



中央研究院
資訊科學研究所

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

TR-IIS-23-002

Projective Space as a Set with a Group of Permutations: A Preliminary Presentation

Kelly McKennon



May 11, 2023

||

Technical Report No. TR-IIS-23-002

<https://www.iis.sinica.edu.tw/zh/page/Library/TechReport/2023.html>

**Projective Space as a Set with a Group of Permutations:
A Preliminary Presentation**

(by Kelly McKennon, May 2023)

Introduction

Projective space is a place where parallel lines intersect and where there is a perfect duality between minimal and maximal subspaces. It is a place where the infinite exists and where one can see how the infinite affects behavior in the finite. It is a place where many seeming anomalies, when regarded from the perspective of the finite, disappear.

The direct way to define a projective space is to begin with a linear space L , and for each family of parallel lines in that linear space, to attach a point “at infinity” where all the lines intersect. This is intuitive, but it implies that the set of all points at infinity, which is a maximal proper subspace, or “hyperplane”, is somehow different than other hyperplanes: and it really is not. It also makes describing the projective group somewhat awkward.

The elegant way to define a projective space, which does not single out any hyperplane as being special, is to take a linear space S one dimension greater than the projective space and adopt each line through the origin of this linear space as an element of the projective space. The linear isomorphisms of S of course send the lines through the origin of S to lines through the origin. Thus each such isomorphism induces a bijection on the abstract projective space, and two isomorphisms induce the same bijection if, and only if, they are non-zero scalar multiples of one another. The induced mappings are called the “homographies” of the projective space.

While elegant, and technically correct, this method is not so intuitive as the direct method. Furthermore, it involves the concepts of “linear space” and “field”, which in some sense are more specialized and really unnecessary. It seems to run counter to the philosophy of eliminating the superfluous.

A third method, known as the “synthetic” approach, is to begin with a family of subsets of a set, known as “lines” and assign to these lines certain requirements. Its advantage is that it lends a geometric perspective which agrees with natural observation. A disadvantage is that the special cases of one and two dimensions must be handled separately.

In 1872 the celebrated mathematician Felix Klein, then a young man working at the University of Erlangen-Nürnberg, published an article “*Vergleichende Betrachtungen ber neuere geometrische Forschungen*”, in which he suggested that the various types of geometries then under investigation could be organized with reference to the specific groups of permutations which preserved their characteristic structures. This idea had much influence on subsequent mathematics, in more fields than just geometry, and became known as the “Erlanger Programm”. At the time, Klein felt that the groups associated with the majority of the important geometries were subgroups of the group of homographies of projective space.

In the present paper we consider a set on which a group P of permutations acts, and provide a short list of postulates necessary and sufficient for P to be the group of homographies of a projective space.

1. Projective Space

1.1 Notation and Terminology A **singleton** is a set with precisely one member, a **doubleton** a set with precisely two members, etc. We shall say that an element of a set S is **in** S , but that a subset of S is **comprehended** by S or **of** S . Thus a doubleton, the members of which are in S , is comprehended by S .

For two sets A and B , we write $A\Delta B$ for their symmetric difference: that is, the set of all elements of $A\cup B$ which are not in $A\cap B$. In particular, when B is a subset of A , $A\Delta B$ is the set complement of B in A .

1.2 Definition Let P be a non-void set and P a non-void group of permutations of P . If P is a singleton, then P is also a singleton, the element of which is the identity function ι . We speak here of the **trivial projective space and group**.

Suppose that P has cardinality greater than one. For any doubleton $\{a,b\}$ of P , we denote by $\overleftrightarrow{a,b}$ the set of all $x\in P$ such that, when ever $\phi\in P$ is such that $\phi(a)=b$ and $\phi(b)=a$, then

$$(\exists y\in P) \quad \{x,y\}=\{\phi(x),\phi(y)\}. \quad (1.2.1)$$

We shall say that $\overleftrightarrow{a,b}$ is the **line determined by a and b**.

A subset S of P will be said to be **closed** provided that, for each doubleton $\{a,b\}$ of S ,

$$\overleftrightarrow{a,b}\subset S. \quad (1.2.2)$$

The intersection of closed sets is closed and P itself is closed. Consequently each set is comprised by a unique minimal closed set: the intersection of all closed subsets of P which comprehend S . We shall denote that set by

$$[S] \quad (1.2.3)$$

and call it the **span** of S .

We shall say that an element α of P is **unique** on a subset S of P provided that

$$(\forall \beta\in P : \beta|_S=\alpha|_S) \quad \beta|_{[S]}=\alpha|_{[S]}. \quad (1.2.4)$$

A subset S of P will be said to be **independent** provided that no singleton of it is comprehended by the span of the complement of that singleton in S .

A subset S of P will be said to be **fundamental** if

$$(\forall x\in S) \quad x\in[S\Delta\{x}] \quad (1.2.5)$$

and

$$(\forall D\subset S \text{ a doubleton}) \quad D\cap[S\Delta D] = \emptyset. \quad (1.2.6)$$

A fundamental set is often called a **frame**.

