



中央研究院
資訊科學研究所

Institute of Information Science, Academia Sinica • Taipei, Taiwan, ROC

TR-IIS-25-001

Projective Space as a Set with a Group of Permutations: Revised Version

Kelly McKennon



May 22, 2025

||

Technical Report No. TR-IIS-25-001

<https://www.iis.sinica.edu.tw/zh/page/Library/TechReport/2025.html>

Introduction

By the 1860's, the work of Èvariste Galois, and in particular the idea of a permutation group, had begun to be known to mathematicians in Germany. The young Felix Klein recognized how this idea could be used to organize and describe the various geometries which were being studied at the time, and presented his thoughts as his inaugural address at the University of Erlangen in 1872. So began the famous "Erlanger Programm" which was to have long lasting influence on the development of mathematics, and not just in the field of geometry.

Set theory had not yet been developed as we know it today. Klein called the domains on which the permutations acted "Mannigfaltigkeiten", or manifolds. He apparently used the word to represent the general conception of a set exhibiting some sort of geometry. The permutation group represented the ways the manifold could be transformed without changing the intrinsic geometric properties of the objects being transformed. In the language of contemporary mathematics his program could be described as follows:

- (1) Begin with a set X exhibiting a certain intrinsic property or properties;
- (2) Take a group of permutations of X and select out the subgroup \mathcal{P} consisting precisely of those elements of \mathcal{P} which preserve the property or properties described in (1);
- (3) Find other properties of X which are preserved by the elements of \mathcal{P} .

Thus there is a symbiotic relationship between the set X which represents the manifestation of the geometry and the family \mathcal{P} , which represents the various ways X can be observed without causing it to lose its defining qualities. Regarding it from this point of view though, something extraneous must be introduced in (1): the "intrinsic properties"; and perhaps also in (2): the larger group from which the elements of \mathcal{P} are selected.

Many of the geometries which were being investigated *circa* 1872 were related to projective geometry, and for the permutation group \mathcal{P} Klein took the group of all projective transformations of projective space.

In the present treatment of projective space we show how projective space can be defined using the spirit of the Erlanger Programm, but entirely within the context of a set paired with a group of permutations, there being no properties of the set or the group introduced *a priori*. These are replaced by three postulates imposed on the relationship between the set and the group.

The principle notion of a projective space is that of alignment: that one point x may somehow be "aligned" with two other points a and b . If a permutation which is to preserve alignment leaves the set $\{a,b\}$ invariant, then it will leave the set M of points aligned with a and b invariant. In particular, if a permutation interchanges a and b , it will do this thing. It is not obvious, but it is a fact, that a projective transformation ϕ which interchanges two points a and b acts in a peculiar manner on M : for any x aligned with a and b , there always exists another point y in M distinct from x such that $\{x,y\} = \{\phi(x),\phi(y)\}$.

This motivates us to define alignment as follows: x is aligned with a and b if, whenever ϕ in \mathcal{P} interchanges a and b , then there exists y distinct from x such that $\{x,y\} = \{\phi(x),\phi(y)\}$.

The first postulate placed on X and \mathcal{P} is that to each distinct a and b is that there exists at least one other point aligned with them.

Once "alignment" is made clear, one can move on to the definition of what is called here a "fundamental set" F . Fundamental sets are sets on which

- (A) a choice of an element of can be freely made
and
 - (B) the values of an element of \mathcal{P} on the fundamental set determines its values elsewhere as well.
- The last two postulates are to ensure that (A) and (B) hold.

The method we employ here to define a projective space may be described as follows: beginning with an arbitrary set X and a group \mathcal{P} of permutations of X , we

- (1) define certain properties of X in terms of the actions of elements of \mathcal{P} on X ;
- (2) impose postulates on \mathcal{P} so that these properties hold;
- (3) show that there exist examples of pairs X and \mathcal{P} such that that the postulates of (2) are satisfied;
- (4) work out the implications of such postulates for X and \mathcal{P} .

This is still a work in progress. We intend in later installments to show how duality theory fits into this framework, how it works in the special case of real projective space and how it can be applied to the Minkowski space of special relativity.

Section 1. Prologue

(1.1) Terminology Most of the terminology used in the sequel will be of standard set theoretical nature. We shall however introduce a few new terms consistent with standard terms, and bring special meaning to a few terms often applied in a more general sense.

Elements of a set will be said to be **contained** by that set, whereas subsets of a set will be said to be **comprehended** by that set.

The symmetric difference being denoted by

$$X\Delta Y, \tag{1}$$

we note that, if X is a subset of Y , then $X\Delta Y$ and $Y\Delta X$ both represent the set complement of X in Y .

The term singleton is commonly attached to a set containing a single element. We shall apply the term **doubleton** to a set containing precisely two elements, the term **tripleton** to a set containing precisely three elements, *et cet.*

A **transformation of a set A onto a set B** will mean a one-to-one function of A onto B , A **permutation** is a transformation of one set onto itself.

A **libra of transformations** is a family \mathcal{L} of transformations having a common domain and a common range and such that

$$(\forall \{\alpha, \beta, \gamma\} \subset \mathcal{L}) \quad \alpha \circ \beta^{-1} \circ \gamma \in \mathcal{L}. \tag{2}$$

Thus a **group of transformations** is a libra of transformations for which the common range equals the common domain and which contains the identity permutation ι of that common domain.

If \mathcal{F} is a libra of transformations from one set X onto another Y , if S is a subset of X and if T is subset of Y , we shall adopt the notation

$$\mathcal{F}|_{S,T} \equiv \{\theta|S \leftrightarrow T : (\exists \phi \in \mathcal{F}) \theta \subset \phi\}. \tag{3}$$

We shall say that $\mathcal{F}|_{S,T}$ is the **restriction of the family \mathcal{F} to $S \times T$** . We note that $\mathcal{F}|_{S,T}$ is also a libra of transformations.

For the case wherein S is identical with T , we shall abbreviate the notation (3) to

$$\mathcal{F}|_S. \tag{4}$$

In this case, if \mathcal{F} is a group, then so is $\mathcal{F}|_S$.

If ϕ is any function, x any element of its domain and X is any subset of the domain of ϕ , we define $\phi(x)$ by

$$[x, \phi(x)] \in \mathcal{F} \tag{5}$$

and

$$\phi[X] \equiv \{\phi(x) : x \in X\}. \tag{6}$$

Section 2. Projective Space

(2.1) Definition We begin with a group

$$\mathcal{P} \tag{1}$$

of permutations on a set

$$P, \tag{2}$$

our object being to prescribe properties for \mathcal{P} which will cause P to resemble our intuitive idea of a projective space.

Perhaps the most basic concept of projective geometry is the idea of alignment: what it means for a point p to be aligned with two other points a and b . It is a signal fact that when a projective mapping interchanges two points, it acts as an involution on the set of points aligned with those two points. That means, that if p is aligned with a and b , and if ϕ is in \mathcal{P} , either $\phi(p)$ should be p , or $\phi(\phi(p))$ should be p . It also is a signal fact that, if an involutive projective mapping has a fixed point, it has at least two fixed points. Consequently, if p is aligned with points a and b , and if ϕ interchanges a and b , then there always exists a fourth point q distinct from a , b and p such that $\{p,q\} = \{\phi(p),\phi(q)\}$. This motivates our definition of alignment: a point p **is aligned with a doubleton** $\{a,b\}$ if

$$(\forall \phi \in \mathcal{P}: \phi(a) = b \text{ and } \phi(b) = a) (\exists q \in (P \Delta \{p\})) \quad \{p,q\} = \{\phi(p),\phi(q)\}. \tag{3}$$

For a doubleton $\{a,b\}$ we shall write

$$\overleftrightarrow{a,b} \tag{4}$$

for the set of all points aligned with $\{a,b\}$. Though tempted to call $\overleftrightarrow{a,b}$ a “line”, we were dissuaded by the fact that “line” means something else in the context of linear spaces. We shall call $\overleftrightarrow{a,b}$ a **meridian**.

Obviously both a and b are aligned with $\{a,b\}$. To provide that our geometry be non-trivial, we posit the following

Postulate of Substance:

$$(\forall \{a,b\} \text{ a doubleton subset of } P) \quad \overleftrightarrow{a,b} \neq \{a,b\}: \tag{5}$$

That is, $\overleftrightarrow{a,b}$ **has at least three distinct points**. Of course, if $\overleftrightarrow{a,b}$ has three distinct points, it follows from (3) that it has at least four as well.

If a set has the property that, whenever it comprehends a doubleton $\{a,b\}$, it also comprehends the entire meridian $\overleftrightarrow{a,b}$, we shall say that that set is **extensive**. The set P is extensive, and the intersection of any family of extensive sets is extensive, whence follows that each subset S of P is comprehended by a minimal extensive set. We shall call that set the **span of S** and denote it by

$$\boxed{S}. \tag{6}$$

A subset I of P is said to be **independent** if there is no element p of I for which p is in $\boxed{I \Delta \{p\}}$. An element x of P is said to be **fundamental for an independent set** I if it is in the span \boxed{I} of I , but not in the span of any proper subset of I . If I is an independent set and x a fundamental point for I , we say that $\{x\} \cup I$ is a **fundamental set**.

Our second postulate for a projective space will be the

Uniqueness Postulate;

$$(\forall \{\alpha,\beta\} \subset \mathcal{P})(\forall F \text{ a fundamental subset of } P) \quad \alpha \text{ and } \beta \text{ agree on } \boxed{F} \text{ if they agree on } F. \tag{7}$$

Our third and final postulate is motivated by the so-called “fundamental theorem of projective geometry”:

Fundamental Postulate:

$$(\forall \theta | F \leftrightarrow G : \theta \text{ is a transformation and } F \text{ and } G \text{ are fundamental sets})(\exists \phi \in \mathcal{P}) \quad \theta \subset \phi. \quad (8)$$

If all three postulates (5), (7) and (8) are satisfied, we shall say that \mathcal{P} is a **projective permutation group with associated projective space** P . In this case, the elements of \mathcal{P} are said to be **homographies**, and the projective group \mathcal{P} will at times be referred to as the **homography group of P** .

By a **trivial projective space**, we shall mean a singleton.

In the sequel, P will always denote a projective space and \mathcal{P} its group of homographies.

(2.2) Projective Isomorphisms Let P be a projective space with projective group \mathcal{P} and let Q be a projective space with projective group \mathcal{Q} . A transformation $\theta | P \leftrightarrow Q$ is said to be a **projective isomorphism** if

$$\mathcal{P} = \{ \phi \circ \theta \circ \phi^{-1} : \theta \in \mathcal{Q} \}. \quad (1)$$

When Q is just P , we call a projective isomorphism a **projective automorphism**. Evidently

$$\text{homographies are projective automorphisms.} \quad (2)$$

The converse however does not always hold.

(2.3) Initial Observations Let $\{a, b\}$ be a doubleton subset of P . It is trivial that

$$\{a, b\} \subset \overleftrightarrow{a, b}. \quad (1)$$

Let ϕ be a projective isomorphism from one projective space P onto another Q . If $\{a, b, x\}$ is a tripleton such that x is aligned with $\{a, b\}$, then

$$(\forall \phi \in \mathcal{P}) \quad \phi(x) \text{ is aligned with } \{ \phi(a), \phi(b) \}. \quad (2)$$

Let θ be any element of \mathcal{Q} which interchanges $\phi(a)$ and $\phi(b)$. Then $\phi^{-1} \circ \theta \circ \phi$ interchanges a and b . Since x is aligned with $\{a, b\}$, it follows that there exists $y \in (P \Delta \{a, b, x\})$ such that

$$\{x, y\} = \{ \phi^{-1} \circ \theta \circ \phi(x), \phi^{-1} \circ \theta \circ \phi(y) \}.$$

Applying ϕ to each side of the above, we obtain

$$\{ \phi(x), \phi(y) \} = \{ \theta(\phi(x)), \theta(\phi(y)) \}.$$

It follows that (2) holds.

