

FREE MOBILITY AND ORTHOGONALITY

BY
REINHOLD BAER

If F is an algebraically ordered, though not necessarily commutative, field, P the system of its positive numbers, and if b_1, \dots, b_i are i linearly independent vectors in the n -dimensional vector space V over F , then the manifolds $\sum_{j=1}^{i-1} Fb_j + Pb_k$ for $1 \leq k \leq i$ form an *i -dimensional chain of incident sub-half-spaces of V* [= i -dimensional direction element of V]. The group Γ of linear transformations of V is said to have the Property (P. i) of *i -dimensional free mobility* if Γ is simply transitive on the set of all the i -dimensional chains of incident sub-half-spaces of V . We are going to characterize these groups, and incidentally the spaces possessing such groups, under the additional hypotheses that $1 < i$ and $2 < n$. These characterizations may be concentrated into the following theorems.

THEOREM A. *The group Γ of linear transformations of the vector space V of dimension n greater than 2 has Property (P. n) if, and only if, F is Pythagorean and there exists a symmetrical, positive definite bilinear form $f(x, y)$ [from V to F] such that Γ consists of all the linear transformations of V which preserve the form f .*

Here as always we say that the field F is *Pythagorean*, if it [possesses an algebraical order,] is commutative, and if every $1+t^2$ with t in F is the square of an element, not 0, in F ; and we term the bilinear form $f(x, y)$ *positive definite*, if $f(x, x)$ for $x \neq 0$ is the square of an element, not 0, in F .

Theorem A makes it clear that the groups with Property (P. n) are just the full orthogonal groups of V ; and one deduces from Theorem A without difficulty that the Pythagorean character of F is necessary and sufficient for the existence of a full orthogonal group and that any two groups with Property (P. n) are conjugate within the group of all linear transformations of V .

THEOREM B. *The group ϕ of linear transformations of the vector space V of dimension greater than 2 has Property (P. $n-1$) if, and only if, ϕ is the subgroup of index 2 of a [uniquely determined] group Γ with Property (P. n).*

Theorem B implies that the groups with Property (P. $n-1$) are just the proper orthogonal groups of V .

THEOREM C. *If the group Λ of linear transformations of V has Property (P. i), then $i=1$ or $n-1$ or n .*

Presented to the Society, April 22, 1950; received by the editors August 31, 1949.

When proving these theorems we show also that the actual algebraical ordering of the field F [that is, the special choice of the domain P of positivity] is not really important, since groups with Property $(P'.i)$ will also have Property $(P''.i)$ [for P' , P'' domains of positivity]. To see this we show the equivalence of these properties with properties that are, in their very formulation, completely independent of any possible ordering of the field F .

In Chapter I we shall characterize the full orthogonal group; and all the other results we shall obtain by reference to the characterization of the full orthogonal group. It is worth noting that when characterizing the proper orthogonal group [in Chapter II] we have to treat separately the case of odd dimension [which is rather simple] and the case of dimension greater than 3 [which is somewhat more intricate].

The reason for this last complication may partly be looked for in the quite different situation arising for $n=2$. Though some of our arguments remain applicable in the case $n=2$, there are enough of them that fail. Actually Pickert [1, p. 498]⁽¹⁾ has given an interesting example which shows that Theorem B ceases to be true for $n=2$. On the other hand we can show (§6) that the characterization of the full orthogonal group remains true for $n=2$, if we impose an additional hypothesis on F .

Historically our problems originate from Helmholtz's space problem. It is an important step in its treatment to deduce the existence of an invariant quadratic form from the validity of a free mobility condition; and as the problem concerned itself with real space only, analytical means were used in its treatment (see, for instance, Weyl [1, p. 29-43]). To obtain a purely algebraical treatment of this phase of Helmholtz's space problem one has to substitute for the field of real numbers some formally real field as the field of coordinates. This has been done for the full orthogonal group by Iyanaga-Abe [1] and for the proper orthogonal group by Pickert [1]. Both impose, however, a number of additional requirements concerning group and field apart from $(P.n)$ and $(P.n-1)$ respectively.