If P is non-trivial, we shall say that P is a **projective group** and that P is a **projective space** provided that the following two requirements are fulfilled:

Axiom I each line is closed and has some point other than a and b (1.2.7)

and, whenever θ is a bijection from one finite fundamental set F onto another H , then

Axiom II $(\exists \phi\in P \text{ unique on } F) \quad \phi|_F=\theta$. (1.2.8)

Suppose that there exists a maximal cardinality for fundamental subsets of P and that n is the integer such that $n+2$ equals that cardinality. We shall say that P is **finite dimensional** and that n is the **dimension** of P .

1.3 Notation Let I be an independent set. We shall adopt the notation

$$I^\circ \equiv \{x\in[I] : (\forall S\subset I \text{ proper}) \quad x\notin[S].\} \quad (1.3.1)$$

1.4 Lemma Let P be projective group of transformations of a projective space P . Let $\{a,b\}$ be a doubleton of P and let ϕ be an element of P . Then

$$\{\phi(x) : x\in\overleftrightarrow{a,b}\} = \overleftrightarrow{\phi(a),\phi(b)}. \quad (1.4.1)$$

Proof. If x is any element of $\overleftarrow{a,b}$, then there exists $y \in P \Delta \{x\}$ such that, for each $\theta \in P$ such that $\theta(a)=b$ and $\theta(b)=a$, $\{x,y\}=\{\theta(x),\theta(y)\}$. Suppose that $\rho \in P$ is such that $\rho(\phi(a))=\phi(b)$ and $\rho(\phi(b))=\phi(a)$. Setting $\sigma \equiv \phi^{-1} \circ \rho \circ \phi$, we have

$$\sigma(a)=\phi^{-1} \circ \rho(\phi(a))=\phi^{-1}(\phi(b))=b \text{ and, similarly, } \sigma(b)=a.$$

Consequently there exists y in P such that $\{x,y\}=\{\sigma(x),\sigma(y)\}$. Since

$$\rho(\phi(y))=\phi \circ \phi^{-1} \circ \phi(y)=\phi(\sigma(y)) \text{ and, similarly } \rho(\phi(x))=\phi \circ \phi^{-1} \circ \phi(x)=\phi(\sigma(x)),$$

it follows that

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

We have shown that

$$\{\phi(x) : x \in \overleftarrow{a,b}\} \subset \overleftarrow{\phi(a),\phi(b)}. \quad (1.4.2)$$

Let u be any element of $\overleftarrow{\phi(a),\phi(b)}$ and define w to be the element of P such that $\phi(w)=u$. We shall show that w is in $\overleftarrow{a,b}$, which will establish the reverse inclusion of (2.4.2), whence will follow that Lemma (2.4) holds. There exists v in P such that, for each θ which interchanges $\phi(a)$ and $\phi(b)$, $\{u,v\}=\{\theta(u),\theta(v)\}$. Let γ be any element of P which interchanges a and b , and define τ to be $\phi \circ \gamma \circ \phi^{-1}$. We have

$$\tau(\phi(a))=\phi \circ \gamma(a)=\phi(b) \text{ and, similarly, } \tau(\phi(b))=\phi \circ \gamma(b)=\phi(a).$$

Since u is in $\overleftarrow{\phi(a),\phi(b)}$, it follows that there exists v in P such that $\{u,v\}=\{\tau(u),\tau(v)\}$. Let z be such that $\phi(z)=v$. We have

$$\{w,z\}=\{\phi^{-1}(u),\phi^{-1}(v)\}=\{\phi^{-1}(\tau(u)),\phi^{-1}(\tau(v))\}=\{\gamma(w),\gamma(z)\}.$$

It follows that w is in $\overleftarrow{a,b}$. QED

1.5 Theorem Let P be projective group of transformations of a projective space P . Let I be an independent subset of P of finite cardinality greater than 1. Then

$$(\forall p \in P \Delta [I]) \quad \{p\} \cup I \text{ is independent} \quad (1.5.1)$$

and

$$(\forall a \in I) \quad I^o = \bigcup_{c \in (I \Delta \{a\})^o} \{a,c\}^o. \quad (1.5.2)$$

Proof: Let I be a doubleton. Then (2.5.2) holds by Axiom I. Let p be an element of $P \Delta [I]$. If $\{p\} \cup I$ were not independent, there would be an element a of I such that $a \in [\{p\} \cup (I \Delta \{a\})]$. Let b the element of I that would be distinct from a . In view of Axiom I, we would $\overleftarrow{p,b} = \overleftarrow{a,b}$ which would be absurd since $\overleftarrow{a,b}$ equals $P \Delta [I]$. Thus Theorem 2.5 holds if the cardinality of I equals 2.

Let n be any positive integer such that (2.5.1) and (2.5.2) hold for any I of cardinality less than or equal to n .