Let ϕ be a projective isomorphism from one projective space P onto another Q . Let S be any subset of P . Then

$$\boxed{\phi[S]} = \phi[\boxed{S}]. \quad (3)$$

This is a direct consequence of (1.1.6) and (2).

Let ϕ be a projective isomorphism from one projective space P onto another Q . Let p be a fundamental point for an independent set I . Then

$$\phi[I] \text{ is independent and } \phi(p) \text{ is a fundamental point for } \phi[I]. \quad (4)$$

That $\phi[I]$ is independent is a consequence of (3). That $\phi(p)$ is a fundamental point for $\phi[I]$ also follows from (3).

Let $\{a, b, x\}$ be a tripleton comprehended by P . Then

$$x \text{ is aligned with } \{a, b\} \iff x \text{ is fundamental for } \{a, b\}. \quad (5)$$

\implies : Since singletons cannot comprehend doubletons, we know that both $\{a\}$ and $\{b\}$ are extensive (by default). It follows that $\{a\} = \boxed{\{a\}}$, that $\{b\} = \boxed{\{b\}}$ and that $\{a,b\}$ is independent. Since x is aligned with $\{a,b\}$, it is in $\boxed{\{a,b\}}$ but in neither $\{a\}$ nor $\{b\}$. It follows that x is fundamental for the independent set $\{a,b\}$.

\impliedby : We suppose now that x is fundamental for $\{a,b\}$. It is a consequence of the **postulate of substance** that there exists an element p distinct from a and b aligned with $\{a,b\}$. It is a consequence of the first paragraph of this proof that p is fundamental for $\{a,b\}$. It is a consequence of the **fundamental postulate** that there exists a homography ϕ which leaves a and b fixed and sends p to x . Since p is aligned with $\{a,b\}$, it follows from (2) that x is also aligned with $\{a,b\}$.

Let F be any fundamental set and let p be any element of F . Then

$$F \Delta \{p\} \text{ is independent and } p \text{ is a fundamental element for } F \Delta \{p\}. \quad (6)$$

Since F is a fundamental set, it has an independent subset I and an element q which is fundamental for I . It follows from the **fundamental postulate** that there exists an element ϕ of \mathcal{P} which interchanges p and q and leaves every other element of F fixed. It now follows from (4) that (6) holds.

(2.4) Subspace of a Projective Space Let P be a projective space with projective group \mathcal{P} and let S be an extensive subset of P . Such sets S are projective spaces in their own right with projective groups defined by

$$\mathcal{P}_S \equiv \{\phi|_S : \phi \in \mathcal{P} \text{ and } (\forall x \in S) \phi(x) \in S\}. \quad (1)$$

That \mathcal{P}_S is a projective group follows directly from the postulates and the definitions. We shall at times refer to extensive sets as **subspaces**.

(2.5) Homography Notation The **fundamental postulate** and the **uniqueness postulate** together beg introduction of special notation. Let θ be a transformation of one finite fundamental set F onto another G . We know that there exists an element of \mathcal{P} unique on \boxed{F} which extends θ . If $F = \{a,b,c,\dots\}$, we shall denote that element of \mathcal{P} by

$$\begin{array}{cccc} \theta(a) & \theta(b) & \theta(c) & \dots \\ \hline a & b & c & \dots \end{array}. \quad (1)$$

For example, the expression

$$\begin{array}{ccc} b & d & f \\ \hline a & c & e \end{array} \quad (2)$$

means that $\{a,c,e\}$ is a tripleton in one meridian comprised by P , that $\{b,d,f\}$ is another such tripleton and that $\begin{array}{ccc} b & d & f \\ \hline a & c & e \end{array}$ is the restriction to $\boxed{\{a,c,e\}}$ of an homography ϕ of P which sends a to b , c to d and e to f .

For fundamental subsets of meridians, this terminology may often be abbreviated, due to the following fact: Let $\{a,b\}$ be a doubleton in P and let ϕ be any homography which interchanges a and b . Then

$$(\forall x \in \overleftrightarrow{a,b}) \quad \phi^{-1}(x) = \phi(x). \quad (3)$$

Since x is aligned with $\{a,b\}$, it follows that there exists y in P such that $\{x,y\} = \{\phi(x), \phi(y)\}$. If $x = \phi(x)$, then $\phi^{-1}(x) = \phi(x)$ and, if $x = \phi(y)$, then $\phi^{-1}(x) = y = \phi(x)$. In both cases we have (3).

When (3) holds and ϕ does *not* fix each element of $\overleftrightarrow{a,b}$, we say that ϕ is **involutive on** $\overleftrightarrow{a,b}$. If for any reason we know that ϕ is involutive, and we know that the terms c and d are distinct, it follows that the expression $\begin{array}{ccc} b & d & f \\ \hline a & c & e \end{array}$ gives the same function as $\begin{array}{ccc} b & d & c \\ \hline a & c & d \end{array}$. This suggests that we introduce an abbreviated notation for this expression:

$$\boxed{\begin{array}{cc} \mathbf{b} & \mathbf{d} \\ \mathbf{a} & \mathbf{c} \end{array}}. \quad (4)$$

In the sequel, an expression of the form as in (4) will always represent an element of \mathcal{P} which is involutive on the meridian $\overleftrightarrow{\mathbf{a},\mathbf{b}}$, \mathbf{a} is sent to \mathbf{b} , \mathbf{c} is sent to \mathbf{d} and $\{\mathbf{a},\mathbf{b},\mathbf{c}\}$ is a tripleton.

(2.6) Meridians Let M be a meridian and let $\{\mathbf{p},\mathbf{q}\}$ be a doubleton subset of M . Then

$$M = \overleftrightarrow{\mathbf{p},\mathbf{q}}. \quad (1)$$

Assume that (1) did not hold. Then there would exist a homography ϕ on M which interchanged \mathbf{p} and \mathbf{q} and an element \mathbf{c} of M such that

$$\mathbf{d} \equiv \phi \circ \phi(\mathbf{c}) \neq \mathbf{c}. \quad (i)$$

It is a consequence of the **postulate of substance** that there exists an element \mathbf{r} of $\overleftrightarrow{\mathbf{p},\mathbf{q}}$ distinct from \mathbf{p} and \mathbf{q} . Since M is a meridian, there exists a doubleton $\{\mathbf{a},\mathbf{b}\}$ such that $M = \overleftrightarrow{\mathbf{a},\mathbf{b}}$. It follows from (2.3.5) that $\{\mathbf{a},\mathbf{b},\mathbf{c}\}$ and $\{\mathbf{p},\mathbf{q},\mathbf{r}\}$ are fundamental sets. It follows from the **fundamental postulate** that there would exist a homography θ of M such that

$$\theta(\mathbf{a}) = \mathbf{p}, \theta(\mathbf{b}) = \mathbf{q} \text{ and } \theta(\mathbf{d}) = \mathbf{r}. \quad (ii)$$

Let

$$\psi \equiv \theta^{-1} \circ \phi \circ \theta \text{ and } \mathbf{e} \equiv \theta^{-1}(\mathbf{c}). \quad (iii)$$

We would have by (i)

$$\psi \circ \psi(\mathbf{e}) \stackrel{\text{by (iii)}}{=} \theta^{-1} \circ \phi \circ \phi(\mathbf{c}) \neq \theta^{-1}(\mathbf{c}) \stackrel{\text{by (iii)}}{=} \mathbf{e}. \quad (iv)$$

By (ii) and (iv) we would have

$$\psi(\mathbf{a}) = \mathbf{b} \text{ and } \psi(\mathbf{b}) = \mathbf{a}$$

whence follows that $\psi \circ \psi$ would be the identity function on M . By (iv) this were absurd.

Let $\{\mathbf{a},\mathbf{b},\mathbf{c}\}$ be a tripleton subset of a meridian. Then

$$\{\mathbf{a},\mathbf{b},\mathbf{c}\} \text{ is fundamental set.} \quad (2)$$

From (1) we know that $\overleftrightarrow{\mathbf{a},\mathbf{b}}$ is just the meridian, and so \mathbf{c} is aligned with $\{\mathbf{a},\mathbf{b}\}$. From (2.3.5) we know then that $\{\mathbf{a},\mathbf{b},\mathbf{c}\}$ is fundamental.

We shall call an involutive homography of a meridian a **meridian involution**. It is an idiosyncrasy that

$$\text{a meridian involution } \phi \text{ either has no fixed point or two fixed points.} \quad (3)$$

If ϕ had 3 fixed points, we would know from (2) that the set of these points would be a fundamental set and so by the **uniqueness postulate** ϕ would agree on the span of those fixed points. But, by (3), that span would be the whole meridian, and so ϕ could not be a *bona-fide* involution.

Suppose that ϕ has a fixed point \mathbf{x} . From the **postulate of substance** we know that there exists a doubleton $\{\mathbf{a},\mathbf{b}\}$ not containing \mathbf{x} . Since \mathbf{x} is in alignment with $\{\mathbf{a},\mathbf{b}\}$, we know that there exists \mathbf{y} distinct from \mathbf{x} such that $\{\mathbf{x},\mathbf{y}\} = \{\phi(\mathbf{x}),\phi(\mathbf{y})\}$. Evidently, $\phi(\mathbf{y})$ must be \mathbf{y} .

If $\{\mathbf{a},\mathbf{b}\}$ is a doubleton subset of a meridian, then

$$\text{there is a unique involution of that meridian which fixes both } \mathbf{a} \text{ and } \mathbf{b}. \quad (4)$$

We shall denote that involution by

$$\boxed{\begin{array}{cc} \mathbf{a} & \mathbf{b} \\ \mathbf{a} & \mathbf{b} \end{array}} \quad (5)$$

From (1) we know that the meridian is just $\overleftrightarrow{a,b}$ and from the **postulate of substance** we know that there exists some c in $\overleftrightarrow{a,b}$ distinct from a and b . It follows from (3) that there exists an element d of $\overleftrightarrow{a,b} \Delta \{a,b,c\}$ such that $\begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} (d) = d$. Direct calculation shows that

$$\begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} (a) = a \quad \text{and} \quad \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} (b) = b.$$

and that $\begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix}$ is an involution. This proves the existence of $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$.

Let ϕ be any involution of $\overleftrightarrow{a,b}$ which fixes both a and b . Let e denote $\phi(c)$. Direct calculation shows that $\begin{bmatrix} c & a & e \\ a & c & b \end{bmatrix} \circ \phi \circ \begin{bmatrix} c & a & e \\ a & c & b \end{bmatrix}$ fixes both c and e and interchanges a and b . It follows from the **fundamental postulate** that $\begin{bmatrix} c & a & e \\ a & c & b \end{bmatrix} \circ \phi \circ \begin{bmatrix} c & a & e \\ a & c & b \end{bmatrix}$ is just $\begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix}$. It follows from (3) that $\begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix}$ fixes only c and d . Consequently $e = d$. It follows from the **fundamental postulate** that $\phi = \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix}$, which establishes the uniqueness part of (5).

A homography on a meridian is said to be a **translation** if it has a single fixed point. If two distinct involutions α and β of a meridian have a common fixed point a , then

$$\alpha \circ \beta \quad \text{is a translation with fixed point } a. \quad (6)$$

If $\alpha \circ \beta$ were not a translation, then it would fix another point e distinct from a . Then α and β would agree on the distinct points a and e and so by (5), α and β would be identical: an absurdity. This establishes (6).

