1, \cdots, q\}$.

In the first case, let r be an arbitrary affine line through A_j. As M_{A_2} is transitive on lines through A_j, there exists $\varphi \varepsilon M_{A_2}$ such that $m^\varphi = r$. Thus $m^{\varphi\alpha} = r^\alpha$, and as $\alpha \varepsilon Z(M_{A_2})$, $r^\alpha = m^{\varphi\alpha} = m^\varphi$. Thus $r^\alpha = m^{\varphi\alpha} = r^{\alpha^2}$, i.e. $r = r\alpha$; i.e. α fixes every line through A_j. Thus α is a central collineation with centre A_j. To show that its axis is ℓ, it suffices to show that no point of $\pi - \{\ell\}$ is fixed by α. Suppose that $C \varepsilon \pi - \{\ell\}$ and suppose that $C^\alpha = C$. Then as α fixes A_s, $s \varepsilon \{1, \cdots, q\}$ and $s \neq j$, $(CA_s)^\alpha = CA_s$ and thus by the dual of lemma 1.3, $\alpha = 1$, contrary to hypothesis (note that as $q \geq 2$, an A_s can always be found). Hence α is a non-trivial elation with axis ℓ and we are finished.

The second case cannot arise; for suppose $\ell \cap m = D$ where $D \neq A_j$, $j = 1$ to q. Consider the orbit of m under M_{A_2}. As D is not fixed by M_{A_2}, there is a line $r \varepsilon (\mathrm{Orb}_{M_{A_2}} m)$ such that $r \cap m = E$ and $E \not\varepsilon \ell$. By the argument used in the previous paragraph, as α fixes m it also fixes r; hence $E^\alpha = (m \cap r)^\alpha = E$.

Hence in all possible cases π is a translation plane with respect to ℓ.

<u>Lemma 5.5</u> Let π be a finite projective plane of odd order n, and G a collineation group of π fixing ℓ, the "line at infinity", and transitive on the lines of π_ℓ. Let μ be a minimal 2-subplane of π with respect to G; i.e. let it contain no non-degenerate 2-subplane of π with respect to G. Let H be the subgroup of G consisting of all elements of G that map μ onto itself. Then, as H has an action on μ:

(1) For every affine flag of μ there exists an involutory homology in H fixing this flag.

(2) If A and B are distinct points of ℓ restricted to μ, and if $\bar{\ell}$ is an affine line of μ through B such that there exists an involutory homology in H fixing A,B, and $\bar{\ell}$, then if m is any other affine line of μ through B there exists an involutory homology in H fixing A,B, and m.

<u>Proof of (1)</u> Let K be a maximal (in that no 2-subgroup of G containing K has the property) 2-subgroup of G fixing μ, and only μ, elementwise. Let $(C,\bar{\ell})$ be an arbitrary affine flag of μ (and hence of π). Let $|G_{C,\bar{\ell}}| = k$. From the corollary of lemma 5.3, $|G| = k(n+1)n^2$. If u,v, and w are defined by $2^u \| n+1$, $2^v \| k$, and $|K| = 2^w$, then as n is odd, $u > o$ and $2^{u+v} \| |G|$. Evidently K is a subgroup of $G_{(C,\bar{\ell})}$, and so $w \leq v$. Thus as Sylow 2-subgroups of G have order 2^{u+v}, K is not a Sylow 2-subgroup of G. Hence there exists, by the theory

of groups of prime power order, a 2-subgroup $\bar{K}$ of G of order 2^{w+1} containing K. Then K is normal in $\bar{K}$. As K fixes μ and only μ elementwise, by lemma 4.3 $\bar{K}$ permutes the elements of μ amongst themselves. Thus $\bar{K}$ has an action on μ, and induces a collineation group of μ. By the maximality of K, $\bar{K}$ is not the identity on μ. Now $\bar{K}$ is generated by K and $\bar{k}$, where $\bar{k}\varepsilon\bar{K}-K$ and $\bar{k}$, considered as a collineation of μ, has order 2. The action of $\bar{K}$ restricted to μ is evidently isomorphic to $\frac{\bar{K}}{K}$, which is isomorphic to the group $\{1,\bar{k}\}$. Thus $\bar{K}$ acts on μ as a collineation group of order 2 generated by $\bar{k}$. Thus by theorem 4.7, $\bar{k}$ is either a central collineation of μ or else fixes a non-degenerate subplane of μ. The latter alternative is impossible by the minimality of μ; hence as π has odd order, by lemma 5.1 so has μ, and hence by theorem 1.2 $\bar{k}$ acts as an involutory homology of μ. As $\bar{k}\varepsilon G$, it fixes $\ell\cap\mu$ (where $\ell\cap\mu = \{P \mid P\varepsilon\ell,\ P\varepsilon\mu\}$); hence either ℓ is the axis of $\bar{k}$ or the centre of $\bar{k}$ is on ℓ. In either case it is evident that $\bar{k}$ fixes some affine flag, say (D,m), of μ. Thus $\bar{K}\leq G_{(D,m)}$ and as $|\bar{K}| = 2^{w+1}$, $(w+1)$ divides $|G_{(D,m)}| = k$. Hence as $2^v \| k$, $(w+1)\leq v$, i.e. $w<v$. Thus K is not a Sylow 2-subgroup of $G_{(C,\bar{\ell})}$. It follows that $G_{(C,\bar{\ell})}$ contains a 2-subgroup L of order 2^{w+1} containing K as a normal subgroup of index 2. By lemma 4.3, L permutes the elements of μ amongst themselves and so L is a subgroup of H. By the argument used

for $\bar{K}$, it follows that L contains an element which acts on μ as an involutory homology and fixes $(C, \bar{\ell})$. This element will be in H, and as $(C, \bar{\ell})$ was arbitrary, assertion (1) holds.

<u>Proof of (2)</u> The group K as defined above is not a Sylow 2-subgroup of $H_{A,B,\bar{\ell}}$; for let $\bar{H}$ be the subgroup of H that fixes μ elementwise. Then $\bar{H}$ is a normal subgroup of H, as is easily verified, and K is a subgroup of $\bar{H}$. By hypothesis there is an element of $H_{A,B,\bar{\ell}}$ that, considered as a collineation of μ, is of order 2; consequently the factor group $\frac{H_{A,B,\bar{\ell}}}{\bar{H}}$ has even order, and so K cannot be a Sylow 2-subgroup of $H_{A,B,\bar{\ell}}$. Consequently K is not a Sylow 2-subgroup of $G_{A,B,\bar{\ell}}$. By the corollary of lemma 5.4, $|G_{A,B,\bar{\ell}}| = |G_{A,B,m}|$. Thus by definition of K, K is a 2-subgroup of $G_{A,B,m}$ but not a Sylow 2-subgroup of $G_{A,B,m}$. Then by the argument used in case (1), there exists a 2-subgroup $\bar{K}$ of $G_{A,B,m}$ inducing a permutation on μ, possessing K as a normal subgroup of index 2, and possessing an involutory homology fixing A,B, and m. As $\bar{K}$ is a subgroup of H, H possesses such an involutory homology and assertion (2) holds.

<u>Lemma 5.6</u> Let μ be a finite projective plane and H a collineation group of μ fixing a line ℓ of μ and possessing the properties of H in lemma 5.5, i.e.

(1) For every affine flag of μ there exists an involutory homology in H fixing this flag.

(2) If A and B are distinct points of ℓ and $\bar{\ell}$ is an affine line of μ through B such that H contains an involutory homology of H fixing A, B, and $\bar{\ell}$, then for any other affine line m of μ through B there exists an involutory homology in H fixing A, B, and m. Then one of the following must hold:

(i) μ is a translation plane with respect to ℓ,

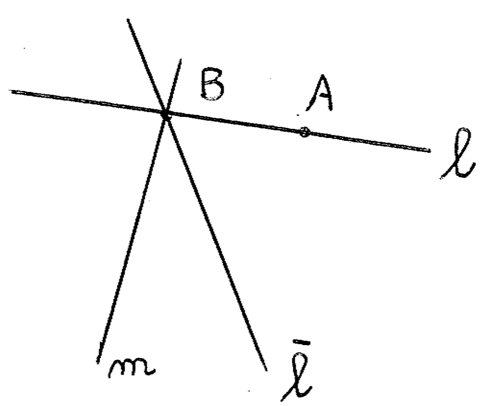
(ii) μ is the dual of a translation plane,

(iii) μ possesses the homology property.

<u>Proof</u>: There are several cases.

<u>Case I</u>: H contains no involutory homology with centre not on ℓ.

Then by condition (1) H contains an involutory homology α. Let α have centre A and axis $\bar{\ell}$; then $A \varepsilon \ell$, and let $\ell \cap \bar{\ell} = B \neq A$. Evidently, A, B, and $\bar{\ell}$ satisfy the prerequisites of condition (2), so for any affine line m through B, there exists an involutory homology $\beta \varepsilon H$ such that β fixes A, B, and m. Evidently β has either A or B as its centre; if the



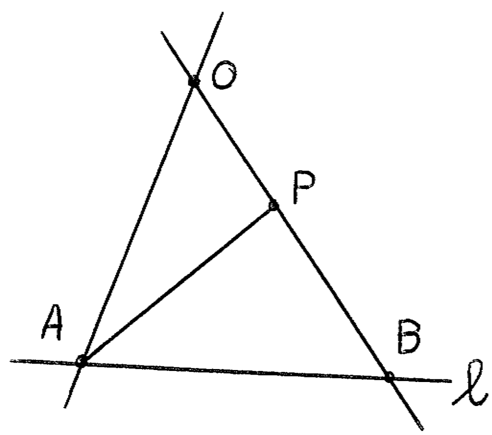
centre is B, then the axis $\bar{m}$ is an affine line through A and by lemma 1.10, $\alpha\beta$ is an involutory homology with centre $\bar{m} \cap \bar{\ell}$, which is not on ℓ; this contradicts the assumption. Hence β has centre A and, as it fixes m, axis m. Thus for every affine line m through B there is an involutory homology β with centre A and axis m. By the dual of theorem 4.4, part (1), μ is (A, ℓ)-transitive. There are now two possibilities.