(1) Assume that (2.5.1) did not hold for some independent I with cardinality $n+1$. Then there were an element $p \in (P \Delta [I])$ such that $\{p\} \cup I$ were not independent. Since p could not be in the span of I , we could find $q \in I$ such that q were in the span of $\{p\} \cup (I \Delta \{q\})$. Assume q were in the span of some proper subset of $\{p\} \cup (I \Delta \{q\})$. Then there would be a minimal such subset S . Furthermore S could not be comprehended by I , since I is independent: that is, p would be in S . Due to the minimality of S , the set $\{q\} \cup S$ would be fundamental. It would follow from the induction hypothesis and (2.5.2) that there would exist $c \in [S \Delta \{p\}]$ such that q were in $\overleftarrow{p,c}$. But by Axiom I, this would imply that p would be in $\overleftarrow{q,c}$, which in turn would imply that p were in $[I]$: an absurdity. Consequently (2.5.1) holds for cardinality $n+1$.

(2) We now consider any independent I with cardinality $n+1$. Let a be any element of I , c any element of $(I \Delta \{a\})^o$ and x any element of $\{a,c\}^o$. If x were in $I \Delta \{a\}$, then Axiom I would imply that a would be too, which were absurd. It follows that

$$\bigcup_{c \in (I \Delta \{a\})^o} \{a,c\}^o \subset I^o. \quad (1.5.3)$$

We proceed to establish the containment which is reverse to that in (2.5.3). Let a , x and c be as above and suppose that y is any element of I^o . By Axiom II there exists $\phi \in P$ such that ϕ fixes each element of I and sends y to x . By Lemma (2.4) we know that ϕ maps the line $\overleftarrow{c,y}$ onto the line $\overleftarrow{c,x}$. But $\overleftarrow{c,x} = \overleftarrow{a,c}$ due to Axiom I. Again by Lemma (2.4) we have that y is in $\overleftarrow{a,c}$. QED

1.6 Complements Let P be projective group of transformations of a projective space P . Two closed subsets of P will be said to be **complementary** if they have void intersection and the span of their union equals P .

1.7 Corollary I Let P be projective group of transformations of a projective space P and let A and B be non-void complementary closed subsets of P . Then we have

$$P\Delta(A\cup B) = \bigcup_{a\in A, b\in B} \{a,b\}^o \quad \text{where the union is pairwise disjoint.} \quad (1.7.1)$$

In particular, for any pair of disjoint closed subsets A and B of P ,

$$[A\cup B] = \bigcup_{a\in A, b\in B} \overleftrightarrow{a,b}. \quad (1.7.2)$$

2. Meridians

2.1 Definition A meridian, essentially, is a one dimensional projective space. More immediately, a group M of permutations of a set M is said to be a **meridian group of permutations** of the **meridian** M provided that, for all tripletons $\{a,b,c\}$ and $\{x,y,z\}$ of M , there exists a unique element ϕ in M such that

$$\textbf{Axiom I} \quad \phi(a)=x, \phi(b)=y \text{ and } \phi(c)=z \quad (2.1.1)$$

and, for each doubleton $\{a,b\}$ of M and each element ϕ which interchanges a and b ,

$$\textbf{Axiom II} \quad (\exists y \in M \Delta \{x\}) \quad \{x,y\}=\{\phi(x),\phi(y)\}. \quad (2.1.2)$$

Axiom II evidently holds if, and only if, the following two requirements both hold: first, for each doubleton $\{a,b\}$ of M , each $\phi \in M$ which interchanges a and b , and each $x \in M$ such that $x=\phi(x)$,

$$\textbf{Axiom IIa} \quad (\exists y \in M \Delta \{x\}) \quad \phi(x)=y \text{ and } \phi(y)=x \quad (2.1.3)$$

and second,

$$\textbf{Axiom IIb} \quad \text{if } \theta \in M \text{ interchanges two distinct elements of } M, \text{ then } \theta=\theta^{-1}. \quad (2.1.4)$$

It follows from Axiom I that

$$\text{the } y \in (M \Delta \{x\}) \text{ such that } \phi(y)=y \text{ is unique.} \quad (2.1.5)$$

2.2 Notation Let M be a meridian group of permutations on a meridian M and let $\{a,b,c\}$ and $\{x,y,z\}$ be as in Axiom I. We shall denote the function ϕ provided by Axiom I by

$$\begin{bmatrix} x & y & z \\ a & b & c \end{bmatrix}. \quad (2.2.1)$$

2.3 Fixed Point Theorem Let M be a meridian group of permutations on a meridian M and suppose that $\{a,b\}$ is any doubleton comprehended by M . Then there is a unique element of M equal to its own inverse which fixes both a and b . Furthermore, element of M equal to its own inverse has either is the identity, has no fixed points or has exactly two fixed points.