If a translation τ fixes a point a , if b is distinct from a , and if c represents $\tau(b)$, then

$$\begin{bmatrix} a & c \\ a & c \end{bmatrix} \circ \begin{bmatrix} a & c \\ a & b \end{bmatrix} = \tau. \quad (7)$$

Let a , b and c be as in (7) and let d be $\tau(c)$. Then

$$\tau(a) = a. \quad (i)$$

Evidently $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau$ interchanges b and c . By (2.5.3),

$$\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \quad \text{is an involution.} \quad (ii)$$

We have

$$a \xrightarrow{\text{by (ii)}} \left(\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \right) \circ \left(\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \right) (a) \xrightarrow{\text{by (i)}} \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \circ \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a). \quad (iii)$$

Since $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix}$ interchanges b and d , it follows from (2.5.3) that

$$\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \quad \text{is an involution.} \quad (iv)$$

Thus

$$\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a) \xrightarrow{\text{by (iii)}} \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \left(\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \circ \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a) \right) \xrightarrow{\text{by (iv)}} \tau \left(\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a) \right). \quad (v)$$

Since τ is a translation, it follows from (i) and (v) that

$$a = \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a). \quad (vi)$$

Thus, besides interchanging b and c , $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau$ fixes a , whence follows that

$$\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau = \begin{bmatrix} a & b & c \\ a & c & b \end{bmatrix}. \quad (vii)$$

From (vi) follows that $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} = \begin{bmatrix} a & c \\ a & c \end{bmatrix}$ and so (vii) becomes

$$\begin{bmatrix} a & c \\ a & c \end{bmatrix} \circ \tau = \begin{bmatrix} a & b & c \\ a & c & b \end{bmatrix}$$

whence follows (7).

Let two translations on a meridian have a common fixed point. Then

$$\text{if they agree on any other point, they are identical.} \quad (8)$$

Let \mathbf{a} be the common fixed point and let \mathbf{b} be the point distinct from \mathbf{a} at which they agree. Then it follows from (7) that both equal $\begin{bmatrix} \mathbf{a} & \mathbf{c} \\ \mathbf{a} & \mathbf{c} \end{bmatrix} \circ \begin{bmatrix} \mathbf{a} & \mathbf{c} \\ \mathbf{a} & \mathbf{b} \end{bmatrix}$, where $\mathbf{c} \equiv \tau(\mathbf{b})$.

Let α, β and γ be involutions of a meridian with a common fixed point. Then

$$\alpha \circ \beta \circ \gamma \text{ is an involution.} \quad (9)$$

Let \mathbf{a} denote the common fixed point and let \mathbf{x} be any other point distinct from \mathbf{x} . Let \mathbf{y} be $\alpha \circ \beta(\mathbf{x})$ and let \mathbf{z} be $\gamma(\mathbf{x})$. It follows from (6) that both $\alpha \circ \beta$ and $\begin{bmatrix} \mathbf{a} & \mathbf{z} \\ \mathbf{a} & \mathbf{y} \end{bmatrix} \circ \gamma$ are translations. Both these translations send \mathbf{a} to \mathbf{a} and \mathbf{x} to \mathbf{y} . It follows from (8) that they are identical. Consequently $\alpha \circ \beta \circ \gamma = \begin{bmatrix} \mathbf{a} & \mathbf{z} \\ \mathbf{a} & \mathbf{y} \end{bmatrix}$.

Each fundamental subset $\{\infty, \mathbf{o}, \mathbf{l}\}$ of a meridian M induces a field F of characteristic not equal to 2, which we shall call the **projective field of P with ordered fundamental set $[\infty, \mathbf{o}, \mathbf{l}]$** . The definitions are as follows: $F \equiv M \Delta \{\infty\}$, $G \equiv F \Delta \{\mathbf{o}\}$,

$$(\forall \{x, y\} \subset F) \quad x+y \equiv \begin{bmatrix} \infty & x+y \\ \infty & y \end{bmatrix}(\mathbf{o}), \quad x+(-x) = \mathbf{o}, \quad (10)$$

$$(\forall \{x, y\} \subset G) \quad x \cdot y \equiv \begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix}(\mathbf{l}), \quad x \cdot \mathbf{o} \equiv \mathbf{o} \cdot x \equiv \mathbf{o}, \quad x \cdot (x^{-1}) = \mathbf{l} \quad \text{and} \quad \frac{x}{y} = x \cdot (y^{-1}).$$

We first note that the involutions $\begin{bmatrix} \infty & x+y \\ \infty & \mathbf{o} \end{bmatrix}$ and $\begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}$ agree at both ∞ and \mathbf{o} , so

$$\begin{bmatrix} \infty & x+y \\ \infty & \mathbf{o} \end{bmatrix} = \begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}. \quad (i)$$

It follows from (9) that $\begin{bmatrix} \infty & \mathbf{o} \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & y \end{bmatrix}$ is an involution — consequently it is the same as $\begin{bmatrix} \infty & \mathbf{o} \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & x \end{bmatrix}$.

Direct computation shows that the latter agrees with the involution $\begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}$ at both ∞ and x . So we have

$$\begin{bmatrix} \infty & \mathbf{o} \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & y \end{bmatrix} = \begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}. \quad (ii)$$

Similar reasoning shows that, for $\{x, y\}$ disjoint from $\{\infty, \mathbf{o}\}$,

$$\begin{bmatrix} \infty & x \cdot y \\ \mathbf{o} & \mathbf{l} \end{bmatrix} = \begin{bmatrix} \infty & y \\ \mathbf{o} & x \end{bmatrix} = \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{l} \end{bmatrix}. \quad (iii)$$

For x in F and y in $F \Delta \{\mathbf{o}\}$ we define

$$-x \equiv \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix}(x) \quad \text{and} \quad u^{-1} \equiv \begin{bmatrix} \infty & \mathbf{l} \\ \infty & \mathbf{l} \end{bmatrix}(u). \quad (iv)$$

Then

$$x + \mathbf{o} \stackrel{\text{by (i)}}{=} \begin{bmatrix} \infty & \mathbf{o} \\ \infty & x \end{bmatrix}(\mathbf{o}) = x, \quad u \cdot \mathbf{l} \stackrel{\text{by (iii)}}{=} \begin{bmatrix} \infty & u \\ \infty & \mathbf{l} \end{bmatrix}(\mathbf{l}) = u, \quad (v)$$

$$x + (-x) \stackrel{\text{by (i)}}{=} \begin{bmatrix} \infty & x \\ \infty & -x \end{bmatrix}(\mathbf{o}) \stackrel{\text{by (ii)}}{=} \begin{bmatrix} \infty & \mathbf{o} \\ \infty & -x \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \infty & \mathbf{o} \end{bmatrix}(\mathbf{o}) = \begin{bmatrix} \infty & \mathbf{o} \\ \infty & -x \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix}(x) \stackrel{\text{by (iv)}}{=} \begin{bmatrix} \infty & \mathbf{o} \\ \infty & -x \end{bmatrix}(-x) = \mathbf{o}$$

and, similarly, one obtains

$$u^{-1} \cdot u = \mathbf{l}. \quad (vii)$$

For $\{x, y, z\}$ comprised by F ,

$$x + (y+z) \stackrel{\text{by (i)}}{=} \begin{bmatrix} \infty & y+z \\ \infty & x \end{bmatrix}(\mathbf{o}) \stackrel{\text{by (ii)}}{=} \begin{bmatrix} \infty & \mathbf{o} \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & y+z \end{bmatrix}(\mathbf{o}) \stackrel{\text{by (ii)}}{=} \begin{bmatrix} \infty & \mathbf{o} \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & z \end{bmatrix}(\mathbf{o}) \stackrel{\text{by (ii)}}{=} \begin{bmatrix} \infty & \mathbf{o} \\ \infty & x+y \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{o} \\ \infty & z \end{bmatrix}(\mathbf{o}) \stackrel{\text{by (ii)}}{=} \begin{bmatrix} \infty & x+y \\ \infty & z \end{bmatrix}(\mathbf{o}) = (x+y)+z. \quad (viii)$$

One can deduce in a similar way that, for $\{u, v, w\} \subset (F \Delta \{\mathbf{o}\})$,

$$u \cdot (v \cdot w) = (u \cdot v) \cdot w. \quad (ix)$$

That

$$x+y = y+x \quad \text{and} \quad x \cdot y = y \cdot x \quad (x)$$

is trivial. We have established that “+” and “.” are abelian group operations. It remains to show that the “distributive law” holds.

Let x, y and z be elements of F such that x and $y+z$ are distinct from \mathbf{o} . We define

$$\theta \equiv \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & z \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix}. \quad (xi)$$

Evidently

$$\theta(\infty) = \infty. \quad (xii)$$

Furthermore

$$\begin{aligned} \theta(\mathbf{o}) &\stackrel{\text{by (xi)}}{=} \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} (\mathbf{o}) = \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} (\mathbf{o}) \stackrel{\text{by (i)}}{=} \\ &\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} (y+z) = \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & y+z \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & y+z \end{bmatrix} (y+z) = \\ &\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & y+z \end{bmatrix} (\mathbf{l}) \stackrel{\text{by (iii)}}{=} x \cdot (y+z). \end{aligned} \tag{xiii}$$

Moreover

$$\begin{aligned} \theta(x \cdot y) &\stackrel{\text{by (xi)}}{=} \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} (x \cdot y) \stackrel{\text{by (iii)}}{=} \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} (\mathbf{l}) = \\ &\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} \circ \left(\begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} \right) (\mathbf{l}) \stackrel{\text{by (iii)}}{=} \\ &\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} \circ \left(\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \right) (\mathbf{l}) = \\ &\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \left(\begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \left(\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \left(\begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \mathbf{o} & y \end{bmatrix} \right) \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \right) \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \right) (\mathbf{l}) = \\ &\begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \mathbf{o} & \mathbf{z} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} (\mathbf{l}) = \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} (\mathbf{z}) = \begin{bmatrix} \infty & x \\ \mathbf{o} & \mathbf{l} \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{l} \\ \mathbf{o} & \mathbf{o} \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \mathbf{o} & \mathbf{l} \end{bmatrix} (\mathbf{l}) \stackrel{\text{by (iii)}}{=} x \cdot z. \end{aligned}$$

Since θ is an involution, it follows from this last and (xii) that $\theta = \begin{bmatrix} \infty & x \cdot z \\ \infty & x \cdot y \end{bmatrix}$. Consequently

$$\theta(\mathbf{o}) = \begin{bmatrix} \infty & x \cdot z \\ \infty & x \cdot y \end{bmatrix} (\mathbf{o}) \stackrel{\text{by (i)}}{=} x \cdot y + x \cdot z. \tag{xiv}$$

From (xiii) and (xiv) we have

$$x \cdot (y+z) = x \cdot y + x \cdot z. \tag{xv}$$

We have established that F is a field, if its characteristic were 2, then, for any x in $F \setminus \{0\}$,

$$\begin{bmatrix} \infty & x \\ \infty & x \end{bmatrix} (\mathbf{o}) = x + x = \mathbf{o} = \mathbf{o} + \mathbf{o} = \begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} (\mathbf{o}).$$

Thus, $\begin{bmatrix} \infty & x \\ \infty & x \end{bmatrix}$ and $\begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix} (\mathbf{o})$ would agree on two distinct points and, being involutions, would have to be identical. It would follow that $\begin{bmatrix} \infty & \mathbf{o} \\ \infty & \mathbf{o} \end{bmatrix}$ would fix every point in F . Since the identity function is not an involution, this were absurd.