If H does not fix A, then as H fixes ℓ, there exists $\varphi \varepsilon H$ such that $A^{\varphi} = \bar{A} \neq A$, $\bar{A} \varepsilon \ell$. Then by lemma 1.6 μ is both (A, ℓ)- and $(\bar{A}, \bar{\ell})$-transitive, and by lemma 1.7 μ is a translation plane with respect to ℓ.

If H fixes A, let (P,q) be an arbitrary affine flag of μ such that $C = \ell \cap q \neq A$. By condition (1) there exists an involutory homology $\gamma \varepsilon H$ such that γ fixes (P,q). Now γ also fixes A by hypothesis. If, for every affine line q of m not through A the corresponding involutory homology γ has centre A, by the dual of part (2) of theorem 4.4, μ is the dual of a translation plane with special point A. If there exists an affine line q, $A \notin q$, such that A is not the centre of the corresponding involutory homology γ, then γ has centre C and plays the same role as β did earlier in the argument; and by using the argument employed there, it is found that μ is a translation plane with respect to ℓ.

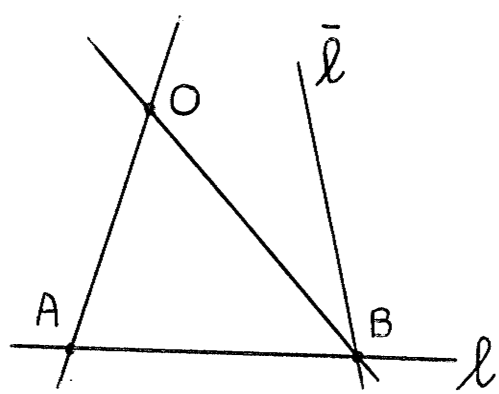
Case II: Only one affine point of μ is the centre of an involutory homology in H.

Let this point be O, and let α be the involutory homology with centre O. Then H fixes O, for if there exists $h \varepsilon H$ such that $O^h = \bar{O} \neq O$, then $\bar{O}$ is an affine point (as H fixes ℓ) and by lemma 1.6 is the centre of the involutory homology $h^{-1}\alpha h$, contrary to hypothesis. Let A and B be arbitrary distinct points of ℓ. Choose $P \varepsilon OB$, $P \neq B$, $P \neq O$. Then by condition (1), there is an involutory homology $\gamma \varepsilon H$ such that γ fixes the affine flag (P,AP). Thus γ fixes P, O, and thus also $OP \cap \ell = B$ and $AP \cap \ell = A$. Thus γ has centre A and axis OB. As A and B were arbitrary on ℓ, μ has the homology property (with respect to the point O and the line ℓ).



Case III: There exist at least two affine points of μ that are centres of involutory homologies in H.

Let O be one of these points, and let δ be an involutory homology with centre O. Let A and B be arbitrary points on ℓ, and let $\bar{\ell}$ be an arbitrary affine line through B. As δ fixes ℓ, OA, and OB it fixes A and B. Thus by condition (2)



there is an involutory homology in H that fixes A,B, and $\bar{\ell}$.

As H fixes ℓ, any homology in H with an affine centre must have axis ℓ; consequently as there are at least two distinct affine centres of homologies in H with axis ℓ, by theorem 4.3 there is a non-trivial elation with axis ℓ in H. There are now two subcases.

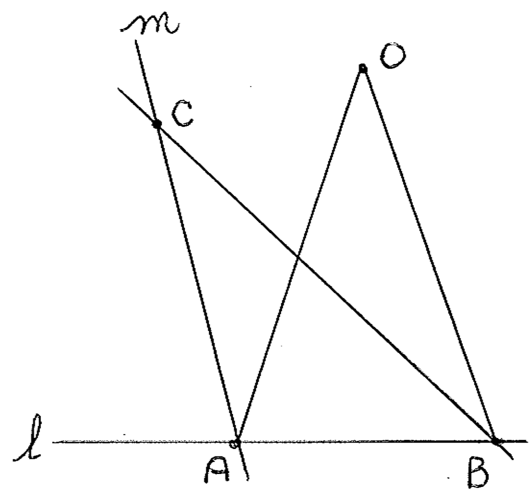
Subcase III(a): Some affine line m does not contain an affine point that is the centre of an involutory homology in H.

Let $\ell \cap m = A$ and let $B \in \ell - \{A\}$. As seen above, there is an involutory homology $\alpha \in H$ that fixes A,B, and m. Either α has centre A and axis through B, or centre B and axis m. In either case α has an action on the points of $\ell - \{A\}$, and fixes only B. There is such an α of order 2 for each $B \in \ell - \{A\}$, so as 2 is a prime, by lemma 4.4 the group generated by all such involutory homologies α is transitive on $\ell - \{A\}$. But this group is evidently a subgroup of $H_{A,m}$, so $H_{A,m}$ is transitive on the points of $\ell - \{A\}$.

If H does not fix A, then H is transitive on the points of ℓ, and as it has been seen that H contains a non-trivial elation with axis ℓ, it follows from lemma 4.10 that μ is a translation plane with respect to ℓ.

If H fixes A, let C be any affine point of m and B any point of $\ell - \{A\}$. By condition (1) there exists an involutory homology $\gamma \in H$ fixing the flag (C,CB). Also,

γ fixes A and $CB \cap \ell = B$, so by applying the argument above with γ playing the role of α (and noting that B is arbitrary in $\ell - \{A\}$), it follows that $H_{A,C}$ is transitive on the points of $\ell - \{A\}$.



For a given B and γ, as C is by hypothesis not the centre of γ, one of A and B is. If A is the centre, then γ is an (A,CB)-homology. If $\varphi \varepsilon H_{A,C}$, then by lemma 1.6 $\varphi^{-1}\gamma\varphi$ is an $(A^{\varphi}, C^{\varphi}B^{\varphi})$-homology, i.e. an (A, CB^{φ})-homology. As $H_{A,C}$ is transitive on $\ell - \{A\}$ it follows that for every line q through C (excepting CA) there is a non-trivial (C,q)-homology. Hence by the dual of part (1) of theorem 4.4, μ is (A,AC)-transitive.

If γ has centre B (and thus axis AC), then γ is a (B,m)-homology. Thus as $H_{A,C}$ is transitive on points of $\ell - \{A\}$ and as $H_{A,C}$ fixes m, by lemma 1.6 there is a non-trivial (P,m)-homology for every point $P \varepsilon \ell - \{A\}$. Hence by theorem 4.4, part (1), μ is (A,m)-transitive.

Thus in either case μ is (A,m)-transitive; hence as the involutory homology δ with centre $O \notin \ell$ fixes A, by lemma 1.6 μ is (A, m^{δ})-transitive, and $m^{\delta} \neq m$; hence by the dual of lemma 1.7, μ is the dual of a translation plane with respect to the point A.

<u>Subcase III(b)</u>: Every affine line of μ has on it an affine point of μ that is the centre of an involutory homology in H.

Then let A be an arbitrary point of ℓ and let m be an arbitrary affine line through A. Then there is an involutory homology $\alpha \varepsilon H$ whose centre is an affine point of m, and whose axis is ℓ. If S_A denotes the set of affine lines through A, then as α fixes A it permutes the elements of S_A amongst themselves and fixes only m. As there is such an α of order 2 for each $m \varepsilon S_A$, it follows by lemma 4.3 that the group generated by all such α, and hence H_A, is transitive on S_A. As A was arbitrary on ℓ, it follows by lemma 5.4 that H is transitive on the points of $\mu - \{\ell\}$. Hence by lemma 1.6, there is a non-trivial (C, ℓ)-homology for every $C \varepsilon \mu - \{\ell\}$, and thus by theorem 4.4, part (3), μ is a translation plane with respect to ℓ.

This completes the proof of lemma 5.6.

<u>Theorem 5.2</u> Let π be a finite projective plane of order n and let G be a collineation group of π fixing a line ℓ (the "line at infinity") and transitive on affine lines of π. Then π is a translation plane with respect to ℓ and G contains the group of elations with axis ℓ.

<u>Proof</u>: If n is even the result is immediate by theorem 5.1. If n is odd, let μ be a minimal 2-subplane

of π. Then by lemma 5.1 μ has odd order, and by lemmas 5.5 and 5.6 μ is either a translation plane with respect to ℓ, the dual of a translation plane, or possesses the homology property. If μ is a translation plane with respect to ℓ then by theorem 1.1 the group of all elations with axis ℓ has prime power order. Hence if $C \varepsilon \ell$, the group $G_{C,\ell}$ of elations with centre C and axis ℓ has prime power order, and by lemma 1.4 $|G_{C,\ell}| = n$. Hence n has prime power order. If μ is the dual of a translation plane, the dual argument gives the same result. If μ possesses the homology property, n is of prime power order by lemma 5.2. Hence if n is odd, μ has prime power order. By lemma 5.1 this implies that π has prime power order; hence by theorem 5.1 π is a translation plane with respect to ℓ and G contains the group of all elations of π with axis ℓ.