Proof. Let c be an element of M distinct from a and b . It follows from Axiom IIa that there exists $y \in M$ distinct from c such that $\begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix}(d)=d$. It follows from Axiom IIb that $\begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix}(d)=b$. Direct calculation shows that

$$\begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix}(a)=a \text{ and } \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix}(b)=b. \quad (2.3.1)$$

Suppose that ϕ is any self-inverse element of M which fixes a and b and 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 c and interchanges a and b . It follows from Axiom I that this permutation must be identical with $\begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix}$. It follows that d must equal e , whence follows that $\phi = \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix} \circ \begin{bmatrix} b & a & c \\ a & b & c \end{bmatrix} \circ \begin{bmatrix} c & a & d \\ a & c & b \end{bmatrix}$. QED

2.4 More Notation If an element of M is not the identify permutation but equals its own inverse, we shall call it an **involution**. For a and b distinct elements of M , we shall denote the unique involution which fixes both of them by

$$\begin{bmatrix} a & b \\ a & b \end{bmatrix}. \quad (2.4.1)$$

It follows from Axiom II that an involution ϕ is determined by its values on any two distinct elements a and b of M , provided that b is not $\phi(a)$. Consequently, the notation

$$\begin{bmatrix} c & d \\ a & b \end{bmatrix} \quad (2.4.2)$$

will be used to denote an involution which sends a to c and b to d .

2.5 Harmonic Pairs Let M be a meridian group of permutations on a meridian M and let $\{a,b,c,d\}$ be a quadruplet comprehended by M . If

$$\begin{bmatrix} b & c & d \\ a & b & c \end{bmatrix}(d)=a, \quad (2.5.1)$$

we shall say that $\{\{a,c\},\{b,d\}\}$ is a **harmonic pair**.

It is not difficult to show that a pair $\{\{a,c\},\{b,d\}\}$ is harmonic if, and only if,

$$(\exists \phi \in M) \quad a=\phi(a), \quad c=\phi(c), \quad d=\phi(b) \quad \text{and} \quad b =\phi(d). \quad (2.5.2)$$

2.6 Translation A **translation** of M is an element of M with a single fixed point.

2.7 Translation Theorem If distinct inversions α and β fix a common point a , then

$$\alpha \circ \beta \text{ is a translation fixing } a. \quad (2.7.1)$$

If a translation τ fixes a point a , and if b is a point distinct from a , then

$$\text{if } c \equiv \tau(b), \quad \begin{bmatrix} a & c \\ a & c \end{bmatrix} \circ \begin{bmatrix} a & c & b \\ a & b & c \end{bmatrix} = \tau. \quad (2.7.2)$$

Proof. Let α and β be distinct inversions agreeing on a point a . If $\alpha \circ \beta$ were not a translation, then there would be another point e distinct from a at which they agreed. It would follow that $\beta(e)=\alpha(e)$. Since α and β are distinct, if they both fixed e , Theorem (2.3) would be violated. Thus e would not be fixed. But then, if $o \equiv \alpha(e)$, both α and β would equal $\begin{bmatrix} a & o & e \\ a & e & o \end{bmatrix}$: an absurdity.

Let τ be a translation and let a be its fixed point. Let b be any element of M distinct from a , let $c \equiv \tau(b)$ and let $d \equiv \tau(c)$. We know from (2.7.1) that $\begin{bmatrix} a & c \\ a & c \end{bmatrix} \circ \begin{bmatrix} a & c & b \\ a & b & c \end{bmatrix}$ is a translation. It follows that the permutation $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau$ interchanges b and d and so it is an involution. Thus

$$a = \left(\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \right) \circ \left(\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \right) (a) = \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau \circ \begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a)$$

whence follows that τ fixes $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} (a)$. Consequently $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix}$ must fix a . It follows that $\{\{a,c\},\{b,d\}\}$ is a harmonic pair. We have $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} = \begin{bmatrix} a & c \\ a & c \end{bmatrix}$ and $\begin{bmatrix} c & d & b \\ c & b & d \end{bmatrix} \circ \tau = \begin{bmatrix} a & c & b \\ a & b & c \end{bmatrix}$. Thus (2.7.2) holds. QED

2.8 Libras A **function libra** is a family F of bijections from one set A onto another set B such that

$$(\forall \{\alpha,\beta,\gamma\} \subset F) \quad \alpha \circ \beta^{-1} \circ \gamma \in F. \quad (2.8.1)$$

We say that A is the **common domain** and B is the **common range** of the function libra. A libra closely resembles a group of permutations, the difference being that the common domain and the common range may be distinct. If the common range and common domain are identical, and if the identity function is in the libra, then the libra is a group of permutations.

We find it often useful to adopt the following notation

$$\llbracket \alpha,\beta,\gamma \rrbracket \equiv \alpha \circ \beta^{-1} \circ \gamma. \quad (2.8.2)$$

An **abstract libra** is a set F with ternary operation $F \ni (x,y,z) \mapsto [x,y,z] \in F$ which, for all $\{v,w,x,y,z\} \subset F$, satisfies the equalities

$$[v,v,w]=[w,v,v]=w \quad \text{and} \quad \llbracket [v,w,x],y,z \rrbracket = [v,w,[x,y,z]]. \quad (2.8.3)$$

One can deduce from these two axioms that the equality

$$[v,[w,x,y],z]=[v,y,x],x,z] \quad (2.8.4)$$

holds as well. A meridian is abelian provided that, for all $\{x,y,z\} \subset F$,

$$[x,y,z] = [z,y,x]. \quad (2.8.5)$$

A group G is a libra relative to the ternary operation $G \ni (x,y,z) \mapsto (x \cdot y^{-1} \cdot z) \in G$. Conversely a libra F is a group with identity e in F relative to the operation

$$(\forall \{x,y\} \subset F) \quad x \cdot y \equiv [x,e,y]. \quad (2.8.6)$$

A libra is abelian if, and only if, the groups associated with it as above are abelian.