There is a converse to (10). Let F be a field of characteristic not equal to 2. We form a larger set M by adducing an element ∞ not already an element of F . For elements a, b, c and d in F such that $a \cdot d \neq b \cdot c$, we define $\begin{pmatrix} a & b \\ c & d \end{pmatrix} | M \leftrightarrow M$ by, for each x in M

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (x) \equiv \begin{cases} \infty & \text{if } x = \infty \text{ and } c = 0; \\ \frac{a}{c} & \text{if } x = \infty \text{ and } c \neq 0; \\ \infty & \text{if } x \neq \infty \text{ and } c \cdot x = 0; \\ \frac{a \cdot x + b}{c \cdot x + d} & \text{if } x \neq \infty \text{ and } c \cdot x + d \neq 0. \end{cases} \tag{11}$$

These functions are called **linear fractional transformations** and they form a projective group on M , where composition corresponds to matrix multiplication.

When the field originates from a meridian, as in (10), the linear fractional transformations are just the homographies of M .

(2.7) Decomposition Let ϕ be a non-involutive homography of a meridian M . Then

$$\text{there exist two involutions } \alpha \text{ and } \beta \text{ of } M \text{ such that } \phi = \alpha \circ \beta. \tag{1}$$

Since the composition of two involutions is the identity, we may presume that ϕ is not the identity. Suppose that $\phi \circ \phi \circ \phi = \iota$ the identity. Let p be any element of M not fixed by ϕ . If $\phi \circ \phi(p) = p$, then it would follow from (2.5.3) that ϕ were involutive: an absurdity. It follows that $\phi \circ \phi(p) \neq p$ and so $p, q \equiv \phi(p)$ and $r \equiv \phi(q)$ are distinct. The functions ϕ and $\begin{bmatrix} r & q \\ p & q \end{bmatrix} \circ \begin{bmatrix} q & r \\ p & r \end{bmatrix}$ agree at p, q and r , whence from the **uniqueness postulate** follows that they are equal.

Finally we consider the case where there exists p such that $\{p, q \equiv \phi(p), r \equiv \phi(q), s \equiv \phi(r)\}$ is a quadruplet. The homographies ϕ and $\begin{bmatrix} s & r \\ q & r \end{bmatrix} \circ \begin{bmatrix} s & r \\ p & q \end{bmatrix}$ agree at p, q and r . By the **uniqueness postulate**, $\phi = \begin{bmatrix} s & r \\ q & r \end{bmatrix} \circ \begin{bmatrix} s & r \\ p & q \end{bmatrix}$.

(2.8) Fundamental Structure of a Projective Space By an **independent basis for an extensive subset** S of P we shall mean a maximal independent subset of S . The least upper bound of the cardinalities of independent bases, minus 1, is the **dimension of S** . If this is finite, we say that S is **finite dimensional**. Towards constructing bases, we have the following

$$(\forall I \text{ independent and finite})(\forall x \in (P \triangle \boxed{I})) \quad \{x\} \cup I \text{ is an independent basis for } \boxed{\{x\} \cup I}. \quad (1)$$

We establish (1) by induction on the cardinality n of I . It is evidently true for $n = 1$. We suppose that it is known to be true for all n less than or equal to some fixed positive integer m . Assume that (1) were not true for some independent set I of cardinality $m+1$ and x in $P \triangle \boxed{I}$. Then there would exist some p in I also contained in $\boxed{\{x\} \cup (I \triangle \{p\})}$. If F were any finite proper subset of $\{x\} \cup (I \triangle \{p\})$ such that p were in \boxed{F} , then x would have to be in F since I is independent. By our induction hypothesis we would know that F were independent. Since F were independent and its cardinality would be m or less, this would contradict our induction hypothesis, so such an F could not exist. It follows from the induction hypothesis that

$$\{x\} \cup (I \triangle \{p\}) \text{ would be independent.} \quad (i)$$

Consequently, p would be a fundamental point for $\{x\} \cup (I \triangle \{p\})$. It would follow from the **fundamental postulate** that there would exist a homography which interchanged x and p but kept each other element of I fixed. Since It would then follow from (i) and (2.3.4) that $\{x\} \cup I$ would be independent, which would be contrary to our assumption.

If P is finite dimensional and d is its dimension, then any independent subset of P of cardinality $d+1$ is said to be a **simplex for P** . It is a consequence of (1) that

$$\text{if } P \text{ is finite dimensional, then any simplex for } P \text{ is an independent basis for } P. \quad (2)$$

Let I be a finite independent set and let p be a fundamental point for I . Then

$$(\forall q \in I) \quad \{p\} \cup (I \triangle \{q\}) \text{ is independent and } q \text{ is fundamental for } \{p\} \cup (I \triangle \{q\}). \quad (3)$$

Since $\{p\} \cup I$ is a fundamental set, it follows from them **fundamental postulate** that there exists an homography which interchanges $\{p\}$ with $\{q\}$ and leaves the other elements of I fixed. It follows from (2.3.4) that $\{q\}$ is a fundamental point for $\boxed{\{p\} \cup (I \triangle \{q\})}$.

If P is of finite dimension d and

$$\text{if } S \text{ is a set of cardinality } d+1 \text{ or less such that } P = \boxed{S}, \text{ then } S \text{ is independent.} \quad (4)$$

Let S be a minimal set which spans P . If were not independent, then there would be an element p of S in $\boxed{S \triangle \{p\}}$. Then P would equal $\boxed{S \triangle \{p\}}$, which were absurd.

For any independent set I , we shall write

$$\boxed{I} \equiv \{x \in P : x \text{ is fundamental for the set } I.\} \quad (5)$$

Then

$$(\forall I \subset P \text{ independent}) \quad \boxed{J} : J \subset I \text{ is a partition of } \boxed{I}. \quad (6)$$

Let x be an element of \boxed{I} . Then there is a minimal subset S of I such that X is in \boxed{S} . The minimality of S insures that p is fundamental for S . Thus $\boxed{I} \subset \boxed{J} : J \subset I$.

Let S and T be any two distinct subsets of I . Assume that there existed an element p of $\boxed{S} \cap \boxed{T}$.

If $\overset{\square}{S} \subset \overset{\square}{T}$. then p could not be in $\overset{\square}{S}$ by the definition of “fundamental”: thus $\overset{\square}{S} \not\subset \overset{\square}{T}$. Similarly, $\overset{\square}{T} \not\subset \overset{\square}{S}$. It follows that there would exist an element a of $S\Delta\{p\}$ not in T and an element b of $T\Delta\{p\}$ not in S . From (3) follows that a would be fundamental for $\{p\} \cup (S\Delta\{a\})$ and that b would be fundamental for $\{p\} \cup (T\Delta\{b\})$. Consequently

$$\overset{\square}{I} = \overset{\square}{S} \cup \overset{\square}{T} = \overset{\square}{S} \cup \overset{\square}{T} = \overline{\{p\} \cup (S\Delta\{a\})} \cup \overline{\{p\} \cup (T\Delta\{b\})} = \overline{(\{p\} \cup S \cup T)\Delta\{a,b\}}$$

which would imply that $\overset{\square}{I}$ would be spanned by a set of cardinality one less than the cardinality of I . But that would be incompatible with (4). It follows that (6) holds.

Let I be a finite independent set, let p be an element of I , let q be an element of $\overline{I\Delta\{p\}}$ and let x be an element of $\overleftarrow{p,q}\Delta\{p,q\}$ (as provided by the **postulate of substance**). Then

$$x \text{ is in } \overset{\square}{I}. \quad (7)$$

We shall show (7) by induction on the cardinality n of I . It is evident that (7) holds when n equals 2. So we shall suppose that we have established it for all n less than or equal to some m greater than or equal to 2. We then look at I of cardinality equal to $m+1$. That x is in $\overset{\square}{I}$ is evident. Assume that x were not fundamental for I . It follows from (6) that there were a proper subset J of I such that x were in $\overset{\square}{J}$. If p were not in J , then $\overleftarrow{x,q}$ would be comprehended by $\overline{P\Delta\{p\}}$ and, since p is in $\overleftarrow{x,p}$, this would imply that p were in J : an absurdity. Thus p would have to be in J . Since q is in the line $\overleftarrow{p,x}$, it would follow from our induction hypothesis that q would be in $\overset{\square}{J}$. But J and $(P\Delta\{p\})$ would be distinct subsets of I and so by (2) could not have a common point q . It follows that (7) holds.

Let S be a finite dimensional subspace of P , let T be a maximal proper subspace of S and let M be a meridian comprehended by S but not by T . Then

$$M \text{ intersects } T \text{ at precisely one point.} \quad (8)$$

If M intersected T at two points a and b , by (1), M would be $\overleftrightarrow{a,b}$ and so a subset of T : thus the intersection is either void or a singleton. Let p be any element of M . Since T is a maximal proper subspace of S , we know that $\overline{\{p\} \cup T} = S$. Let q be a point of M distinct from p . Let I be an independent set which spans T . From (6) we know that exists a subset J of I such that q is in $\overset{\square}{J}$. If p were not in J , then q would be in a subset of T and (8) would be true, so we shall presume that p is in J . It follows from (7) that there exists an element r of $\overset{\square}{J}$ such that the line $\overleftarrow{p,r}$ intersects $\overline{J\Delta\{p\}}$. Since $(\{q\} \cup J)$ and $(\{r\} \cup J)$ are both fundamental, it follows from the **fundamental postulate** that there exists ϕ in \mathcal{P} which interchanges q and r and leaves each element of J fixed. Recall that the meridian $\overleftarrow{p,r}$ intersects $\overline{J\Delta\{p\}}$ at some point y . It follows its image by ϕ , which is $\overleftarrow{p,q}$, intersects $\overline{J\Delta\{p\}}$, which is comprehended by T . Thus $\overleftarrow{p,q}$ intersects T at $\phi(y)$.

(2.9) The von Staudt Meridian There is a special meridian inherent in any finite dimensional projective space P . To realize this we first take any set of cardinality 4: say

$$\mathbf{III}_4 \equiv \{\heartsuit, \spadesuit, \clubsuit, \diamondsuit\}. \quad (1)$$

Then we consider the set

$$\Omega_P \quad (2)$$

consisting of all functions $f: \mathbf{III}_4 \rightarrow P$ such that the set $\{f(x) : x \in \mathbf{III}_4\}$ is co-aligned and of cardinality at least three. For such a co-aligned¹ set $\{w,x,y,z\}$ within P , we shall adopt the notation

¹ By **co-aligned** we mean that each point is aligned with each doubleton in the set: all the elements of

$$\begin{array}{|c|} \hline w \ x \ y \ z \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} \quad (3)$$

for the function on $\Omega_{\mathcal{P}}$ which sends \heartsuit to w , \spadesuit to x , \clubsuit to y and \diamondsuit to z . We shall adopt the notation

$$\begin{array}{|c|} \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline w \ x \ y \ z \\ \hline \end{array} \quad (4)$$

for its inverse.