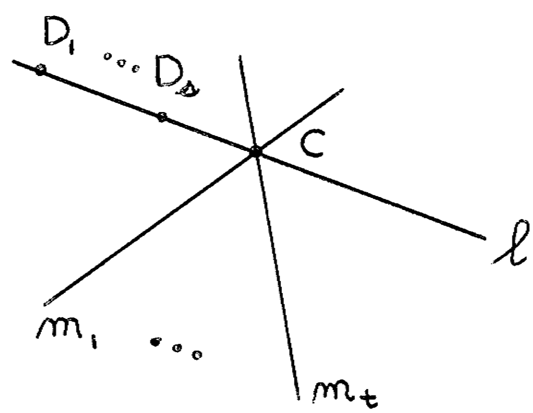
Corollary Let π be a finite projective plane with a collineation group G doubly transitive on the lines of π. Then π is Desarguesian and G contains the little projective group of π.

Proof: As G is doubly transitive on the lines of π, G_ℓ is transitive on the affine lines of the affine plane π_ℓ for any line $\ell \varepsilon \pi$. Thus π is a translation plane with respect to every line of π, and G contains all elations of π. Hence by the conclusions of Chapter III, π is Desarguesian and G contains the little projective group of π.

In the remaining theorems of this chapter we study the extent to which the number of central collineations in the collineation group of the projective plane determines the structure of the plane.

Theorem 5.3 (Wagner (11)). Let π be a finite projective plane possessing a point C and line ℓ, $C \in \ell$, such that C is the centre of an elation and ℓ is the axis of an elation. Then there exists a non-trivial (C, ℓ)-elation in π.

Proof: Suppose on the contrary that there is no non-trivial (C, ℓ)-elation. Let $\{D_i \mid i = 1 \text{ to } s\}$ be the set of all centres of non-trivial elations with axis ℓ and $\{m_j \mid j = 1 \text{ to } t\}$ be the set of all axes of elations with centre C. Then $D_i \neq C$, $i = 1$ to s, and $m_j \neq \ell$, $j = 1$ to t. By the hypotheses of the theorem $s \geq 1$ and $t \geq 1$.



Let α_i be a (D_i, ℓ)-elation and β_1 a (C, m_1)-elation. Then by lemma 1.6 $\alpha_i^{-1}\beta_1\alpha_i$ is a $(C, m_1^{\alpha_i})$-elation. Thus, as α_i does not fix m_1 as $m_1 \cap \ell \neq D_i$, $m_1^{\alpha_i} = m_u$ for some integer u such that $2 \leq u \leq t$. Further, if $i \neq j$ then $m_1^{\alpha_i} \neq m_1^{\alpha_j}$; for otherwise $m_1^{\alpha_i \alpha_j^{-1}} = m_1$, and by lemma 1.5 $\alpha_i \alpha_j^{-1}$ is a non-trivial elation with axis ℓ ; as $\alpha_i \alpha_j^{-1}$ fixes m_1, its centre is C, in contradiction to the assumption that no (C, ℓ)-elation exists. Thus $i \neq j \Rightarrow m_1^{\alpha_i} \neq m_1^{\alpha_j}$. Thus to each of the s points $\{D_i | i = 1 \text{ to } s\}$ corresponds a distinct line of the set $\{m_j | j = 2 \text{ to } t\}$. Hence $s < t$. However, the dual argument gives that $t < s$. This contradiction shows that our assumption is false and that a non-trivial (C, ℓ)-elation exists.

<u>Corollary</u>: If π is a finite projective plane and G is a collineation group of π such that every point is the centre of a non-trivial elation in G and every line is the axis of a non-trivial elation in G, then π is Desarguesian and G contains the little projective group.

<u>Proof</u>: By theorem 5.3, for every point C and line ℓ such that $C \varepsilon \ell$ there is a non-trivial (C, ℓ)-elation. Hence by lemma 4.11 the plane is Desarguesian.

The analogous case for homologies is now treated.

<u>Theorem 5.4</u> (Wagner (11)). Let π be a finite projective plane and let G be a collineation group of π with the following properties:

(1) Every point of π is the centre of some non-trivial homology in G.

(2) Every line of π is the axis of some non-trivial homology in G.

Then one of the following happens:

(a) G fixes a line ℓ of π. Then π is a translation plane with respect to ℓ and G contains the group of elations with axis ℓ.

(b) G fixes a point P of π. The conclusions are the duals of those of case (a).

(c) G fixes no element of π. Then π is Desarguesian and G contains the group generated by the elations of π as a subgroup.

<u>Proof</u>: <u>Case (a)</u>: Let every element of G fix the line ℓ. Then if C is any point not on ℓ, there is a homology φ in G with centre C, and φ fixes ℓ; hence φ has axis ℓ. Thus $C \notin \ell$ implies that G contains a (C, ℓ)-homology. By theorem 4.4, π is a translation plane with respect to ℓ and G contains the group of elations with axis ℓ as a subgroup. As G also contains homologies, this group is a proper subgroup.

By dualizing the argument of case (a), the results of case (b) are obtained.

<u>Case (c)</u>: In order to obtain the results of case (c) three assertions are established:

(1) Either some centre of π has more than one axis or some axis of π has more than one centre.

(2) If some line of π possesses more than one centre but no line possesses three non-collinear centres, then some point of π has three non-concurrent axes.

(3) If some line of π possesses three non-collinear centres then π is Desarguesian and G contains the little projective group of π.

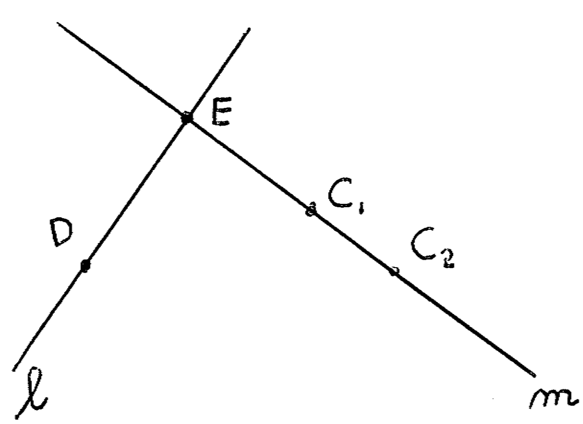
To prove (1), suppose on the contrary that it is false. Hence by the hypotheses every point of π has one and only one axis (of a homology with that point as centre), and every line of π has one and only one centre. Define a mapping φ of points of π onto lines of π and of lines of π onto points of π as follows: if P is a point, P^{φ} is the axis of the homology with centre P; if ℓ is a line, ℓ^{φ} is the centre of the homology with axis ℓ. By the uniqueness of centres and axes hypothesized above, φ is well-defined, and as it evidently is its own inverse, it is onto. As centres (axes) of lines (points) are unique, from the definition of φ it is evident that $\varphi^2 = 1$.

Then φ is a correlation (and in fact a polarity); to prove this it remains to show that $C \varepsilon \ell \Leftrightarrow \ell^{\varphi} \varepsilon C^{\varphi}$ for an arbitrary point C and line ℓ. As $\varphi^2 = 1$, it suffices to show that $C \varepsilon \ell \Rightarrow \ell^{\varphi} \varepsilon C^{\varphi}$; for then

$$\ell^{\varphi} \varepsilon C^{\varphi} \Rightarrow C^{\varphi^2} \varepsilon \ell^{\varphi^2} \Rightarrow C \varepsilon \ell .$$

Let $C \varepsilon \ell$ and let α be a (C, C^{φ})-homology. By lemma 1.6, since there exists an (ℓ^{φ}, ℓ)-homology, there also exists a $(\ell^{\varphi\alpha}, \ell^{\alpha})$-homology; thus by the hypotheses, any homology with axis ℓ^{α} has centre $\ell^{\varphi\alpha}$. But α is a homology with centre C, and $C\varepsilon\ell$; hence $\ell^{\alpha} = \ell$, and hence $\ell^{\varphi\alpha}$ is the centre of any homology with axis ℓ. But there exists an (ℓ^{φ}, ℓ)-homology; consequently $\ell^{\varphi\alpha} = \ell^{\varphi}$ and thus α fixes ℓ^{φ}. Thus by the definition of α, either $\ell^{\varphi} = C$ or $\ell^{\varphi}\varepsilon C^{\varphi}$. However, the first alternative is impossible since ℓ^{φ} is the centre of a homology with axis ℓ, and hence $\ell^{\varphi}\not\varepsilon\ell$, whereas $C\varepsilon\ell$. Hence $\ell^{\varphi}\varepsilon C^{\varphi}$, i.e. $C\varepsilon\ell \Longleftrightarrow \ell^{\varphi}\varepsilon C^{\varphi}$, and so φ is a correlation of order 2, and thus a polarity. However, by theorem 4.6, every polarity φ possesses an absolute point P, i.e. a point P such that $P\varepsilon P^{\varphi}$; however, this does not occur for the polarity defined above, as for any point Q, Q^{φ} is the axis of the homology with centre Q and hence $Q\not\varepsilon Q^{\varphi}$. This contradicts the hypothesis that (1) is false; thus (1) holds.