We introduce the concept of libra here because there are numerous significant libras contained within a meridian.

2.9 Inversion Libras Let M be a meridian group of permutations on a meridian M . Let a and b be elements of M . By $M_{(a,b)}$ we shall mean the set of all inversions which send a to b and b to a . We define

$$M_{(a,b)} \equiv M\Delta\{a,b\}. \quad (2.9.1)$$

The families $M_{(a,b)}$ are libras. We shall write

$$M_{(a)} \quad \text{and} \quad M_{(a)}, \text{ respectively} \quad (2.9.2)$$

for $M_{(a,a)}$ and $M_{(a,a)}$, respectively.

Proof. That $M_{(a,b)}$ is a libra for $a \neq b$ follows directly from Axiom IIb. We shall examine the case where $a=b$. Let $\{\alpha, \beta, \gamma\} \subset M_{(a)}$ for a in M . Let $\delta \equiv \alpha \circ \beta \circ \gamma$: we must show that δ is an involution.

It follows from (2.7.1) that $\beta \circ \gamma$ is a translation τ . Thus $\theta \equiv \alpha \circ \delta$ is that same translation τ . The inversion α has precisely one other fixed point besides a : we shall denote it by c . Let b be the element that $\tau(b)=c$. From Theorem (2.7.2) follows that $\begin{bmatrix} a & c \\ a & c \end{bmatrix} \circ \begin{bmatrix} a & c & b \\ a & b & c \end{bmatrix} = \tau$. But $\begin{bmatrix} a & c \\ a & c \end{bmatrix}$ is just α , so $\begin{bmatrix} a & c & b \\ a & b & c \end{bmatrix}$ must be δ , an element of $M_{(a)}$ ts. QED

2.10 Meridian Fields Let $\{a,b\}$ be a doubleton of a meridian M . Then $M_{(a,b)}$ has a libra operator defined as follows: for all $\{x,y,z\} \subset M_{(a,b)}$

$$[x,y,z] \equiv \begin{bmatrix} b & z & x \\ a & x & z \end{bmatrix}(y). \quad (2.10.1)$$

Evidently it is abelian. These libras fit into two isomorphism classes: those where $a=b$, and those where $a \neq b$. And these two classes are always distinct.

Let $\{o, l, \infty\}$ be a tripleton comprehended by M . For $\{x,y\} \subset M_{o,\infty}$ and $\{u,v\} \subset M_{\infty,\infty}$ we define

$$x \cdot y \equiv \begin{bmatrix} \infty & y & x \\ \infty & o & y \end{bmatrix}(l) \quad \text{and} \quad u+v \equiv \begin{bmatrix} \infty & v & u \\ \infty & u & v \end{bmatrix}(o). \quad (2.10.2)$$

If we further define, for all $x \in M_{\infty,\infty}$,

$$o \cdot x \equiv x \cdot o \equiv o, \quad (2.10.3)$$

we shall find that

$$M_{\infty,\infty} \text{ is a field of characteristic not equal to } 2. \quad (2.10.4)$$

We call the operations “ \cdot ” **multiplication** and “ $+$ ” **addition**.

Proof. The involution $\begin{bmatrix} \infty & x+y \\ \infty & o \end{bmatrix}$ agrees with $\begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}$ at both ∞ and o , so they must be equal:

$$\begin{bmatrix} \infty & x+y \\ \infty & o \end{bmatrix} = \begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}. \quad (2.10.5)$$

Since the involution $\begin{bmatrix} \infty & o \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & y \end{bmatrix}$ agrees with $\begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}$ at both ∞ and x , we have (along with (2.10.5))

$$\begin{bmatrix} \infty & x+y \\ \infty & o \end{bmatrix} = \begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix} = \begin{bmatrix} \infty & o \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & y \end{bmatrix}. \quad (2.10.6)$$

Similar reasoning shows that, for $o \notin \{x,y\}$ that

$$\begin{bmatrix} \infty & x \cdot y \\ \infty & o \end{bmatrix} = \begin{bmatrix} o & y \\ \infty & x \end{bmatrix} = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & y \end{bmatrix}. \quad (2.10.7)$$

For $\{x,u\} \in M_{(\infty)}$ such that $u \neq o$ we define

$$-x \equiv o \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix}(x) \quad \text{and} \quad u^{-1} \equiv \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix}(u). \quad (2.10.8)$$