Besides the identity permutation of \mathbf{III}_4 , there are three other permutations of particular interest here: the one that interchanges \heartsuit with \diamondsuit and \spadesuit with \clubsuit , the one that interchanges \spadesuit with \diamondsuit and \clubsuit with \heartsuit , and the one that interchanges \clubsuit with \diamondsuit and \spadesuit with \heartsuit : we shall denote them, respectively, by

$$\begin{array}{|c|} \hline \heartsuit \ \spadesuit \\ \hline \diamondsuit \ \clubsuit \\ \hline \end{array}, \quad \begin{array}{|c|} \hline \spadesuit \ \clubsuit \\ \hline \diamondsuit \ \heartsuit \\ \hline \end{array}, \quad \text{and} \quad \begin{array}{|c|} \hline \clubsuit \ \spadesuit \\ \hline \heartsuit \ \diamondsuit \\ \hline \end{array}, \quad (5)$$

respectively. We shall denote that group of four permutations by²

$$K. \quad (6)$$

We define, for all $\{f, g\}$ comprised by $\Omega_{\mathcal{P}}$,

$$f \approx g \iff (\exists \phi \in \mathcal{P} \text{ and } \kappa \in K) \quad \phi \circ f \circ \kappa = g. \quad (7)$$

We shall denote the family of \approx -equivalence classes by

$$\mathfrak{W}_{\mathcal{P}}. \quad (8)$$

Von Staudt used the terminology ‘‘Wurf’’ for an element of $\mathfrak{W}_{\mathcal{P}}$: we shall use here the English translation **throw**. For any element t of $\Omega_{\mathcal{P}}$, we shall denote the \approx -equivalence class or throw containing it by

$$\boxed{t}. \quad (9)$$

Members of $\Omega_{\mathcal{P}}$ with ranges of cardinality 3 all fall inside the three distinct equivalence classes:

$$\infty \equiv \left\{ \begin{array}{|c|} \hline a \ b \ c \ a \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} : \{a, b, c\} \text{ is a coaligned tripleton} \right\} \cup \left\{ \begin{array}{|c|} \hline a \ b \ b \ c \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} : \{a, b, c\} \text{ is a coaligned tripleton} \right\}, \quad (10)$$

$$0 \equiv \left\{ \begin{array}{|c|} \hline a \ b \ c \ b \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} : \{a, b, c\} \text{ is a coaligned tripleton} \right\} \cup \left\{ \begin{array}{|c|} \hline a \ b \ a \ c \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} : \{a, b, c\} \text{ is a coaligned tripleton} \right\} \quad (11)$$

$$\text{and } 1 \equiv \left\{ \begin{array}{|c|} \hline a \ b \ c \ c \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} : \{a, b, c\} \text{ is a coaligned tripleton} \right\} \cup \left\{ \begin{array}{|c|} \hline a \ a \ b \ c \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array} : \{a, b, c\} \text{ is a coaligned tripleton} \right\}. \quad (12)$$

Let M be any meridian comprised by \mathcal{P} and let $\{a, b, c\}$ be any tripleton comprised by M . We shall call the function

$$\phi_{a, b, c} \big| M \ni x \mapsto \boxed{\begin{array}{|c|} \hline a \ b \ c \ x \\ \hline \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \\ \hline \end{array}} \in \mathfrak{W}_{\mathcal{P}} \quad (13)$$

a **scalar function on M** . The family

$$\mathcal{W}_{\mathcal{P}} \equiv \{ \alpha \circ \beta^{-1} : \alpha \text{ and } \beta \text{ are scalar functions on } M \} \quad (14)$$

is a projective group of permutations of $\mathfrak{W}_{\mathcal{P}}$, relative to which $\mathfrak{W}_{\mathcal{P}}$ is a meridian. Furthermore $\mathcal{W}_{\mathcal{P}}$ does not depend on the choice of M . For each tripleton $\{u, v, w\}$ in M and each tripleton $\{r, s, t\}$ of throws, there is a unique scalar function on M which sends u to r , v to s and w to t : we shall denote it by

$$\boxed{\begin{array}{|c|} \hline r \ s \ t \\ \hline u \ v \ w \\ \hline \end{array}} \quad \text{and its inverse by} \quad \boxed{\begin{array}{|c|} \hline u \ v \ w \\ \hline r \ s \ t \\ \hline \end{array}}. \quad (15)$$

the set are in a single meridian.

² Sometimes called the **Klein 4-group**.

The inverses of scalar functions will be called **von Staudt injections**. A direct calculation shows that, for the function of (13),

$$\phi_{\alpha, \beta, \gamma} = \begin{bmatrix} \alpha & \beta & \gamma \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}. \quad (16)$$

We shall call \mathfrak{M}_P the **von Staudt meridian for P**, and we shall say that $\{\mathbf{0}, \mathbf{0}, \mathbf{1}\}$ is the **canonical fundamental subset of \mathfrak{M}_P** . We shall denote the projective field of \mathfrak{M}_P with ordered fundamental set $[\mathbf{0}, \mathbf{0}, \mathbf{1}]$ by

$$\mathfrak{F}_P \quad (17)$$

and we shall call it the **von Staudt field of P**.

Let M be a meridian comprehended by P and let $\{\infty, \mathbf{0}, \mathbf{1}\}$ be a tripleton subset of M . Let F denote the projective field of M with ordered fundamental set $[\infty, \mathbf{0}, \mathbf{1}]$. Perhaps the most easy to compute of the functions of (15) is $\begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \infty & \mathbf{0} & \mathbf{1} \end{bmatrix}$: we have

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \infty & \mathbf{0} & \mathbf{1} \end{bmatrix} | M \ni x \leftrightarrow \begin{bmatrix} \infty & \mathbf{0} & \mathbf{1} & x \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix} \in \mathfrak{M}_P. \quad (18)$$

With the aid of (18) it is not difficult to show that

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \infty & \mathbf{0} & \mathbf{1} \end{bmatrix} |_{\mathbb{F}} \quad \text{and} \quad \begin{bmatrix} \infty & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} |_{\mathfrak{F}} \quad \text{are field isomorphisms.} \quad (19)$$

Let \mathbf{s} be any scalar. Then there is a unique element s of M such that $\begin{bmatrix} \infty & \mathbf{0} & \mathbf{1} & s \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix} = \mathbf{s}$. For each x in F we define

$$\mathbf{s} \bullet x \equiv s \cdot x. \quad (20)$$

There is an alternate definition neither dependent on a choice of $\mathbf{1}$ nor a representative of \mathbf{s} :

$$\mathbf{s} \bullet x = \begin{bmatrix} \infty & \mathbf{0} & x \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} (\mathbf{s}). \quad (21)$$

We first note that, for all x and y in F , it follows from (2.6.10) and (2.6.11) that

$$\begin{bmatrix} \infty & \mathbf{0} & y \\ \infty & \mathbf{0} & \mathbf{1} \end{bmatrix} (x) = y \cdot x. \quad (i)$$

We have

$$\mathbf{s} \bullet x \stackrel{\text{by (20)}}{=} s \cdot x \stackrel{\text{by (i)}}{=} \begin{bmatrix} \infty & \mathbf{0} & x \\ \infty & \mathbf{0} & \mathbf{1} \end{bmatrix} (\mathbf{s}) \stackrel{\text{by (18)}}{=} \begin{bmatrix} \infty & \mathbf{0} & x \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} (\mathbf{s})$$

which yields (21).

(2.10) Homographic Isomorphisms We shall say that the transformation θ is **homographic** if

$$(\forall a \in \Omega_P) \quad a \approx \theta \circ a, \quad (1)$$

where \approx is the equivalence relation associated with the von Staudt meridian. If P is finite dimensional, then

$$\text{a projective automorphism is a homography if, and only if, it is homographic.} \quad (2)$$

Let ϕ be an element of \mathcal{P} . Let \mathbf{s} and \mathbf{t} be equivalent throws. Then there exists ψ in \mathcal{P} and κ in K such that $\mathbf{s} = \psi \circ \mathbf{t} \circ \kappa$. Then

$$\phi \circ \mathbf{s} = \phi \circ \psi \circ \mathbf{t} \circ \kappa = (\phi \circ \psi \circ \phi^{-1}) \circ (\phi \circ \mathbf{t}) \circ \kappa$$

whence follows that $\phi \circ \mathbf{s}$ is equivalent to $\phi \circ \mathbf{t}$. Thus ϕ is homographic.

Now suppose instead that ϕ is a homographic automorphism of P . Let F be a maximal fundamental subset of P . That $\phi[F]$ is a fundamental set follows from (2.3.4). It follows from the **fundamental postulate** that there exists an element ψ of \mathcal{P} which agrees with ϕ on F . Suppose first that P is a meridian and that F equals $\{a, b, c\}$. For any element x of P , we have

$$\begin{array}{c} \phi(a) \ \phi(b) \ \phi(c) \ \phi(x) \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} \approx \begin{array}{c} a \ b \ c \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} \approx \psi \circ \begin{array}{c} a \ b \ c \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} \approx \begin{array}{c} \psi(a) \ \psi(b) \ \psi(c) \ \psi(x) \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} \approx \begin{array}{c} \phi(a) \ \phi(b) \ \phi(c) \ \psi(x) \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array}$$

which implies that $\psi(x) = \phi(x)$. Thus

$$\psi \text{ is the homography } \phi \text{ for the one dimensional case.} \quad (i)$$

We move on to the case wherein P has dimension greater than 1. Let I denote $F \Delta \{p\}$ and let

$$S \equiv \{t \in P : \phi^{-1} \circ \psi(t) = t\}.$$

We first show that

$$(\forall J \subset I) (\exists x_j \in J) \quad \phi^{-1} \circ \psi(x_j) = x_j. \quad (ii)$$

Assume that (i) did not hold and that J were a set of maximal cardinality for which it did not hold. The set J could not be I since p is in I . There would exist a superset K of J cardinality one more than the cardinality of J an element q be an element of $S \cap K$ and an element r of $K \Delta J$. By 2.8.8 the meridian $\overleftrightarrow{q}, \overleftrightarrow{r}$ would intersect J at some point x . If x were not in J , then q could not be fundamental for $K \Delta \{q\}$. So x would have to be in J , which would be absurd. It follows that (ii) holds.

We now consider the family

$$\{J \subset I : J \subset S\}.$$

Assume that there were some subset J of I not in that family and choose such a subset of minimal cardinality. In view of (i) and (ii), we know that the cardinality of J would be larger than 2. From (ii) we know that there would exist an element q of $J \cap S$ and by our choice of J an element x of J not in S . We could choose a maximal proper subset K of J such that $\overleftrightarrow{p}, \overleftrightarrow{x} \cap J \not\subset K$. It would follow from 2.8.8 that the line $\overleftrightarrow{p}, \overleftrightarrow{x}$ would intersect K at some point r . Because of the minimality of I , r would have to be in S . The function $\phi^{-1} \circ \psi$ would fix r and q , whence follows by (2.3.3) that $\phi^{-1} \circ \psi[\overleftrightarrow{r}, \overleftrightarrow{q}] = \overleftrightarrow{r}, \overleftrightarrow{q}$. It also would follow from (2.3.3) that $\phi^{-1} \circ \psi[K] = K$. This would imply that $\phi^{-1} \circ \psi[\overleftrightarrow{r} \cap K] = \overleftrightarrow{r} \cap K$, which would mean $\phi^{-1} \circ \psi(r) = r$. It would follow that r would be in S . Since q is also in S , it would follow from (i) and (ii) that $\overleftrightarrow{r}, \overleftrightarrow{q}$ would be a subset of S . But x would be an element of $\overleftrightarrow{r}, \overleftrightarrow{q}$ and so x would be in S . That would be absurd. It follows that each subset J of I is a subset of S . That ϕ equals ψ is now a consequence of (2.8.6). We have now established (2).

The scalar functions of (2.9.13) are all homographic isomorphisms of meridian subsets of P onto the von Staudt meridian \mathfrak{W}_P .

(2.11) Harmonic Pairs Let M be a meridian. Let $\{a, b, u, v\}$ be a quadruplet in M . We shall say that $\{\{a, b\}, \{u, v\}\}$ is a **harmonic pair (of pairs)** if

$$\begin{array}{c} u \ b \ v \\ a \ u \ b \end{array} (v) = a. \quad (1)$$

If (1) holds

$$\begin{array}{c} u \ b \ v \\ a \ u \ b \end{array} \text{ is then is of order 4 as a group element.} \quad (2)$$

From (1) follows that $\begin{array}{c} u \ b \ v \\ a \ u \ b \end{array} \circ \begin{array}{c} u \ b \ v \\ a \ u \ b \end{array} \circ \begin{array}{c} u \ b \ v \\ a \ u \ b \end{array} \circ \begin{array}{c} u \ b \ v \\ a \ u \ b \end{array}$ agrees with the identity ι on each of the elements of the fundamental subset $\{a, u, b\}$ of M . It follows from the **uniqueness postulate** that the two homographies are identical.