To prove assertion (2), let σ_1 and σ_2 be (C_1, ℓ)- and (C_2, ℓ)-homologies respectively $(C_1 \neq C_2)$; i.e. let ℓ be an axis with more than one centre. Let $C_1C_2 = m$, and let $m \cap \ell = E$. For an arbitrary point $D\varepsilon\ell - \{E\}$, let α be a homology with centre D (by hypothesis α exists). By lemma 1.6, there exist $(C_1^{\alpha}, \ell^{\alpha})$ and $(C_2^{\alpha}, \ell^{\alpha})$-homologies; as $D\varepsilon\ell$, $\ell^{\alpha} = \ell$ so these are (C_1^{α}, ℓ) and (C_2^{α}, ℓ)-homologies. As ℓ does



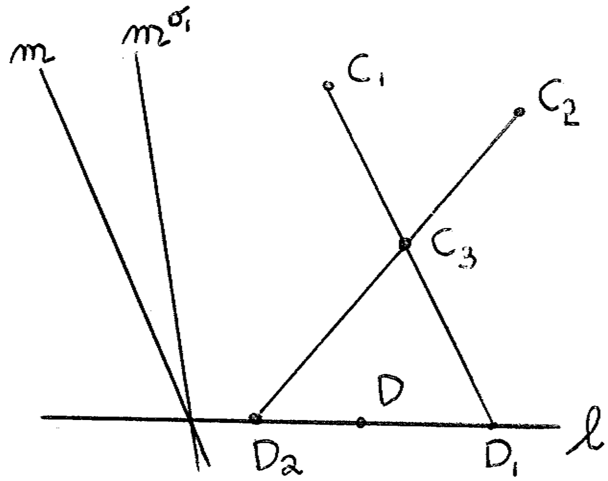
not have three non-concurrent centres, it follows that $C_1^{\alpha} \varepsilon m$ and $C_2^{\alpha} \varepsilon m$; hence $(C_1C_2)^{\alpha} = C_1^{\alpha}C_2^{\alpha} = C_1C_2$ and α fixes m. Hence as $D \not\varepsilon m$, the axis of α is m. However, D was arbitrary on $\ell - \{E\}$, so for any $D \varepsilon \ell - \{E\}$ there exists a non-trivial (D,m)-homology; consequently by theorem 4.4, π is (E,m)-transitive.

Evidently there are homologies with distinct centres on ℓ and with axis m, so by reversing the roles of ℓ and m in the above argument it follows that π is (E, ℓ)-transitive.

Hence by the dual of lemma 1.7, π is the dual of a translation plane with respect to E, and thence G is transitive on lines not through E; hence, by lemma 1.6, as there is one homology in G with centre E, for any line q of π not through E there is an (E,q)-homology in G. Hence E has three non-concurrent axes.

To prove assertion (3), suppose that the line has three non-collinear centres C_1, C_2, C_3. Define $C_2C_3 \cap \ell = D_2$ and $C_1C_3 \cap \ell = D_1$. Then $D_1 \neq D_2$. By theorem 4.3 the group generated by the (C, ℓ), (C_2, ℓ) and (C_3, ℓ)-homologies contain elations σ_1 and σ_2, each with axis ℓ, such that $C_1^{\sigma_1} = C_3$ and $C_2^{\sigma_2} = C_3$. Evidently σ_1 is a (D_1, ℓ)-elation and σ_2 is a (D_2, ℓ)-elation.

Let D be an arbitrary point of ℓ distinct from

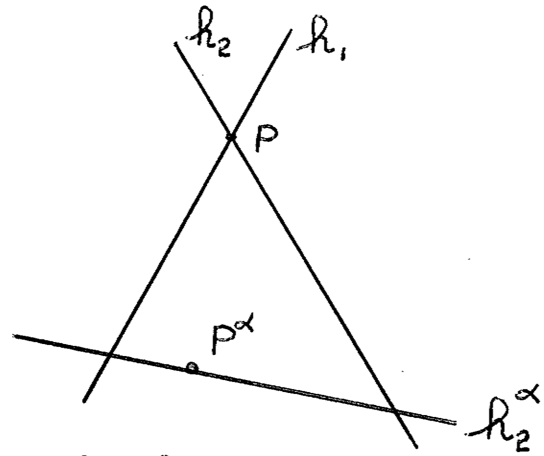


D_1 and D_2. It will be shown that there exists a non-trivial (D,ℓ)-elation. By hypothesis there exists a (D,m)-homology in G for some axis m. As $D\varepsilon\ell$, $m\neq\ell$ and hence not both D_1 and D_2 are on m. Without loss of generality it can be assumed that $D_1\not\varepsilon m$.

As there exists a (D,m)-homology, by lemma 1.6 there also exists a $(D^{\sigma_1},m^{\sigma_1})$-homology. As $D\varepsilon\ell$, $D^{\sigma_1} = D$ and as $D_1\not\varepsilon m$, $m^{\sigma_1}\neq m$. Thus there are homologies in G with centre D and distinct axes m and m^{σ_1}. Hence by the dual of theorem 4.3 there exists an elation φ with centre D such that $m^{\varphi} = m^{\sigma_1}$. As σ_1 is an elation with axis ℓ, $(m\cap m^{\sigma_1})\varepsilon\ell$, i.e. $(m\cap m^{\varphi})\varepsilon\ell$. Hence φ has axis ℓ and there exists a non-trivial (D,ℓ)-elation for any $D\varepsilon\ell$ (as D was arbitrary in $\ell-\{D_1\cup D_2\}$ and as there exist (D_1,ℓ)- and (D_2,ℓ)-elations).

The collineation group G has an action on the set $\mathcal{L}$ of lines of π. Every orbit of $\mathcal{L}$ under G contains three non-concurrent lines; for let $h_1,h_2\varepsilon\mathcal{L}$ and $h_1\varepsilon\text{Orb } h_2$, and define $h_1\cap h_2 = P$. As by the hypotheses of case (c) no point of π is fixed by G, there exists $\alpha\varepsilon G$ such that $P^{\alpha}\neq P$. Thus $h_1{}^{\alpha}\cap h_2{}^{\alpha}\neq P$. Hence if

$P \varepsilon h_1^{\alpha}$, $P \not\varepsilon h_2^{\alpha}$ and h_1, h_2, and h_2^{α} are three non-concurrent lines in the same orbit under G; if $P \varepsilon h_2^{\alpha}$ then h_1, h_2, and h_1^{α} are the desired non-concurrent lines.

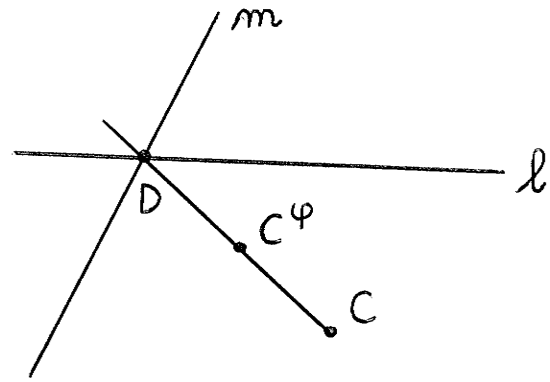


Hence in particular there exist lines ℓ_2 and ℓ_3, both in Orb ℓ, such that ℓ, ℓ_2, and ℓ_3 are non-concurrent. Thus there exists $\beta \varepsilon G$ such that $\ell^{\beta} = \ell_2$, and as there exists a non-trivial (D, ℓ)-elation for each $D \varepsilon \ell$, by lemma 1.6 there exists a non-trivial $(D^{\beta}, \ell^{\beta})$-elation for every $D \varepsilon \ell$. Thus for every point $E \varepsilon \ell_2$ there exists a non-trivial (E, ℓ_2)-elation; a similar result holds for ℓ_3.

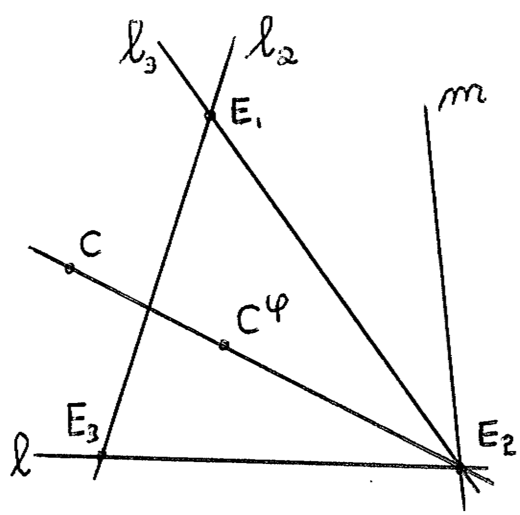
From this it can be deduced that every line of π is the axis of a non-trivial elation; obviously it suffices to show that any line m distinct from ℓ, ℓ_2, and ℓ_3 is such an axis. Such a line m is by hypothesis the axis of a homology σ with centre C; as ℓ, ℓ_2, and ℓ_3 are non-concurrent, and as every point on each of these three lines is the centre of an elation with that line as axis, it can be assumed without loss of generality that $C \not\varepsilon \ell$.

Let $m \cap \ell = D$; then there exists a (D, ℓ)-elation

φ. Then $m^\varphi = m$ and $C^\varphi \neq C$, so by lemma 1.6 there exists a (C^φ, m)-homology. Thus by theorem 4.3 there is an elation α with axis m such that $C^\alpha = C^\varphi$. But $\equiv D, C, C^\varphi$; hence α has centre D and there exists a non-trivial (D,m)-elation. As m was arbitrary, all lines of π are axes of non-trivial elations.