Then

$$x+o = \begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}(o) = x, \quad u \cdot l = \begin{bmatrix} o & 1 \\ \infty & u \end{bmatrix}(u), \quad (2.10.9)$$

$$(-x)+x = \begin{bmatrix} \infty & x \\ \infty & -x \end{bmatrix}(o) = \begin{bmatrix} \infty & o \\ \infty & -x \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & x \\ \infty & x \end{bmatrix} = \begin{bmatrix} \infty & o \\ \infty & -x \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix}(x) = \begin{bmatrix} \infty & o \\ \infty & -x \end{bmatrix}(-x) = o, \quad (2.10.10)$$

$$u^{-1} \cdot u = \begin{bmatrix} o & u \\ \infty & u^{-1} \end{bmatrix}(l) = \begin{bmatrix} o & 1 \\ \infty & u^{-1} \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & u \end{bmatrix}(l) = \begin{bmatrix} o & 1 \\ \infty & u^{-1} \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix}(u) = \begin{bmatrix} o & 1 \\ \infty & u^{-1} \end{bmatrix}(u^{-1}) = l. \quad (2.10.11)$$

For $\{x,y,z,u,v,w\} \subset M_{(\infty)}$ such that $o \notin \{u,v,w\}$, we have

$$x+(y+z) = \begin{bmatrix} \infty & y+z \\ \infty & x \end{bmatrix}(o) = \begin{bmatrix} \infty & o \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & y+z \end{bmatrix}(o) = \begin{bmatrix} \infty & o \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & y \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & o \end{bmatrix}(o) = \quad (2.10.12)$$

$$\begin{bmatrix} \infty & x+y \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & o \end{bmatrix}(o) = \begin{bmatrix} \infty & x+y \\ \infty & z \end{bmatrix}(o) = (x+y)+z \quad (2.10.13)$$

and, similarly,

$$u \cdot (v \cdot w) = (u \cdot v) \cdot w. \quad (2.10.14)$$

That

$$x+y=y+x \quad \text{and} \quad u \cdot v=v \cdot u \quad (2.10.15)$$

is trivial. We have established that “+” and “·” are abelian group operators.

It remains to show that the “distributive law” holds. Let x, y and z be elements of $M_{(\infty)}$ such that both x and $y+z$ are distinct from o . We define

$$\theta \equiv \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix}. \quad (2.10.16)$$

Evidently

$$\theta(\infty)=\infty. \quad (2.10.17)$$

Furthermore

$$\begin{aligned} \theta(o) &= \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix}(o) = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix}(o) = \\ & \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix}(y+z) = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & y+z \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & y+z \\ \infty & 1 \end{bmatrix}(y+z) = \\ & \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & y+z \\ \infty & 1 \end{bmatrix}(1) = \begin{bmatrix} o & y+z \\ \infty & x \end{bmatrix}(1) = x \cdot (y+z). \end{aligned} \quad (2.10.18)$$

Moreover, since $\begin{bmatrix} o & y \\ \infty & x \end{bmatrix} = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & y \end{bmatrix}$.

$$\begin{aligned} \theta(x \cdot y) &= \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix}(x \cdot y) = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & y \\ \infty & x \end{bmatrix}(1) = \\ & \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & y \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & y \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & y \end{bmatrix}(1) = \\ & \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \left(\begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \left(\begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \left(\begin{bmatrix} o & y \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & y \\ \infty & x \end{bmatrix} \right) \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \right) \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \right) \circ \begin{bmatrix} o & 1 \\ \infty & y \end{bmatrix}(1) = \\ & \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} \infty & z \\ \infty & y \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix}(1) = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix}(z) = \begin{bmatrix} o & 1 \\ \infty & x \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & 1 \end{bmatrix} \circ \begin{bmatrix} o & 1 \\ \infty & z \end{bmatrix}(1) = \begin{bmatrix} o & z \\ \infty & x \end{bmatrix}(1) = x \cdot z. \end{aligned}$$

It follows this last and from (2.10.17) that $\theta = \begin{bmatrix} \infty & x \cdot z \\ \infty & x \cdot y \end{bmatrix}$, so that

$$\theta(o) = \begin{bmatrix} \infty & x \cdot z \\ \infty & x \cdot y \end{bmatrix}(o) = x \cdot y + x \cdot z. \quad (2.10.19)$$

From (2.10.18) and (2.10.19) we have that

$$x \cdot (y+z) = x \cdot y + x \cdot z. \quad (2.10.20)$$

It follows that we have a field. If the field were of characteristic 2, then for any $x \in M_{(\infty)}$,

$$\begin{bmatrix} \infty & x \\ \infty & x \end{bmatrix}(o) = x+x=o = \begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix}(o). \quad (2.10.21)$$

But then $\begin{bmatrix} \infty & x \\ \infty & x \end{bmatrix}$ and $\begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix}$ would agree on two point, which would mean that they were the same. That would imply that $\begin{bmatrix} \infty & o \\ \infty & o \end{bmatrix}$ would fix each point x , which, since the identity function is not in $M_{(\infty)}$. QED

2.11 Alternate Definition The definition for addition in (2.10) has an alternate form, which we mention here, because this form extends to higher dimensions. Using the same terminology as (2.10) we can say, for all $\{x,y\} \subset M_{(\infty)}$,

$$x+y = \begin{bmatrix} \infty & m \\ \infty & m \end{bmatrix}(o) \quad \text{where} \quad m \equiv \begin{bmatrix} x & y \\ x & y \end{bmatrix}(\infty). \quad (2.11.1)$$