CHAPTER I. THE FULL ORTHOGONAL GROUP

1. Groups of linear transformations defining an orthogonality relation. Throughout our discussion F is going to be a [not necessarily commutative] field of characteristic different from 2; and V is going to be an n -dimensional vector space over F —the elements in F act as left multipliers on the elements in V . Expressions like subspace, linear submanifold, F -admissible subgroup of V will be used alternately; and subspaces of dimensions 1, 2, and $n-1$ will be called lines, planes, and hyperplanes respectively.

Transformations of V will always be linear, one-to-one, and exhaustive.

(¹) Numbers in brackets refer to the bibliography at the end of the paper.

If σ is a transformation of V , then we denote by $J(\sigma)$ the totality of vectors v such that $v\sigma = v$ and by $R(\sigma)$ the totality of vectors v such that $v\sigma = -v$. $J(\sigma)$ and $R(\sigma)$ are subspaces of V with cross cut 0. The following well known fact will be useful:

$$\sigma^2 = 1 \quad \text{if, and only if,} \quad V = J(\sigma) \oplus R(\sigma).$$

Here as always \oplus indicates the direct sum. Transformations σ such that $\sigma^2 = 1$ will be referred to as involutions.

DEFINITION. The group ϕ of linear transformations of V defines an orthogonality relation, if

(a) to every subspace S of V there exists one and only one involution $\sigma(S)$ in ϕ such that $S = J[\sigma(S)]$ and

(b) $S' \leq S''$ implies $R[\sigma(S'')] \leq R[\sigma(S')]$.

If ϕ defines an orthogonality relation, then $\sigma(S)$ is a single-valued function of the subspaces S of V ; and we may let $S^\phi = R[\sigma(S)]$. The following simple inferences from (a) and (b) show that the mapping of S onto S^ϕ constitutes an orthogonality relation in the strictest sense of the word.

(c) ϕ contains the reflection ρ in the origin [$v\rho = -v$ for every v] since $\rho = \sigma(0)$.

(d) $S^\phi = S$ for every subspace S of V ,

since $\sigma\rho$ is, for every involution σ in ϕ , an involution in ϕ which satisfies $J(\sigma\rho) = R(\sigma)$ and $R(\sigma\rho) = J(\sigma)$.

(e) $V = S \oplus S^\phi$ for every subspace S of V ,

since $V = J(\sigma) \oplus R(\sigma)$ for every involution σ .

(f) $(S\tau)^\phi = (S^\phi)\tau$ for every subspace S and every τ in ϕ ,

since $J(\sigma)\tau = J(\tau^{-1}\sigma\tau)$ and $R(\sigma)\tau = R(\tau^{-1}\sigma\tau)$.

THEOREM. The group ϕ of linear transformations of V defines an orthogonality relation if, and only if, ϕ satisfies the following two conditions:

(U) If τ is in ϕ and if there exists a basis b_1, \dots, b_n of V such that $b_i\tau \equiv b_i$ modulo $\sum_{j=1}^{i-1} Fb_j$ for $i=1, \dots, n$, then $\tau=1$.

(E) If b_1, \dots, b_n is a basis of V , and if $0 \leq k \leq n$, then there exists a transformation τ in ϕ such that

$$b_i\tau \equiv \begin{Bmatrix} +b_i \\ -b_i \end{Bmatrix} \text{ modulo } \sum_{j=1}^{i-1} Fb_j \quad \text{for} \quad \begin{Bmatrix} i \leq k \\ k < i \end{Bmatrix}.$$