Now define $\ell \cap \ell_2 = E_3$, $\ell \cap \ell_3 = E_2$, $\ell_2 \cap \ell_3 = E_1$. Let m be an arbitrary line through E_2. Then by hypotheses G contains a (C,m)-homology. As $(\ell \cap \ell_3) \varepsilon m$, C is not on both ℓ and ℓ_3, so without loss of generality suppose $C \notin \ell$. As $E_2 \varepsilon \ell$ there exists an (E_2, ℓ)-elation σ; as $E_2 \varepsilon m$, $m^\sigma = m$ and as $C \notin \ell$, $C^\sigma \neq C$. Hence by lemma 1.6 G contains a (C^σ, m)-homology.



Thus by theorem 4.3 there exists an elation with centre $CC^\varphi \cap m = E_2$ and axis m. But m was an arbitrary line through E_2, and the argument used for E_2 can with equal validity be applied to E_1 and E_3; consequently there exists, for an arbitrary line m through E_i, a non-trivial

(E_i, m)-elation $(i = 1,2,3)$. Thus as E_1, E_2, and E_3 are non-collinear, they are points with the property dual to that obtained for lines ℓ, ℓ_2, ℓ_3. Hence by dualizing the argument of the previous paragraph it follows that all points of π are centres of non-trivial elations.

Combining this with the fact that all lines of π are axes of non-trivial elations, it follows at once from the corollary of theorem 5.3 that π is Desarguesian. Hence assertion (3) holds.

The conclusion of case (c) is proved as follows: by assertion (1), either a point of π has more than one axis or a line of π has more than one centre. If the latter holds, suppose that a line of π has three non-collinear centres. Then by assertion (3), π is Desarguesian. If no line of π has three non-collinear centres, by assertion (2) some point of π has three non-concurrent axes and by the dual of assertion (3), π is again Desarguesian.

If a line of π has more than one centre, then the above argument can be dualized to obtain again that π is Desarguesian. In all cases, by the corollary of theorem 5.3 G contains the little projective group.

To show that the situation treated in case (a) of theorem 5.4 can arise, let π be a projective plane and G the group of all collineations of π fixing a line of π. Co-ordinatize π by choosing ℓ to be the line at infinity , and pick any affine point to be the origin. Further suppose that the ternary ring R of π turns out to be a distributive quasifield ; i.e. addition in R is an abelian group, multiplication in R-$\{o\}$ is a loop, and both distributive laws hold. Then consider the mapping σ of points and lines of π defined as follows:

$$(x,y)^\sigma = (-x,-y) \qquad [m,b]^\sigma = [m,-b]$$
$$(m)^\sigma = (m) \qquad [x]^\sigma = [-x]$$
$$(\infty)^\sigma = (\infty) \qquad [\infty]^\sigma = [\infty].$$

Then σ is a one-to-one mapping (as inverses are unique). Using lemmas 2.2 and 2.3 and the fact that R is a distributive quasifield, it can easily be verified that σ preserves incidence and hence is a collineation. As σ fixes $\mathcal{l}$, $\sigma\varepsilon G$. But the origin O was arbitrary, and by theorems 2.3 and 2.4 the fact that R is a distributive quasifield is independent of what affine point has been chosen to be the origin; hence an $(O,\mathcal{l})$-homology σ can be defined as above for every affine point O. Thus every affine point is the centre of a non-trivial homology (assuming that R does not have characteristic 2).

Next consider the mapping τ defined by

$$(x,y)^\tau = (x,-y) \qquad [m,b]^\tau = [-m,-b]$$
$$(m)^\tau = (-m) \qquad [x]^\tau = [x]$$
$$(\infty)^\tau = (\infty) \qquad [\infty]^\tau = [\infty].$$

Then τ is a (V,OU)-homology (that τ preserves incidence is again easily verified by employing the algebraic laws at our disposal), so G possesses a homology with centre V.

Finally, consider the mapping α of π defined as follows:

$$(x,y)^\alpha = (-x,y) \qquad [m,b]^\alpha = [-m,b]$$
$$(m)^\alpha = (-m) \qquad [x]^\alpha = [-x]$$
$$(\infty)^\alpha = (\infty) \qquad [\infty]^\alpha = [\infty].$$

It is easily verified that α is a (U,OV)-homology. Since by theorem 2.4 π is (V,OV)-transitive with respect to G (as R is a distributive quasifield), for every point $P \varepsilon [\infty]$, $P \neq V$, there will be a non-trivial (V,OV)-elation mapping U onto P. Thus by lemma 1.6 there will be a non-trivial homology with centre P. Thus every point of π is the centre of some non-trivial homology. As in general a finite distributive quasifield is not a field, π will be non-Desarguesian and yet satisfy the hypotheses of theorem 5.4, case (a).

<u>Theorem 5.5</u> (Wagner (11)) Let π be a finite projective plane. Let G be a collineation group of π which, considered as a permutation group on the points of π, is transitive. Then if G contains a non-trivial central collineation σ, π is Desarguesian and G contains the little projective group of π.

<u>Proof</u>: It follows from the hypotheses and from theorem 4.5 that G, considered as a permutation group on the set of lines of π, is transitive on these lines. Let σ have centre C and axis ℓ. There are two cases.

<u>Case (1)</u>: If σ is an elation, let D be an arbitrary

point of π. As G is transitive on points, there exists $\varphi \varepsilon G$ such that $C^{\varphi} = D$. Thus by lemma 1.6, $\varphi^{-1}\sigma\varphi$ is a (D, ℓ^{φ})-elation and hence every point of π is the centre of an elation. As G is transitive on lines of π, the dual argument gives that every line of π is the axis of an elation. Thus by the corollary of theorem 5.3, π is Desarguesian and G contains the little projective group.

Case (2): If σ is a homology, an argument completely analogous to that used in case (1) gives that every point of π is the centre of a non-trivial homology in G and every line is the axis of some non-trivial homology in G. As G is transitive on points and lines it fixes no point nor line of π; hence case (c) of theorem 5.4 applies and π is Desarguesian with G containing the little projective group of π.

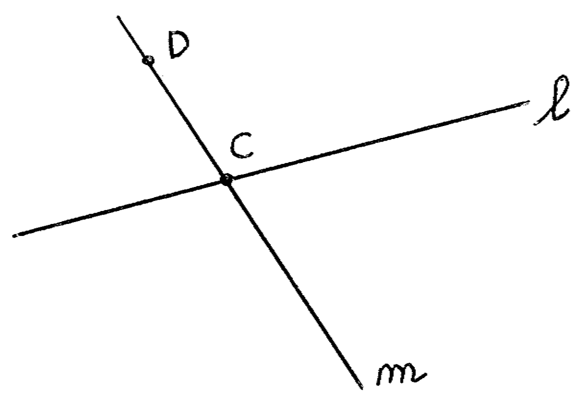
Corollary Let π be a finite projective plane of order n and let G be a collineation group of π transitive on the points of π. If n is not a square and if G has even order, then π is Desarguesian and G contains the little projective group of π as a subgroup.

Proof: As $|G|$ is even, it contains an element σ of order 2. As n is not a square, by theorem 4.7 σ is a central collineation. Thus the hypotheses of theorem 5.5 are satisfied and the conclusions follow immediately.

The following theorem (theorem 5.6) is an extension of the result of the corollary to theorem 5.3. The method is due to Piper.

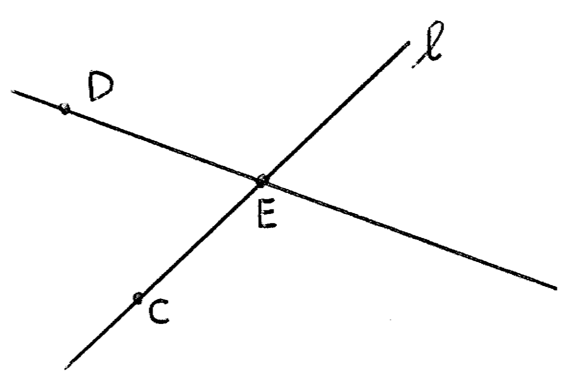
<u>Lemma 5.7</u> (Piper (10)) If every point of a finite projective plane π is the centre of an elation of π, then all elations of π have the same prime order.

<u>Proof</u>: Let C be an arbitrary point of π and let C be the centre of an elation with axis ℓ. Let D be an arbitrary point not on ℓ, and let D be the centre of an elation with axis m. There are two possibilities; either $C = \ell \cap m$ or $C \neq \ell \cap m$.



If $C = \ell \cap m$, then there is a (C,m)-elation in π by theorem 5.3. Thus as $C \neq D$, by the corollary of theorem 1.1, the (C,m) and (C,ℓ)-elations have the same prime order p. By theorem 1.1 the (C,m) and (D,m)-elations have the same prime order p; hence the (C,ℓ)-elation and the (D,m)-elation have the same prime order p.

If $\ell \cap m = E \neq C$, then by theorem 5.3, as E is the centre of an elation and ℓ is the axis of one, there is a non-trivial (E,ℓ)-elation.



By theorem 1.1 the (E,ℓ) and (C,ℓ)-elations have the same prime order p. By theorem 5.3 there is a non-trivial (E,m)-elation; by theorem 1.1 and its corollary this has the same prime order as the (E,ℓ)-elation and the (D,m)-elation. Hence again the (C,ℓ)-elation and the (D,m)-elation have the same prime order. Consequently the (C,ℓ)-elation and the (D,m)-elation have the same prime order.