Proof. From the properties of harmonic pairs we know that $\begin{bmatrix} \infty & m \\ \infty & m \end{bmatrix}$ interchanges x and y . Consequently $\begin{bmatrix} \infty & m \\ \infty & m \end{bmatrix}$ agrees with $\begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}$ on three points and so they are the same. But $x+y$ is just $\begin{bmatrix} \infty & y \\ \infty & x \end{bmatrix}(o)$. QED

2.12 The Affine Space $M_{(\infty)}$ We note that what we have shown for the additive group of the field in (2.10) and (2.11) can be applied to the libra $M_{(\infty)}$. If we define, for all $\{x,y,z\} \subset M_{(\infty)}$,

$$[x,y,z] \equiv \begin{bmatrix} \infty & z \\ \infty & x \end{bmatrix}(y), \quad (2.12.1)$$

then $M_{(\infty)}$ is a libra relative to this operation and

$$[x,y,z] = \begin{bmatrix} \infty & m \\ \infty & m \end{bmatrix}(y) \text{ where } m \equiv \begin{bmatrix} x & z \\ x & z \end{bmatrix}(\infty). \quad (2.12.2)$$

3. Higher Dimensional Projective Spaces

3.1 Definitions Let P be a finite dimensional projective space of dimension greater than 1. Let P be the corresponding projective group of permutations. Every closed subset S of P is also a projective space relative to the group

$$P|_S \equiv \{\phi|_S : \phi \in P\}. \quad (3.1.1)$$

Thus we may call such subsets **subspaces**. Subspaces of dimension 2 will be called **planes**.

If R and S are disjoint closed subsets of P such that $P=[R \cup S]$, then the dimension of P is the sum of the dimensions of R and S . Subspaces complementary to a singleton will be called **co-points**. Evidently each line in P not comprehended by a co-point, intersects that co-point in a singleton.

3.2 Meridian Lines Let L be a line in a projective space P . It is a consequence of the two projective space axioms that the set

$$\{\phi|_L : \phi \in P \text{ and } \phi(x) \in L \text{ for all } x \in L\} \quad (3.2.1)$$

is a meridian group. Furthermore, for each $\theta \in P$, $\theta|_L$ is a meridian isomorphism onto its image. If K is another line in P , $\{a,b,c\}$ is a tripleton of L and $\{x,y,z\}$ is a tripleton of K , then there is an element α of P unique on L such that $\alpha(a)=x$, $\alpha(b)=y$ and $\alpha(c)=z$. We shall denote the restriction of α to L by

$$\begin{bmatrix} x & y & z \\ a & b & c \end{bmatrix}. \quad (3.2.2)$$

The mappings described by (3.2.2) will be called **projective meridian isomorphisms**.

Each line in P will be called a **projective meridian** and each field of a projective meridian will be called a **projective field**.

3.3 Projections Let V be a co-point and a an element of $P \Delta V$. Then each element x of P not in $P \Delta \{a\}$ is on precisely one line which passes through a : that line intersects V in precisely one point, which we shall call the **projection of x from a onto V** . The function $P \Delta V \leftrightarrow V$ thus described is called the **projection from a onto V** .

3.4 Projection Theorem Let a be a point and V be a co-point not containing a . Let ϕ be the projection from a onto V . Let L be a line neither containing a nor comprehended by V and let K by the image of L by the projection from a onto V . Then the restriction of ϕ to L is a projective meridian isomorphism from L onto K .

Proof. We may presume that K and L are distinct. Since both are in the plane determined by K and a , they must intersect at some point q . Let $\{b,c\}$ be a doubleton subset of L not containing q . Let x be the element of K in $\overleftarrow{a,b}$ and y be the element of K in $\overleftarrow{a,c}$. The set $\{a,b,q,x,y\}$ is a fundamental set and so Axiom II implies that there exists an element θ of P such that

$$\theta(b)=x, \theta(x)=b, \theta(q)=q, \theta(c)=y \text{ and } \theta(y)=c. \quad (3.4.1)$$

Evidently θ sends $\overleftarrow{b,x}$ onto itself and the line $\overleftarrow{c,y}$ onto itself. These two lines intersect at a and so a is fixed by θ . Since the restriction of θ to $\overleftarrow{b,x}$ fixes a , it follows from the Fixed Point Theorem (3.3) that it fixes precisely one other point o . Since q is fixed, the line $\overleftarrow{o,q}$ is sent to itself and so the intersection point p of $\overleftarrow{o,q}$ with $\overleftarrow{c,y}$ must be fixed by θ . The restriction of θ to $\overleftarrow{o,q}$ having three fixed points, it follows from Axiom II that it must fix each point of that line. Now let N be any line through a in $[K \cup \{a\}]$. It intersects $\overleftarrow{o,q}$ in one point v . Since θ fixes v and a , the line N is sent onto itself. Hence the intersecting point of N with L is sent to the intersecting point of N with K . It follows that θ agrees with ϕ on L . Since θ restricted to L is a meridian isomorphism, so is ϕ . QED