Conversely, if ϕ is a homography on M such that ϕ is not an involution, that $\phi \circ \phi \circ \phi \circ \phi$ is the identity

homography ι on M , then

$$(\forall x \in M: \phi(x) \neq x) \quad \{\{x, \phi \circ \phi(x)\}, \{\phi(x), \phi \circ \phi \circ \phi(x)\}\} \text{ is a harmonic pair.} \quad (3)$$

If $\phi \circ \phi \circ \phi \circ \phi = \iota$ and we set $a \equiv x$, $u \equiv \phi(x)$, $b \equiv \phi \circ \phi(x)$ and $v \equiv \phi \circ \phi \circ \phi(x)$ it would follow that (1) would hold, which means that (3) would hold.

A second characterization is

$$\{\{a, b\}, \{u, v\}\} \text{ is a harmonic pair} \iff \begin{bmatrix} a & b \\ a & b \end{bmatrix} (u) = v. \quad (4)$$

Suppose that $\{\{a, b\}, \{u, v\}\}$ is a harmonic pair. From (1) follows that $\begin{bmatrix} a & b \\ u & v \end{bmatrix} \circ \begin{bmatrix} u & b & v \\ a & u & b \end{bmatrix}$ agrees with $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$ at a and b . Since both are involutions which fix the same two points, it follows from (2.6.4) that they are identical. Since $\begin{bmatrix} a & b \\ u & v \end{bmatrix} \circ \begin{bmatrix} u & b & v \\ a & u & b \end{bmatrix}$ sends u to v , this means that $(u) = v$. Now suppose that $\begin{bmatrix} a & b \\ a & b \end{bmatrix} (u) = v$. It follows that $\begin{bmatrix} a & b \\ u & v \end{bmatrix} \circ \begin{bmatrix} a & b \\ a & b \end{bmatrix}$ agrees with $\begin{bmatrix} u & b & v \\ a & u & b \end{bmatrix}$ at b , a and u and so, by the **uniqueness postulate**, they are identical. That $\{\{a, b\}, \{u, v\}\}$ is a harmonic pair follows from (1).

If $\{\{a, b\}, \{u, v\}\}$ is a harmonic pair, then

$$\begin{bmatrix} a & b & v \\ a & u & b \end{bmatrix} \text{ is a translation.} \quad (5)$$

By (2.6.6) we know that $\begin{bmatrix} a & b \\ a & b \end{bmatrix} \circ \begin{bmatrix} a & b \\ a & u \end{bmatrix}$ is a translation. By (4) and direct computation we know that $\begin{bmatrix} a & b \\ a & b \end{bmatrix} \circ \begin{bmatrix} a & b \\ a & u \end{bmatrix} = \begin{bmatrix} a & b & v \\ a & u & b \end{bmatrix}$. This establishes (5).

Conversely, if τ is a translation of M , p is the fixed point of τ and if x is any element of M distinct from p , then

$$\{\{p, \tau(x)\}, \{x, \tau \circ \tau(x)\}\} \text{ is a harmonic pair.} \quad (6)$$

It follows from (2.6.7) that $\tau = \begin{bmatrix} p & \tau(x) \\ p & \tau(x) \end{bmatrix} \circ \begin{bmatrix} p & \tau(x) \\ p & x \end{bmatrix}$. It follows that

$$\begin{bmatrix} p & \tau(x) \\ p & \tau(x) \end{bmatrix} (x) = \begin{bmatrix} p & \tau(x) \\ p & \tau(x) \end{bmatrix} \circ \begin{bmatrix} p & \tau(x) \\ p & x \end{bmatrix} (\tau(x)) = \tau \circ \tau(x)$$

By (4) this establishes (6).

It is sometimes the case that, given a tripleton $\{a, b, u\}$, one wants to express the element v such that $\{\{a, b\}, \{u, v\}\}$ is a harmonic pair. The solution is given by (4):

$$v = \begin{bmatrix} a & b \\ a & b \end{bmatrix} (u). \quad (7)$$

If $\{\{a, b\}, \{u, v\}\}$ is a harmonic pair and ϕ is a projective isomorphism, then

$$\{\{\phi(a), \phi(b)\}, \{\phi(u), \phi(v)\}\} \text{ is a harmonic pair.} \quad (8)$$

Since $\{\{a, b\}, \{u, v\}\}$ is a harmonic pair, there exists a homography θ which sends a to u , u to b , b to v and v to a . Since ϕ is a projective isomorphism, we know that $\phi \circ \theta \circ \phi^{-1}$ is a homography. Evidently this homography sends $\phi(a)$ to $\phi(u)$, $\phi(u)$ to $\phi(b)$, $\phi(b)$ to $\phi(v)$ and $\phi(v)$ to $\phi(a)$. Consequently, (8) holds

(2.12) Projections and Perspectivities Let P be a finite dimensional projective space of dimension greater than one, and let \mathcal{P} be its homography group of permutations. If S is a maximal proper subspace, we say that S is a **co-point**.

Let p be a point in P and B a co-point not containing p . It follows from 2.8.8 that, for any point x distinct from p , the meridian $\overleftrightarrow{x, p}$ intersects B at one point. We shall denote this point by

$$\pi_{(p;B)}(x) . \quad (1)$$

The function $\pi_{(p;B)}$ thus induced will be called the **projection from p onto B**. If N is a meridian neither comprehended by B nor through p, the restriction of $\pi_{(p;B)}$ to N sends N onto a meridian within B: this function is called a **perspectivity**. Then

$$\text{each perspectivity is a homographic meridian isomorphism.} \quad (2)$$

Let $\phi|N \hookrightarrow M$ be the restriction of a projection $\pi_{(p;B)}$ to a meridian N comprehended by P which neither contains p nor is comprehended by B. The sets $\{p\}$, N and M are all comprehended by 2-dimensional subspace T of P. From 2.8.8 we know that N and M intersect at a single point q. Let $\{c,d\}$ be a doubleton comprehended by N and not containing q. Let x be the intersection point of M with $\overleftrightarrow{b,c}$ and y the intersection point of M with $\overleftrightarrow{b,d}$. The set $\{x,y,c,d\}$ is evidently fundamental. By the **fundamental postulate** there exists an element ψ of \mathcal{P} such that

$$\psi(c) = x, \quad \psi(x) = c, \quad \psi(d) = y, \quad \text{and} \quad \psi(y) = d. \quad (i)$$

Since ψ interchanges c with x and since $\overleftrightarrow{c,x}$ is just $\overleftrightarrow{p,x}$, ψ leaves the line $\overleftrightarrow{p,x}$ invariant. Since ψ interchanges d with y and since $\overleftrightarrow{d,y}$ is just $\overleftrightarrow{p,y}$, ψ leaves the line $\overleftrightarrow{p,y}$ invariant. It follows that the intersection of the lines $\overleftrightarrow{p,x}$ and $\overleftrightarrow{p,y}$ is left invariant:

$$\psi(p) = p. \quad (ii)$$

The meridian $\overleftrightarrow{c,d}$ is sent by ψ onto the line $\overleftrightarrow{x,y}$ and *vice-versa*: that is, ψ interchanges N and M. Thus the intersection point is fixed:

$$\psi(q) = q. \quad (iii)$$

In view of (ii) and the fact that the points c and x are interchanged on $\overleftrightarrow{c,x}$, it follows from (2.6.3) that property (2.1.4) that there is precisely one point o $\overleftrightarrow{p,x}$ distinct from p such that

$$\psi(o) = o. \quad (iv)$$

It follows from (iii) and (iv) that the line $\overleftrightarrow{q,o}$ is sent onto itself by ψ and so the intersection r of $\overleftrightarrow{q,o}$ with $\overleftrightarrow{p,y}$ is sent to itself:

$$\psi(r) = r. \quad (v)$$

From (iii), (iv) and (v) follows that ψ agrees with the identity function on the fundamental set $\{q,o,r\}$, and so the **uniqueness postulate** implies that

$$(\forall z \in \overleftrightarrow{q,o}) \quad \psi(z) = z. \quad (vi)$$

Now let t be any element of N. The meridian $\overleftrightarrow{p,t}$ intersects the meridian $\overleftrightarrow{q,o}$ at some point u and intersects the meridian M at some point v. From (vi) follows that $\psi(u) = u$. Thus $\overleftrightarrow{p,u}$ is sent to itself by ψ and $\overleftrightarrow{p,t} = \overleftrightarrow{p,v} = \overleftrightarrow{p,t}$. Since ψ interchanges the lines N and M, it follows that the intersection point v of $\overleftrightarrow{p,u}$ with M is interchanged by ψ with the intersection point t of $\overleftrightarrow{p,u}$ with N. We have

$$\psi(t) = v = \pi_{(p;B)}(t) .$$

We have established that (2) holds.

(2.13) Libras A permutation group is a family of permutations of a set closed under compositions and containing an identity. There are some applications however where one has such a family of permutations, but without containing an identity. We recall that a projective group on a meridian is generated by its involutions (*cf.* (2.7)). When constructing the fields of a meridian we made use of families of meridians which either interchanged two fixed points, or which kept one point fixed. These families were closed under composition (*cf.* (2.6.9)) but which did not contain the identity function. In the sequel we shall have to deal with families similar to this, but whose common domain is not the same as their common range. This suggests we consider a construct a little more general than a group.

By a **transformation libra** we shall mean a family \mathcal{F} of transformations with a common domain and a common range such that

$$(\forall \{\alpha, \beta, \gamma\} \subset \mathcal{F}) \quad \gamma \circ \beta^{-1} \circ \alpha \in \mathcal{F}. \quad (1)$$

It is at times useful to introduce the following notation:

$$(\forall \{\alpha, \beta, \gamma\} \subset \mathcal{F}) \quad \llbracket \gamma, \beta, \gamma \rrbracket \equiv \gamma \circ \beta^{-1} \circ \alpha \in \mathcal{F}. \quad (2)$$

Just as with a permutation group, which has an abstract form (abstract group), there is also an abstract **libra**: a set L along with a ternary operation $\llbracket \cdot \cdot \cdot \rrbracket : L \times L \times L \ni [x, y, z] \mapsto [x, y, z] \in L$ such that

$$(\forall \{x, y\} \subset L) \quad \llbracket x, y, y \rrbracket = \llbracket y, y, x \rrbracket = x, \quad (3)$$

and

$$(\forall \{v, y, x, w, z\} \subset L) \quad \llbracket \llbracket w, v, x \rrbracket, y, z \rrbracket = \llbracket w, v, \llbracket x, y, z \rrbracket \rrbracket. \quad (4)$$

It follows from (3) and (4) that the equality

$$\llbracket v, \llbracket w, x, y \rrbracket, z \rrbracket = \llbracket \llbracket v, y, x \rrbracket, w, z \rrbracket \quad (5)$$

holds as well.