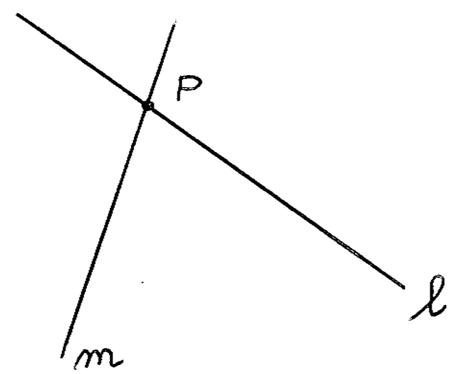
If $D \varepsilon \ell$, then if there is a (D,m)-elation, by theorem 5.3 there exists a (D,ℓ)-elation and repeated use of theorem 1.1 gives that the (C,ℓ) and (D,m)-elations have the same prime order. Hence as all possible cases have been discussed, the lemma is proved.

<u>Theorem 5.6</u> (Piper (10)) Let G be a collineation group of a finite projective plane of order n. If for every point of π there exists a non-trivial elation in G with that point as centre, then one of the following occurs:

(1) G fixes a point P of π; then π is the dual of a translation plane with G containing the group of all elations with centre P. Also G is transitive on flags of π whose lines do not pass through P.

(2) G does not fix a point of π. Then π is Desarguesian and G contains the little projective group as a subgroup.

Proof: Let ℓ be an arbitrary line of π with the property that for any point $P_i \varepsilon \ell$, there exists a non-trivial (P_i, m)-elation $\sigma_i \varepsilon G$, where $m \neq \ell$. As the hypotheses of lemma 5.3 are satisfied, $\{\sigma_i | i = 1, \cdots, (n+1)\}$ is a set of elations all of which have the same prime order. They generate a group which has an action on the points of ℓ and which satisfies the hypotheses of lemma 4.4. Hence this group is transitive on the points of ℓ, and consequently G is also.



As every point of π is the centre of some non-trivial elation, any line of π that is not an axis of some elation in G will satisfy the hypotheses on ℓ in the previous paragraph; as non-axes intersect it follows that G is transitive on the points on non-axes of π.

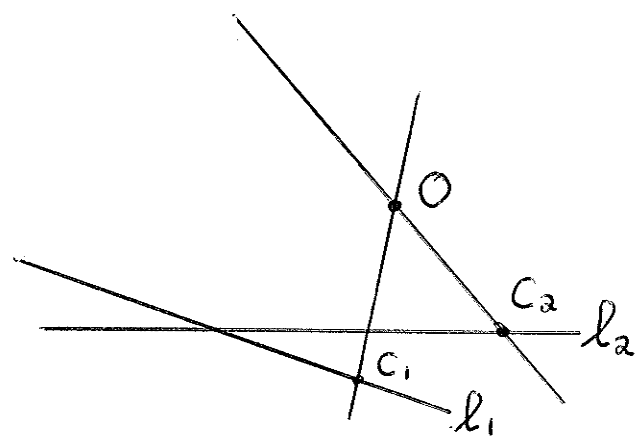
Now suppose that the group G is not transitive on the points of π. Then there exist distinct points P_1 and P_2 of π such that no element of G maps P_1 onto P_2. Thus G is not transitive on the points of $P_1P_2 = \ell$; consequently from the above discussion it follows that there must be a point $P \varepsilon \ell$ such that any elation with centre P has axis ℓ. Consequently all lines through P other than ℓ are non-axes, and so by the previous remarks, G is transitive on the points of all lines through P (except ℓ). It follows that G is transitive on the points of $\pi-\{\ell\}$.

Let Q be a point of $\ell-\{P\}$ and suppose that there exists $\sigma\epsilon G$ such that $Q^\sigma \notin \ell$. Then PQ^σ is a non-axis, and hence there exists $\varphi\epsilon G$ such that $(Q^\sigma)^\varphi = P$. Hence $\sigma\varphi$ maps Q into P; thus if all points of $\ell-\{P\}$ could be mapped into a point not on ℓ by some element of G, G would be transitive on the points of ℓ, in contradiction to the assumption. Thus there must exist a point $O\epsilon\ell$ such that $O^g\epsilon\ell$ for all $g\epsilon G$; i.e. Orb $O \subseteq \{\ell\}$.

Let D be any point of $\pi-\{\ell\}$. Then by hypothesis there exists a non-trivial elation $\alpha\epsilon G$ with centre D and axis m, say. Then $O^\alpha \epsilon OD$, but $O^\alpha\epsilon\ell$ from the preceding paragraph, and hence $O^\alpha = OD \cap \ell = O$. Thus α fixes O and hence m = OD. Consequently any point D of $\pi-\{\ell\}$ is the centre of a non-trivial (D,OD)-elation, and there exists no elation in G with centre $D\notin\ell$ and axis $\neq$ OD. Thus the point D and the line OD have precisely the properties ascribed to the point P and the line ℓ respectively. It then follows by the line of argument used above that G is transitive on the points of $\pi-\{OD\}$. As G is also transitive on the points of $\pi-\{\ell\}$, it is transitive on the points of $\pi-\{o\}$. By the dual of theorem 5.2, it immediately follows that π is the dual of a translation plane with respect to the point

O, and that G contains the group of all elations with centre O.

The group G, considered as a permutation group on the set $\mathcal{L}$ of lines of π, partitions $\mathcal{L}$ into two orbits, namely the set T_1 of lines through O and the set T_2 of lines not through O. (This follows at once from the fact that G fixes O and is transitive on the points of $\pi-\{O\}$.) Now $|T_1| = n+1$ and $|T_2| = n^2$, so $|T_1|$ and $|T_2|$ are relatively prime. Let (C_1, ℓ_1) and (C_2, ℓ_2) be flags with $O \notin \ell_1$, $O \notin \ell_2$. By lemma 4.2, there exists $g_1 \varepsilon G$ such that $(OC_1)^{g_1} = OC_1$ and $\ell_1^{g_1} = \ell_2$. Thus $C_1^{g} = (OC_1 \cap \ell_1)^{g} = OC_1 \cap \ell_2$. Similarly there exists $g_2 \varepsilon G$ such that $\ell_2^{g_2} = \ell_2$ and $(OC_1)^{g_2} = OC_2$. Then $\ell_1^{g_1 g_2} = \ell_2$ and $C_1^{g_1 g_2} = (OC_1 \cap \ell_2)^{g_2} = OC_2 \cap \ell_2 = C_2$. Hence $(C_1, \ell_1)^{g_1 g_2} = (C_2, \ell_2)$ and G is transitive on flags with axes not through O.



Thus if G is not transitive on the points of π, π is the dual of a translation plane. If G is transitive on the points of π, since it also contains elations it immediately follows by theorem 5.5 that π is Desarguesian and that G contains the little projective group of π.

<u>Lemma 5.8</u> Let π be a finite projective plane of order n and G a collineation group of π. Suppose that for any flag in π there exists an elation in G fixing that flag. Then all elations in G have the same prime order.

<u>Proof</u>: If a flag (P,ℓ) is fixed by an elation, then either P is the centre of the elation or ℓ is the axis of the elation. Hence if a line ℓ is not an axis of an elation in G, every point on ℓ is the centre of some elation of G. The dual situation of course also holds.

Suppose that G contains elations of order $p_1,\cdots,p_k$. As conjugation does not affect the order of a group element, by lemma 1.6 G will have an action on the set of centres of elations of given prime order p_i $(i = 1,\cdots,k)$, and dually on the corresponding sets of axes. Let ℓ be a non-axis (if there is no such ℓ the theorem immediately holds by the dual of lemma 5.7). Then every point on ℓ is a centre, so if there are n_i centres of elations of order p_i $(i = 1$ to $k)$, it follows that

$$\sum_{i=1}^{k} n_i = n+1. \qquad \ldots\ldots (1)$$

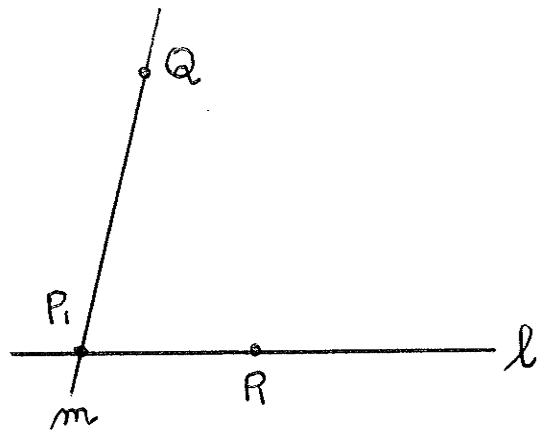
Without loss of generality suppose that $n_1 \leq n_j$, $j = 2$ to k. Let m be an axis through a centre P_1 of an elation of order p_1 $(P_1 \varepsilon \ell)$. (Henceforth such a centre will be referred to as a p_1-centre.) Let m have k_1 p_1-centres and k_2 non-centres. By theorem 1.1 all elations with axis m will have order p_1, so