3.5 Projective Affine Space Let P be a finite dimensional projective space of dimension greater than 1. Let V be a co-point of P and let $A \equiv P \Delta V$. Let $\{a,b,c\}$ be a subset of A . We define $[a,b,c]$ as follows: If $a=c$, we let m be a . Otherwise, the line $\overleftarrow{a,c}$ intersects V in one point v and we may let

$$m \equiv \begin{bmatrix} a & c \\ a & c \end{bmatrix}(v). \quad (3.5.1)$$

If $m=b$, we define $[a,b,c]$ to be b . Otherwise the line $\overleftarrow{b,m}$ intersects V in one point w and we define

$$[a,b,c] \equiv \begin{bmatrix} w & m \\ w & m \end{bmatrix}(b). \quad (3.5.2)$$

We shall say that A is the **affine space** induced by V. We now prove that A is an abelian libra relative to the ternary operator of (3.5.2).

Proof. It is evident that $[a,b,c]=[c,b,a]$. If $a=b$, then $\overleftarrow{m,b}=\overleftarrow{a,c}$ and so $w=v$, whence follows that $[a,b,c]=c$. Similarly, if $b=c$, then $[a,b,c]=a$. This establishes the first part of (2.8.3). It remains to show that the second part holds. Assume that it did not, and choose a subspace S of maximal dimension for which the associative rule did hold: we know from (2.12) that the dimension must be greater than 1.

Let $\{a,b,c,d,e\}$ be a subset A but not a subset of S and assume that

$$[[a,b,c],d,e] \neq [a,b,[c,d,e]]. \quad (3.5.3)$$

Let p be any element of $V \cap S$ not in $\overleftarrow{[[a,b,c],d,e],[a,b,[c,d,e]]}$, and let ϕ be the projection from p onto S. Since ϕ is isomorphic on any line, we see that

$$\phi([a,b,c])=[\phi(a),\phi(b),\phi(c)] \quad \text{and so} \quad \phi([[a,b,c],d,e])=[[\phi(a),\phi(b),\phi(c)],\phi(d),\phi(e)]. \quad (3.5.4)$$

Similarly

$$\phi([a,b,[c,d,e]])=[\phi(a),\phi(b),[\phi(c),\phi(d),\phi(e)]]. \quad (3.5.5)$$

Since p is not in $\overleftarrow{[[a,b,c],d,e],[a,b,[c,d,e]]}$, it follows that the projections from p onto S of $[[a,b,c],d,e]$ and $[a,b,[c,d,e]]$ are not identical. But, since libra associativity does hold for S by our induction hypothesis, we have

$$[[[\phi(a),\phi(b),\phi(c)],\phi(d),\phi(e)]] = [[\phi(a),\phi(b),[\phi(c),\phi(d),\phi(e)]]]. \quad (3.5.6)$$

But (4), (5) and (6) would imply that the projections from p of $[[a,b,c],d,e]$ and $[a,b,[c,d,e]]$ were identical: an absurdity. QED

3.6 Projective Linear Space Let P be a finite dimensional projective space of dimension greater than 1. Let V be a co-point of P, let L denote $P \Delta V$ and let e be an element of L. We know from the (3.5) that L is a libra so we can define, for all $\{a,b\} \subset L$,

$$a+b \equiv [a,e,b]. \quad (3.6.1)$$

From (2.8.5) we know that L is an abelian group. We shall now introduce a “scalar multiplication” on L and show that relative to this scalar multiplication, L is a linear space.

Let M be any of the lines of P, let $\{o,l,\infty\}$ be a tripleton of M and let F be the field defined as in (2.10). We define, for all $r \in L \Delta \{e\}$ and $t \in M$, the **scalar product** $t \cdot r \equiv \begin{bmatrix} e & r & v \\ o & l & \infty \end{bmatrix}(t)$ where $\{v\} = \overleftarrow{e,r} \cap V$.

To show that L is a linear space relative to this scalar multiplication it remains to prove that the distributive property holds:

$$(\forall t \in F \Delta \{e\})(\forall \{a,b\} \subset L) \quad t \cdot (a+b) = (t \cdot a) + (t \cdot b). \quad (3.6.2)$$

Proof. We may presume that P is 2-dimensional. If $t \cdot (a+b) \neq (t \cdot a) + (t \cdot b)$, take $v \in V$ to be not on the line $\overleftarrow{t \cdot (a+b), ((t \cdot a) + (t \cdot b))}$ and let ϕ be the projection from v onto $\overleftarrow{e,r}$. Then

$$t \cdot \phi(a) + t \cdot \phi(b) = \phi(t \cdot (a+b)) \neq \phi(t \cdot (a+b)) = t \cdot \phi(a+b) = t \cdot \phi(a) + t \cdot \phi(b) \quad (3.6.3)$$

which is a patent absurdity. QED

3.7 Recapitulation We began in (1.2) with a definition of a projective space. In Section 2 we investigated the one dimensional case, which in Section 3 we used to show that the definition of Section 1 evolves into the definition of projective space obtained by adding points “at infinity”.

3.8 Remarks The present paper may be considered as a work in progress, as the author has not as yet prepared it in finished form. The author much appreciates the use of the facilities here at Institute of Information Science in Academia Sinica for producing this report.