We have

$$\begin{aligned} v &\stackrel{\text{by (3)}}{=} \llbracket v, w, w \rrbracket \stackrel{\text{by (3)}}{=} \llbracket v, w, \llbracket x, x, w \rrbracket \rrbracket \stackrel{\text{by (3)}}{=} \llbracket v, w, \llbracket x, y, y \rrbracket, x, w \rrbracket \stackrel{\text{by (4)}}{=} \\ &\llbracket \llbracket v, w, \llbracket x, y, y \rrbracket \rrbracket, x, w \rrbracket \stackrel{\text{by (4)}}{=} \llbracket \llbracket \llbracket v, w, x \rrbracket, y, y \rrbracket, x, w \rrbracket \stackrel{\text{by (4)}}{=} \llbracket \llbracket v, w, x \rrbracket, y, \llbracket y, x, w \rrbracket \rrbracket \end{aligned}$$

whence follows that

$$\begin{aligned} \llbracket v, \llbracket y, x, w \rrbracket, z \rrbracket &= \llbracket \llbracket \llbracket v, w, x \rrbracket, y, \llbracket y, x, w \rrbracket \rrbracket, \llbracket y, x, w \rrbracket, z \rrbracket \stackrel{\text{by (4)}}{=} \\ &\llbracket \llbracket v, w, x \rrbracket, y, \llbracket \llbracket y, x, w \rrbracket, \llbracket y, x, w \rrbracket, z \rrbracket \rrbracket \stackrel{\text{by (3)}}{=} \llbracket \llbracket v, w, x \rrbracket, y, z \rrbracket. \end{aligned}$$

A bijection from one libra onto another is said to be a **libra isomorphism** if it preserves the ternary libra operator.

A libra is said to be **abelian** provided that

$$(\forall \{x, y, z\} \subset L) \quad \llbracket x, y, z \rrbracket = \llbracket z, y, x \rrbracket. \quad (6)$$

A group G with binary operation \cdot is a libra relative to the ternary operation

$$\llbracket x, y, z \rrbracket \equiv x \cdot y^{-1} \cdot z. \quad (7)$$

Conversely, a libra L , relative to any element e of L , is a group relative to the operation

$$(\forall \{x, y\} \subset L) \quad x \cdot y \equiv \llbracket x, e, y \rrbracket. \quad (8)$$

In this case we speak of the **libra group with identity** e .

Evidently a libra is abelian if, and only if, any one of the groups associated with it is abelian. In this case, all the groups associated with the libra are abelian.

(2.14) Involution Libras Let $\{a, b\}$ be a subset of a meridian M and let \mathcal{M} be the homography group of M . We define

$$\mathcal{M}_{\{a, b\}} \equiv \{\phi \in \mathcal{M} : \phi \circ \phi = \iota \text{ and } \phi(a) = b\}. \quad (1)$$

Then

$$\mathcal{M}_{\{a, b\}} \text{ is an abelian libra.} \quad (2)$$

If a and b are distinct, it is evident that $\mathcal{M}_{\{a, b\}}$ is a libra. If they are identical, it follows from (2.6.9). That the meridian is abelian follows from the fact that we are dealing with involutions.

(2.15) Affine Space A maximal proper subspace of a finite dimensional projective space is called a **co-point**. Let O be a co-point and let A be its complement $P\Delta O$. We say that A is the **affine space associated with** O .

If $\{a, c\}$ is a doubleton of A , then the meridian $\overleftrightarrow{a, c}$ intersects the co-point O in a single point

$$\infty_O(a, c). \quad (1)$$

We define the **midpoint between** a and c to be

$$m \equiv \boxed{\begin{smallmatrix} a & c \\ a & c \end{smallmatrix}}(\infty_O(a, c)). \quad (2)$$

Thus the midpoint is the unique element m of A such that $\{a, c\}$ and $\{m, \infty_O(a, c)\}$ are harmonic pairs. The midpoint between a singleton a and itself is defined to be a .

If b is another point of A distinct from the midpoint m between a and c , then the **affine libra product**

$$\lfloor a, b, c \rfloor_A \quad (3)$$

is defined to be

$$\boxed{\begin{smallmatrix} b & m \\ b & m \end{smallmatrix}}(\infty_O(b, m)). \quad (4)$$

If b is identical with m , it is defined to be just b . Thus, $\lfloor a, b, c \rfloor_A$ may be regarded as the element of A such that the points a , b , c and $\lfloor a, b, c \rfloor_A$ form the vertices of a parallelogram.

Suppose that S is any co-point of P which does not contain p . Then the projection $\pi_{(p;S)}$ from p onto S preserves the ternary operation defined by (3):

$$(\forall \{a, b, c\} \subset A) \quad \pi_{(p;S)}(\lfloor a, b, c \rfloor) = \lfloor \pi_{(p;S)}(a), \pi_{(p;S)}(b), \pi_{(p;S)}(c) \rfloor. \quad (5)$$

Let m be as in (2). We know from (2.12.2) that the restriction μ of $\pi_{(p;S)}$ to $\overleftrightarrow{a, c}$ is a meridian homographic isomorphism onto the meridian $\overleftrightarrow{\pi_{(p;S)}(a), \pi_{(p;S)}(c)}$. Since by (2.11.8) $\pi_{(p;S)}$ preserves harmonic pairs, if m is the midpoint of a and c in A , it follows that

$$\pi_{(p;S)}(m) \text{ is the midpoint of } \overleftrightarrow{\pi_{(p;S)}(a), \pi_{(p;S)}(c)}. \quad (i)$$

We know from (2.12.2) that the restriction ν of $\pi_{(p;S)}$ to $\overleftrightarrow{b, m}$ is a meridian homographic isomorphism onto the meridian $\overleftrightarrow{\pi_{(p;S)}(b), \pi_{(p;S)}(m)}$. Since by (2.11.8) $\pi_{(p;S)}$ preserves harmonic pairs, it follows from (i) that

$$\pi_{(p;S)}(\pi_{(p;S)}(m)) \text{ is the midpoint of } \overleftrightarrow{\pi_{(p;S)}(b), \pi_{(p;S)}(\infty_O(b, m))}. \quad (ii)$$

From (i) and (ii) follows that (5) holds.

We may deduce in part from this that, relative to (3),

$$A \text{ is an abelian libra.} \quad (6)$$

It is evident from the definition that the operator (3) is abelian. We first consider the case where P is one dimensional. In this case O is a point which we shall denote ∞ . Let $\{a, o, c\}$ be any tripton distinct from ∞ . We know from (2.6.10) that A is a group with identity o relative to the binary operation defined by $a+c \equiv \begin{bmatrix} \infty & a \\ \infty & c \end{bmatrix} (o)$. Let $m \equiv \begin{bmatrix} a & c \\ a & c \end{bmatrix} (\infty)$. From (2.11.4) we know that $\{\{a, c\}, \{m, \infty\}\}$ is a harmonic pair. It follows that $\begin{bmatrix} \infty & m \\ \infty & m \end{bmatrix}$ interchanges a and c . Thus $\begin{bmatrix} \infty & a \\ \infty & c \end{bmatrix}$ and $\begin{bmatrix} \infty & m \\ \infty & m \end{bmatrix}$ agree on the fundamental set $\{a, c, \infty\}$. It follows from the **uniqueness postulate** that they must be equal. Consequently

$$\lfloor a, o, c \rfloor = a+c. \quad (i)$$

By (2.6.10) we know that A is a group with identity o , whence follows that A is the corresponding group libra. Let n be a positive integer and suppose that we have shown that (2.13.4) holds for A for all dimensions of P less than n . Suppose that P is of dimension n and let $\{v, w, x, y, z\}$ be a subset of A . Assume that

$$\lfloor \lfloor v, w, x \rfloor, y, z \rfloor \neq \lfloor v, w, \lfloor x, y, z \rfloor \rfloor. \quad (ii)$$

Then we could find a proper subspace S of P containing both $\lfloor \lfloor v, w, x \rfloor, y, z \rfloor$ and $\lfloor v, w, \lfloor x, y, z \rfloor \rfloor$. It follows from (5) that

$$\lfloor \lfloor \pi_{(p;S)}(v), \pi_{(p;S)}(w), \pi_{(p;S)}(x) \rfloor, \pi_{(p;S)}(y), \pi_{(p;S)}(z) \rfloor \stackrel{\text{by (5)}}{=} \pi_{(p;S)}(\lfloor \lfloor v, w, x \rfloor, y, z \rfloor) = \lfloor \lfloor v, w, x \rfloor, y, z \rfloor \neq$$

by (ii)

$$\lfloor v, w, \lfloor x, y, z \rfloor \rfloor = \pi_{(p;S)}(\lfloor v, w, \lfloor x, y, z \rfloor \rfloor) \stackrel{\text{by (5)}}{=} \lfloor \pi_{(p;S)}(v), \pi_{(p;S)}(w), \lfloor \pi_{(p;S)}(x), \pi_{(p;S)}(y), \pi_{(p;S)}(z) \rfloor \rfloor$$

which were absurd by our induction hypothesis.

Let θ be an element of \mathcal{P} which leaves O invariant. Then, for all $\{a, b, c\}$,

$$\theta(\lfloor a, b, c \rfloor) = \lfloor \theta(a), \theta(b), \theta(c) \rfloor. \quad (7)$$

This follows from (2.11.8).

(2.16) Lemma For our treatment of linear space below, we shall require the following equalities for elements a, b, c, d and e of a meridian:

$$\begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} = \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} \circ \begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} \quad (1)$$

and

$$\begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} (e) = \begin{bmatrix} a & b & e \\ a & b & c \end{bmatrix} (d) \quad (2)$$

Direct computation shows that

$$\begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} = \begin{bmatrix} a & d \\ b & c \end{bmatrix} \circ \begin{bmatrix} a & c \\ b & c \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} = \begin{bmatrix} a & c \\ b & e \end{bmatrix} \circ \begin{bmatrix} a & e \\ b & e \end{bmatrix}. \quad (i)$$

By (2.14.2) we know that $\mathcal{M}_{\{a, b\}}$ is an abelian libra. Thus

$$\begin{aligned} \begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} &\stackrel{\text{by (i)}}{=} \begin{bmatrix} a & d \\ b & c \end{bmatrix} \circ \begin{bmatrix} a & c \\ b & c \end{bmatrix} \circ \begin{bmatrix} a & c \\ b & e \end{bmatrix} \circ \begin{bmatrix} a & e \\ b & e \end{bmatrix} = \llbracket \begin{bmatrix} a & d \\ b & c \end{bmatrix}, \begin{bmatrix} a & c \\ b & c \end{bmatrix}, \begin{bmatrix} a & c \\ b & e \end{bmatrix} \rrbracket \circ \begin{bmatrix} a & e \\ b & e \end{bmatrix} = \llbracket \begin{bmatrix} a & c \\ b & e \end{bmatrix}, \begin{bmatrix} a & c \\ b & c \end{bmatrix}, \begin{bmatrix} a & d \\ b & c \end{bmatrix} \rrbracket \circ \begin{bmatrix} a & e \\ b & e \end{bmatrix} \\ &= \begin{bmatrix} a & c \\ b & e \end{bmatrix} \circ \llbracket \begin{bmatrix} a & c \\ b & c \end{bmatrix}, \begin{bmatrix} a & d \\ b & c \end{bmatrix}, \begin{bmatrix} a & e \\ b & e \end{bmatrix} \rrbracket = \begin{bmatrix} a & c \\ b & e \end{bmatrix} \circ \llbracket \begin{bmatrix} a & e \\ b & e \end{bmatrix}, \begin{bmatrix} a & d \\ b & c \end{bmatrix}, \begin{bmatrix} a & c \\ b & c \end{bmatrix} \rrbracket = \begin{bmatrix} a & c \\ b & e \end{bmatrix} \circ \begin{bmatrix} a & e \\ b & e \end{bmatrix} \circ \begin{bmatrix} a & d \\ b & c \end{bmatrix} \circ \begin{bmatrix} a & c \\ b & c \end{bmatrix} \stackrel{\text{by (i)}}{=} \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} \circ \begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} \end{aligned}$$

which yields (1).

Noting that $\begin{bmatrix} a & b & e \\ a & b & c \end{bmatrix}^{-1} = \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix}$, we have

$$\begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} (e) = \begin{bmatrix} a & b & e \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} \circ \begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} (e) \stackrel{\text{by (1)}}{=} \begin{bmatrix} a & b & e \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} a & b & d \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} a & b & c \\ a & b & e \end{bmatrix} (e) = \begin{bmatrix} a & b & e \\ a & b & c \end{bmatrix} (d)$$

which yields (2).