$$k_1+k_2 = n+1. \qquad \ldots\ldots (2)$$

Let Q be a non-centre on m. (Such a $Q \notin \ell$ must exist; for otherwise every point of π is the centre of a non-trivial elation and the conclusion follows from lemma 5.7.) Then every line joining Q to a p_1-centre on ℓ is a p_1-axis; for every line through a non-centre is an axis, and by theorems 5.3 and 1.1, any elation with such an axis will be a p_1-elation. No other line through Q is a p_1-axis, for it meets ℓ at a point that is not a p_1-centre and hence cannot be a p_1-axis by the above argument. Hence there are n_1 p_1-axes through Q. Now each elation with axis m has an action on the (n_1-1) p_1-axes through Q (excluding m). Let $\bar{\ell}$ be a p_1-axis through Q ($\bar{\ell} \neq m$). If α_i and α_j are elations with axis m ($i \neq j$, $i,j \in \{1,\cdots,k\}$), then $\bar{\ell}^{\alpha_i} = \bar{\ell}^{\alpha_j} \Longrightarrow \bar{\ell}^{\alpha_i\alpha_j^{-1}} = \bar{\ell}$, i.e. the non-trivial elation $\alpha_i\alpha_j^{-1}$ with axis m fixes the line $\bar{\ell}$ through a non-centre of Q. This is a contradiction, and hence $\bar{\ell}^{\alpha_i} = \bar{\ell}^{\alpha_j} \Longrightarrow \alpha_i = \alpha_j$, so there are at least as many p_1-axes through Q (excluding $\bar{\ell}$ and m), and hence p_1-centres on ℓ, excluding two, as there are centres of elations with axis m. Thus

$$k_1 < n_1-1. \qquad \ldots\ldots (3)$$

Let R be the centre of a p_j elation, $R\varepsilon\ell$ and $j\geq 2$. By theorem 1.1 and the above remarks, the k_2 lines joining R to non-centres of m are p_j-axes. Let this set of p_j-axes be denoted $\{m_i \mid i = 1,\cdots,k_2\}$. By theorem 5.3 there exists an (R,m_i)-elation α_i $(i=1,\cdots,k_2)$. If



$i,j\varepsilon\{1,\cdots,k_2\}$, $i\neq j$, and $P_1^{\alpha_i} = P_1^{\alpha_j}$, then $P_1^{\alpha_i\alpha_j^{-1}} = P_1$, so as $\alpha_i\alpha_j^{-1}$ is an elation with centre R it must have axis ℓ, contradicting the hypothesis that ℓ is a non-axis. Thus $i\neq j \Rightarrow P_1^{\alpha_i}\neq P_1^{\alpha_j}$, so as each α_i has an action on p_1-centres, the number of p_1-centres on ℓ (excluding P_1) is at least as large as k_2;

i.e. $$n_1-1\geq k_2. \qquad \ldots\ldots (4)$$

Thus by equations (2), (3) and (4)

$$n+1 = k_1+k_2 < 2n_1-1. \qquad \ldots\ldots (5)$$

As $n_1\leq n_j$, $j = 1,\cdots,k$, it follows from (1) that

$$2n_1\leq \sum_{i=1}^{k} n_i = n+1.$$

This contradicts equation (5). Hence the assumption that there can exist elations with different prime orders is false and the lemma holds.

<u>Theorem 5.7</u> Let π be a finite projective plane of order n and let G be a collineation group of π. Suppose that for every flag of π there is an elation in G fixing that flag. Then one of the following must hold:

(i) G fixes a point of π. Then π is the dual of a translation plane and G contains the dual of the translation group.

(ii) G fixes a line of π. Then π is a translation plane and G contains the translation group.

(iii) G fixes neither a point nor a line of π. Then π is Desarguesian. If $n \neq 4$, G contains the group of all elations of π.

<u>Proof</u>: As remarked in lemma 5.8, under the hypotheses of the theorem any point on a line that is not an axis of an elation in G is the centre of some elation in G. There are now three cases.

<u>Case I</u>: G fixes a point of π.

Let the point be O. Hence all axes of elations in G pass through O. Let P be an arbitrary point of $\pi-\{O\}$, and let ℓ be any line through P (except OP). Then G possesses an elation fixing the flag (P,ℓ). As ℓ is not the axis, P must be the centre. As all axes pass through O, OP is the axis. Hence any point $P\varepsilon\pi-\{O\}$ is the centre of a (P,OP)-elation. Thus for any line m through O and any point $P\varepsilon m-\{O\}$, there is a non-trivial (P,m)-elation; by lemma 1.11 there also exists an (O,m)-elation. Hence every point of π is the centre of a non-trivial elation. Hence by theorem 5.6, case (1), π is the dual of a translation plane, and G contains the dual of the translation group.

Case II: G fixes a line of π. The dual of the argument of case I gives the duals of its conclusions.

Case III: G fixes neither a point nor a line of π.

If all points of π are centres of non-trivial elations of G, or if all lines of π are axes of non-trivial elations of G, then by theorem 5.6 or its dual π is Desarguesian and G contains the group of all elations of π. Hence assume that there exist both a point of π that is not the centre of an elation in G and a line of π that is not the axis of an elation in G.

Now G is transitive on the points of non-axes; for if ℓ is a non-axis, all points of ℓ are centres of elations with axis $\neq \ell$. By lemma 5.8 all such elations are of the same prime order p. Now the subgroup of G fixing ℓ (denoted G_ℓ) has an action on the points of ℓ, and $P \varepsilon \ell \Rightarrow$ there exists $\sigma \varepsilon G_\ell$ (σ of order p) such that $P^\sigma = P$ and σ fixes no other point of ℓ. Hence by lemma 4.4 G_ℓ, and hence G, is transitive on points of ℓ. As non-axes intersect, G is transitive on all points of π that lie on some non-axis. Dually G is transitive on all lines of π that pass through some non-centre.

Secondly, every point P of π has at least two axes through it. This is obviously true if P is a non-centre, as all lines through non-centres are axes; hence suppose P is a centre with precisely one axis through it. Then by the previous paragraph G maps P onto any point of $\pi - \{\ell\}$. If, for every $Q \varepsilon \ell$, there exists $\alpha \varepsilon G$ such that $Q^{\alpha} \not\varepsilon \ell$, it immediately follows that G is transitive on the points of π, which by lemma 1.6 contradicts the fact that both centres and non-centres of elations of G exist in π. Thus there exists $Q \varepsilon \ell$ such that $Q^{\alpha} \varepsilon \ell$ for all $\alpha \varepsilon G$. But if there exist two such points Q_1 and Q_2 on ℓ, then $\ell^{g} = (Q_1 Q_2)^{g} = \ell$ for all $g \varepsilon G$ and G fixes ℓ, contrary to the hypotheses of case III. If there exists only one such $Q \varepsilon \ell$, it is evident that Q is fixed by G, again in contradiction to the hypotheses of case III. Thus every point of π has at least two axes through it. Dually, every line of π has at least two centres on it.

Thirdly, G is transitive on centres of π and on axes of π; for let P and Q be distinct centres. If the line PQ is a non-axis then previously used arguments show that G is transitive on the points of PQ. If however the line $PQ = \ell$ is an axis, one may argue as follows; by the preceding paragraph there is an axis m through P, $m \neq \ell$, and by theorem 5.3 there is thus a (P,m)-elation $\varphi \varepsilon G$. Such a φ can be found for every centre $P \varepsilon \ell$, and by lemma 5.8 all such elations φ are of the same prime order. The group H that they generate has an action on the centres of ℓ (as centres map into centres under collineations, and as H fixes ℓ), so as the hypotheses of lemma 4.4 have been verified, H, and hence G, is transitive on the centres of ℓ. Thus in any case there is a $\varphi \varepsilon G$ such that $P^{\varphi} = Q$, and thus G is transitive on centres of π. Dually G is transitive on axes of π.

Fourthly, G is transitive on non-centres of π and on non-axes of π; for let ℓ be an axis and P a centre on ℓ. Then as seen earlier, there is an axis m through P, $m \neq \ell$, and by theorem 5.3 a (P,m)-elation α. Let A be the group generated by α; then A has prime order p, and the centres on ℓ (excluding P) are permuted amongst themselves by A. Thus the non-centres on are partitioned into disjoint orbits each of length p by the action of A. Hence there are kp non-centres on ℓ for some integer k, and as G is transitive on axes, kp non-centres on every axis of π. Let Q be an arbitrary non-centre of π; then every line through Q is an axis, and every non-centre of π is on one of these (n+1) lines. Hence the total number N of non-centres of π is

$$N = (n+1)(kp-1)+1 = (n+1)kp-n. \qquad \ldots\ldots (*)$$

Assume that there exists more than one orbit of non-centres in π under the action of G. Let Q and R lie in distinct orbits of non-centres, and let S_Q be the number of points in Orb Q that are also on QR. As every line through R is an axis and as G is transitive on axes, by lemma 1.6 the number of points in Orb Q of any line through R is S_Q. Thus as $R \notin$ Orb Q,

$$|\text{Orb } Q| = (n+1)S_Q.$$

As Q was arbitrary, all orbits of non-centres are of order divisible by (n+1); i.e. $N = r(n+1)$ for some integer r. Thus from equation (*),

$$r(n+1) = (n+1)kp-n.$$

The left-hand side is divisible by (n+1) but the right-hand side is not. This contradiction implies that all non-centres are in the same orbit under G, and so G is transitive on non-centres of π. Dually G is transitive on non-axes of π.

Hence G splits the points of π into two orbits, the centres and the non-centres; dually it splits the lines into two orbits, the axes and the non-axes. Thus each axis has the same number of centres, and each centre has the same number of axes.

If there are kp non-centres on an axis, then there are n/kp non-axes through a centre; for let C be a centre and let t be the number of axes through it. On each such axis there are kp non-centres, and this accounts for all the non-centres of π; hence π has tkp non-centres. From equation ($*$), it follows that

$$tkp = (n+1)kp-n.$$

Thus $$n+1-t = n/kp.$$

As the number of non-axes through a centre is $(n+1)-t$, it is evident that there are n/kp non-axes through a centre.

Now let ℓ be an arbitrary axis and P an arbitrary centre on ℓ. As G is transitive on centres, the group $G_{P,\ell}$ of elations with centre P and axis ℓ has the same prime power order p^α for every $P\varepsilon\ell$ (by theorem 1.1, as there is more than one centre on an axis). Let r be the number of axes through a centre and $\bar{r}$ the number of centres on an axis. Then as seen before, an elation with centre P and axis $\neq \ell$ partitions the centres of $\ell-\{P\}$ into orbits each of length p. Hence

$$\bar{r} = 1+\bar{u}p$$

for some integer $\bar{u}$. Dually $r = 1+up$ for some integer u. Without loss of generality assume that $\bar{r} \geq r$. Hence $\bar{u} \geq u$. Now let H_ℓ denote the group of all elations with axis ℓ, and $H_{P,\ell}$ the group of all elations with centre P and axis ℓ. Then $H_\ell = \bigcup_{P\varepsilon\ell} H_{P,\ell}$, and distinct groups $H_{P_1,\ell}$ and $H_{P_2,\ell}$ have only the identity in common; hence $$|H_\ell| = (1+\bar{u}p)(p^\alpha-1)+1.$$

By theorem 1.1, H_ℓ is a p-group of order p^β, say; hence

$$p^\beta = (\bar{u}p+1)(p^\alpha-1)+1. \qquad \ldots\ldots (1)$$

Let m be an axis through P ($m \neq \ell$). Then as H_ℓ has an action on the axes through P (excepting ℓ) and as the stabilizer of m is $H_{P,\ell}$, by lemma 4.1,

$$|\mathrm{Orb}_{H_\ell} m||H_{P,\ell}| = |H_\ell| . \qquad \ldots\ldots (2)$$

Evidently H_ℓ splits the axes through P (distinct from ℓ) into s orbits of equal length, so equation (2) becomes

$$\frac{up}{s}(p^\alpha) = (\bar{u}p+1)(p^\alpha-1)+1$$

i.e. $$\frac{up^{\alpha+1}}{s} = \bar{u}p(p^\alpha-1)+p^\alpha = p^\beta. \qquad \ldots\ldots (3)$$

As $\bar{u} \geq u$ by assumption, it follows that

$$\frac{up^{\alpha+1}}{s} \geq up(p^\alpha-1)+p^\alpha,$$

$$up^{\alpha+1} \geq sup^{\alpha+1}-sup+sp^\alpha,$$

$$up(p^\alpha+s) \geq sp^\alpha(up+1).$$

Thus $$p^\alpha+s \geq sp^\alpha$$

and so $s = 1$ since $s \geq 1$.

Equation (3) becomes

$$u = p^{\beta-\alpha-1}. \qquad \ldots\ldots (4)$$

Let H_P be the group of all elations with centre P. Then by the dual of theorem 1.1, $|H_P| = P^\gamma$. By the dual of the above argument, the analogue of equation (2) is obtained, namely

$$p^\gamma = (up+1)(p^\alpha-1)+1. \qquad \ldots\ldots (5)$$

As $\bar{u} \geq u$, it follows by comparison with equation (1) that $\gamma \leq \beta$. Combining equations (4) and (5) gives

$$p^\gamma = (p^{\beta-\alpha}+1)(p^\alpha-1)+1,$$

i.e. $$p^{\beta}+p^{\alpha}-p^{\beta-\alpha} = p^{\gamma} \qquad \ldots\ldots (6)$$

If $\beta < 2\alpha$, dividing equation (6) by $p^{\beta-\alpha}$ gives

$$p^{\alpha}+p^{2\alpha-\beta}-1 = p^{\gamma+\alpha-\beta}$$

and as $\gamma+2 > 2\alpha > \beta$, p divides the right-hand side but not the left-hand side, which is impossible.

If $\beta > 2\alpha$, dividing equation (6) by p^{α} gives

$$p^{\beta-\alpha}+1-p^{\beta-2\alpha} = p^{\gamma-\alpha}$$

and as $\gamma > \alpha$, p divides the right-hand side but not the left-hand side, which is again impossible. Hence $\beta = 2\alpha$.

Now equation (2) applies in general whether m is an axis or not; hence

$$\left|\text{Orb}_{H_{\ell}}\, m\right| p^{\alpha} = p^{2\alpha},$$

and so $$\left|\text{Orb}_{H_{\ell}}\, m\right| = p^{\alpha}.$$

Hence the n lines through P (excluding ℓ) can be partitioned into v orbits of length p^{α}; consequently $vp^{\alpha} = n$ for some integer v. As G is transitive on axes and non-axes and as there exist both axes and non-axes amongst the n lines through P (excepting ℓ), $v \neq 1$ as otherwise H_{ℓ} would map axes into non-axes.

Assuming as before that there are kp non-centres on an axis, and thus n/kp non-axes through a centre, it follows that $\bar{r} = n+1-kp$. The assumption that $\bar{r} \geq r$ is equivalent to the assumption that $kp \leq \sqrt{n}$. Then equation (1) can be rewritten as

$$p^{\beta} = (n+1-kp)(p^{\alpha}-1)+1.$$

Substituting $vp^{\alpha} = n$ and $p^{\beta} = p^{2\alpha}$, this becomes

$$p^{2\alpha} = (vp^{\alpha}+1-kp)(p^{\alpha}-1)+1$$
$$= vp^{2\alpha}-vp^{\alpha}+p^{\alpha}-kp^{\alpha+1}+kp.$$

But $\quad kp \leq \sqrt{n} = \sqrt{a}p^{\frac{\alpha}{2}}$ and so

$$p^{2\alpha} \geq vp^{2\alpha}-vp^{\alpha}+p^{\alpha}-\sqrt{a}p^{\frac{\alpha}{2}}(p^{\alpha}-1)$$

i.e. $\quad vp^{\alpha}(p^{\alpha}-1)-p^{\alpha}(p^{\alpha}-1)-\sqrt{a}p^{\frac{\alpha}{2}}(p^{\alpha}-1) \leq 0.$

As $p^{\alpha}-1 > 0$, this implies that

$$vp^{\alpha}-p^{\alpha}-\sqrt{a}p^{\frac{\alpha}{2}} \leq 0.$$

Let $X^2 = vp^{\alpha}$, $X > 0$. Then

$$X^2-\frac{X^2}{v}-X \leq 0$$

i.e. $\quad X-\frac{X}{v}-1 \quad 0,$

i.e. $\quad X \leq \frac{v}{v-1}$.

If $v = 2$, then $X \leq 2$ and $p^{\alpha} \leq 2$, i.e. $p = 2$ and $\alpha = 1$, and thus $n = vp^{\alpha} = 4$, and planes of order 4 are Desarguesian. If $v \geq 3$, then $X \leq \frac{3}{2}$, but from the definition of X, $X \geq \sqrt{3}p^{\frac{\alpha}{2}} > \sqrt{3} > \frac{3}{2}$, and there is a contradiction. Hence unless $n = 4$, the assumption that π possesses both non-centres and non-axes is false, and by theorem 5.4 or its dual, π is Desarguesian and G contains the little projective group as a subgroup.

This completes the proof of the theorem.

The case in which $n = 4$ will now be considered briefly, and the results of Piper (10) will be summarized. There is but one projective plane π_4 of order 4 and it is Desarguesian. There are two collineation groups of π_4 such that every flag of π_4 is fixed by an elation in the group; one is isomorphic to A_4 and the other to S_6. There are six points of π_4 that are not centres of elations of the group isomorphic to A_4, and no three of these are collinear.

BIBLIOGRAPHY

(1) Andre, J.: Uber Perspektivitäten in Endlichen Projektiven Ebenen. Arch. Math. 6, 29-32 (1954).

(2) Baer, R.: Polarities in Finite Projective Planes. Bull. Amer. Math. Soc. 52, 77-93 (1946).

(3) ___: Projectivities with Fixed Points on Every Line of the Plane. Bull. Amer. Math. Soc. 52, 273-286 (1946).

(4) Gleason, A.M.: Finite Fano Planes. Amer. J. Math. 78, 797-807 (1956).

(5) Hall, M.: The Theory of Groups. New York, 1959.

(6) Ostrom, T.G.: Double Transitivity in Finite Projective Planes. Canad. J. Math. 8, 563-567 (1956).

(7) ___, and Wagner, A.: On Projective and Affine Planes with Transitive Collineation Groups. Math. Z. 71, 186-199 (1959).

(8) Pickert, G.: Lectures on Projective Planes (mimeographed notes). Saskatoon, 1963.

(9) ___: Projektive Ebenen. Heidelberg, 1955.

(10) Piper, F.C.: Elations of Finite Projective Planes. Math. Z. 82, 247-258 (1963).

(11) Wagner, A.: On Perspectivities of Finite Projective Planes. Math. Z. 71, 113-123 (1959).

(12) ___: A Theorem on Doubly Transitive Permutation Groups. Math. Z. 85, 451-453 (1964).

(13) ___: On Finite Affine Line Transitive Planes. Math. Z. 87, 1-11 (1965).

(14) Wielandt, H.: Permutation Groups. (Lectures at the University of Tubingen, 1954-55).