(2.17) Projective Linear Space Let P be a finite dimensional projective space, O a co-point of O , A the set-theoretic complement of O and o an element of A . We know from (2.15.6) that A is an affine space and a libra. The group group associated with o is called a **linear space**. The group operation of (2.13.8) we shall denote by $+$: thus

$$(\forall \{a,b\} \subset A) \quad a+b \equiv [a,o,b]. \quad (1)$$

We recall the Von Staudt meridian \mathfrak{W}_P , the special elements ∞ , $\mathbf{0}$ and $\mathbf{1}$ of \mathfrak{W}_P , and the projective field \mathfrak{F}_P of \mathfrak{W}_P with ordered fundamental set $[\infty, \mathbf{0}, \mathbf{1}]$. For any scalar r in \mathfrak{F}_P and any element x of P , we define scalar multiplication as in (2.9.21):

$$r \bullet x \equiv \begin{cases} \mathbf{0}, & \text{if } r = \mathbf{0} \text{ or } x = \mathbf{0}; \\ \begin{bmatrix} \infty & \mathbf{0} & x \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} (r), & \text{for } x \in A, r \neq \mathbf{0} \text{ and } x \neq \mathbf{0}; \\ x, & \text{for } x \in O \text{ and } r \neq \mathbf{0}. \end{cases} \quad (2)$$

For any non-zero scalar r , the function

$$r \bullet | P \ni x \mapsto r \bullet x \in P \text{ is a homography.} \quad (3)$$

Let M be any meridian comprehended by P containing $\mathbf{0}$. By (2.8.8) the meridian M intersects O at a single point which we shall denote by ∞ . Let l be any element of $(M \triangle \{\mathbf{0}, \infty\})$. There is a unique element r of M such that $\begin{bmatrix} \infty & \mathbf{0} & l & r \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix} \in r$. For each x in M

$$r \bullet x \stackrel{\text{by (3)}}{=} \begin{bmatrix} \infty & \mathbf{0} & x \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} (r) = \begin{bmatrix} \infty & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{0} & l \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} (r) \stackrel{\text{by (3)}}{=} \begin{bmatrix} \infty & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix} (r \bullet l) \quad (i)$$

$$\begin{bmatrix} \infty & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix} (r \bullet l) \stackrel{(2.9.21)}{=} \begin{bmatrix} \infty & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix} (r) \stackrel{\text{by (2.16.2)}}{=} \begin{bmatrix} \infty & \mathbf{0} & r \\ \infty & \mathbf{0} & l \end{bmatrix} (x)$$

It follows that (4) holds when P is one dimensional.

We now presume that P has dimension greater than 1. Let B be a maximal independent subset of O . It follows from (2.8.8) that $(B \cup \{\mathbf{0}\})$ is a maximal independent subset of P . We know from (2.8.7) that $\overline{B \cup \{\mathbf{0}\}}$ is non-void. Let l be an element of $\overline{B \cup \{\mathbf{0}\}}$. Thus $(B \cup \{\mathbf{0}, l\})$ is a fundamental set. Evidently $(B \cup \{\mathbf{0}, r \bullet l\})$ is also fundamental. It follows from the **fundamental postulate** that there exists ϕ in \mathcal{P} such that

$$\phi(l) = r \bullet l \quad \text{and} \quad (\forall x \in (B \cup \{\mathbf{0}\})) \quad \phi(x) = x. \quad (ii)$$

We shall show that

$$(\forall x \in A) \quad \phi(x) = r \bullet x. \quad (iii)$$

Let now M be $\overleftrightarrow{\mathbf{0}, l}$ and let r in M be such that $\begin{bmatrix} \infty & \mathbf{0} & l & r \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix} \in r$. Since ϕ agrees with $\begin{bmatrix} \infty & \mathbf{0} & r \\ \infty & \mathbf{0} & l \end{bmatrix}$ on $\mathbf{0}, l$ and ∞ , it follows from the **uniqueness postulate** that they agree on M . Consequently, in view of (i), we know that (iii) holds for all x in M . Suppose that x is not in M . Choose a co-point S containing $\mathbf{0}$ and x but not l . Let p be the point where $\overleftrightarrow{x, l}$ intersects S . It follows from (2.12.2) that the restriction μ to M of $\pi_{(p;S)}$ is a meridian isomorphism onto $\overleftrightarrow{\mathbf{0}, x}$. In fact, if we denote by w the intersection point of $\overleftrightarrow{\mathbf{0}, x}$ with S , we have

$$\mu = \begin{bmatrix} w & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix}. \quad (iv)$$

It follows from (ii) that ϕ fixes both w and $\mathbf{0}$, whence follows that ϕ leaves $\overleftrightarrow{\mathbf{0}, w}$ invariant. Consequently the intersection point x of the meridians $\overleftrightarrow{v, l}$ and $\overleftrightarrow{\mathbf{0}, w}$ is mapped by ϕ to the intersection point of the meridians $\overleftrightarrow{v, r}$ and $\overleftrightarrow{\mathbf{0}, w}$. This intersection point is just $\pi_{(p;S)}(r)$: that is,

$$\phi(x) = \pi_{(p;S)}(r) \stackrel{\text{by (iv)}}{=} \begin{bmatrix} w & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix} (r). \quad (v)$$

Since $\begin{bmatrix} \infty & \mathbf{0} & l & r \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix}$ is in r , it follows that $\begin{bmatrix} w & \mathbf{0} & x \\ \infty & \mathbf{0} & l \end{bmatrix} \circ \begin{bmatrix} \infty & \mathbf{0} & l & r \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix}$ is in r as well. By (v) this last is just $\begin{bmatrix} w & \mathbf{0} & x & \phi(r) \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \end{bmatrix}$. It follows from (2.9.21) that (iii) holds for x .

Let r and s be elements of \mathfrak{F}_P and let x be an element of A . Then

$$r \bullet (s \bullet x) = (r \bullet s) \bullet x. \quad (4)$$

We may presume that x is not o and let w be the intersection of $\overleftrightarrow{o, \tilde{w}}$ with O . Let r and s be the elements of $\overleftrightarrow{o, \tilde{w}}$ such that

$$\begin{array}{c} w \ o \ l \ r \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} \in r \quad \text{and} \quad \begin{array}{c} w \ o \ l \ s \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} \in s. \quad (i)$$

We have

$$r \bullet (s \bullet x) \stackrel{\text{by (2)}}{=} \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (r \bullet s) \stackrel{\text{by (2.9.19)}}{=} \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (r) \cdot \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (s) \stackrel{\text{by (2.9.20)}}{=} r \bullet x \bullet s \bullet x$$

If $\mathbf{1}$ is the multiplicative identity for \mathfrak{W}_P and x is in $(A \Delta \{o\})$, then

$$\mathbf{1} \bullet x = x. \quad (5)$$

Let w denote the intersection point of $\overleftrightarrow{o, \tilde{x}}$ and O . It follows from (2.9.12) that $\begin{array}{c} w \ o \ x \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array}$ is in $\mathbf{1}$, so

$$\mathbf{1} \bullet x \stackrel{\text{by (2)}}{=} \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (r \bullet s)$$

Furthermore

$$(r+s) \bullet x = (r \bullet x) + (s \bullet x). \quad (6)$$

We have

$$(r+s) \bullet x \stackrel{\text{by (2)}}{=} \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (r+s) \stackrel{\text{by (2.9.19)}}{=} \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (r) + \begin{array}{c} w \ o \ x \\ \heartsuit \ \spadesuit \ \clubsuit \ \diamondsuit \end{array} (s) \stackrel{\text{by (2)}}{=} (r \bullet x) + (s \bullet x).$$

Finally, for y in A also distinct from o ,

$$r \bullet (x+y) = (r \bullet x) + (r \bullet y). \quad (7)$$

We have

$$r \bullet (x+y) \stackrel{\text{by (1)}}{=} r \bullet [x, o, y] \stackrel{\text{by (3) and (2.15.7)}}{=} [r \bullet x, r \bullet o, r \bullet y] \stackrel{\text{by (1)}}{=} (r \bullet x) + (r \bullet y).$$

Section 3. Examples

(3.1) Field Meridians If F is any field of characteristic different than 2, one can attach an additional point to form a set M and use the formulae of (2.6.11) to obtain the permutation group of homographies. When the field is the field of real numbers, we shall speak of **the real meridian**, and any meridian isomorphic to the real meridian may be referred to as **a real meridian**. When the field is the field of complex numbers, we shall speak of **the complex meridian**, and any meridian isomorphic to the complex meridian may be referred to as **a complex meridian**.

On the complex meridian, the involution of complex conjugation evidently is a homography, but it is a meridian isomorphism.

(3.2) Circle Meridian Let C be a circle in a plane. Each point p of the plane not on the circle projects the circle onto itself and so defines a self-inverse transformation of the circle. Given any line in the plane, the set of lines parallel to it also defines a self-inverse transformation of C . We shall call these functions the **planar involutions of the circle** C . The composition of two planar involutions will be called a **planar homography**.

One can show that

$$\text{each planar involution is a planar homography.} \tag{1}$$

Furthermore,

$$\text{each homography which is an involution is a planar involution} \tag{2}$$

and

$$\text{each circle meridian is a real meridian.} \tag{3}$$

(3.3) Spherical Meridian Let S be a sphere in 3-dimensional Euclidian space. Each straight line L which intersects at least two points of S induces a self-inverse function ϕ on S . If the line L is a diameter, each point x on S is on precisely one line through and orthogonal to L and so intersects S at another point $\phi(x)$. If the line L is not a diameter, there is exactly one line L' which does not intersect S which is the intersection of the two planes tangent of S at the points through which L intersects S . If x is any point on S , there is just one line K which contains x and which intersects both L and L' . The other point through which K pierces S is the value $\phi(x)$. These involutions ϕ , one for each L , will be called the **spatial involutions of the sphere**.

Any function on S which is the composition of two spatial involutions will be called a **spatial homography of the sphere**. The family of all spatial homographies of the sphere constitutes a projective permutation group relative to which S is a meridian. We shall call it a **sphere meridian**.

One can show that

$$\text{each spatial involution is a spatial homography.} \tag{1}$$

Furthermore,

$$\text{each homography which is an involution is a planar involution} \tag{2}$$

and

$$\text{each spatial meridian is a complex meridian.} \tag{3}$$

Each point p of Euclidian space projects S onto itself and so defines a self-inverse function on S . Such a function evidently is not a spatial involution and not a spatial homography.

Acknowledgement The author is grateful to the Institute of Information Sciences at Academia Sinica in Taipei for use of their facilities in preparing the present manuscript.

Bibliography

- [1] Felix Klein, Vergleichende Betrachtungen über neuere geometrische Forschungen, A. Deichert, Erlangen, 1872 (Gesammelte mathematische Abhandlungen, Springer-Verlag, Berlin, Heidelberg, New York, 1973, 460497).
- [2] Felix Klein, Vergleichende Betrachtungen der neuere geometrische Forschungen, Mathematische Annalen, 43 (1893) pp. 63-100.
- [3] Abraham Seidenberg, Lectures in Projective Geometry, Princeton, D. Van Nostrand Company 1962.
- [4] Otto Shreier and Emanuel Sperner, Projective Geometry, New York, Chelsea Publishing Company 1961.
- [5] Jacques Tits, Generalisation des groupes projectifs bases sur la notion de transitivite, Mem. Acad. Roy. Belg. 27 (1952), 115 p.
- [6] Karl von Staudt, Beiträge der Geometrie der Lage, Heft 2, 1857.

Kelly McKennon, 775 SE Edge Knoll Drive, Pullman WA 99163, USA
KellyMack@ProtonMail.com