Proof. Assume first that the group ϕ meets requirement (a) of Definition 1, and that b_1, \dots, b_n is a basis of V . Consider a transformation τ in ϕ such that $b_i\tau \equiv b_i$ modulo $\sum_{j=1}^{i-1} Fb_j$ for $i=1, \dots, n$. Then we have $b_1\tau = b_1$, and thus may make the inductive hypotheses that $1 < i$ and that $b_j\tau = b_j$ for $j < i$. There exists by (a) one and only one involution σ in ϕ such that $J(\sigma) = \sum_{j=1}^{i-1} Fb_j$. Naturally we have $\sum_{j=1}^i Fb_j = J(\sigma) \oplus [R(\sigma) \cap \sum_{j=1}^i Fb_j]$ so that $R(\sigma)$ contains an element $w = v + b_i$ with v in $\sum_{j=1}^{i-1} Fb_j$. It follows from the inductive hypothesis that $J(\tau^{-1}\sigma\tau) = J(\sigma)$, and hence it follows from (a) that

$\sigma = \tau^{-1}\sigma\tau$. It follows from our hypothesis concerning τ that $b_i\tau = u + b_i$ with u in $\sum_{j=1}^{i-1} Fb_j$, and now one verifies that

$$\begin{aligned} u - w &= (u + w)\sigma = (v + u + b_i)\sigma = (v + b_i)\tau\sigma = w\sigma\tau = -w\tau \\ &= -(v + b_i)\tau = -v - (u + b_i) = -u - w \end{aligned}$$

or $u = 0$ or $b_i\tau = b_i$. This completes the induction, showing $\tau = 1$; and thus we have verified (U). To prove (E) one has just to remember that as a consequence of (a) there exists in ϕ an involution σ' such that $J(\sigma') = \sum_{j=1}^k Fb_j$.

Assume now the validity of conditions (U) and (E). Then one deduces from (U) immediately that

(J₀) *the transformation τ in ϕ is an involution, if there exists a basis b_1, \dots, b_n of V such that $b_i\tau = \pm b_i$ modulo $\sum_{j=1}^{i-1} Fb_j$ for every i .*

Next we prove:

(U') *If σ' and σ'' are involutions in ϕ such that $J(\sigma') \leq J(\sigma'')$, then $R(\sigma'') \leq R(\sigma')$.*

There exists a basis b_1, \dots, b_n of V such that $J(\sigma') = \sum_{i=1}^{h-1} Fb_i$, $R(\sigma') \cap J(\sigma'') = \sum_{i=h}^{k-1} Fb_i$, $R(\sigma') = \sum_{i=k}^n Fb_i$. It is clear then that $b_i = b_i\sigma'\sigma''$ for $i < h$, $-b_i = b_i\sigma'\sigma''$ for $h \leq i < k$ and $b_i\sigma'\sigma'' = -2b_i + b_i$ for $k \leq i \leq n$, if $b_i = b_i + t_i$ with t_i in $J(\sigma'')$ and t_i' in $R(\sigma'')$. But then it follows from (J₀) that $\sigma'\sigma''$ is an involution, and this implies $\sigma'\sigma'' = \sigma''\sigma'$, since σ' and σ'' are involutions. Consider now an element w in $R(\sigma'')$. Then $w = u + v$ with u in $J(\sigma')$ and v in $R(\sigma')$, and consequently

$$2u + w = w\sigma'\sigma'' = w\sigma''\sigma' = -2u + w \quad \text{or} \quad u = 0 \quad \text{and} \quad w = v.$$

Hence $w = v$ belongs to $R(\sigma')$ and this proves the desired inequality $R(\sigma'') \leq R(\sigma')$.

From (U') we infer in particular that $J(\sigma') = J(\sigma'')$ implies $R(\sigma') = R(\sigma'')$ and hence $\sigma' = \sigma''$, and thus (U') implies (b) as well as the uniqueness part of (a).

Consider now any subspace S of V . Then there exists a basis d_1, \dots, d_n of V such that $S = \sum_{i=1}^m Fd_i$. It follows from (E) that there exists a transformation σ in ϕ such that

$$d_i\sigma \equiv \begin{cases} +d_i \\ -d_i \end{cases} \text{ modulo } \sum_{j=1}^{i-1} Fd_j \quad \text{for} \quad \begin{cases} i \leq m \\ m < i \end{cases}.$$

It is an immediate consequence of (J₀) that σ is an involution, and now one verifies easily that $S = J(\sigma)$. This completes the verification of (a) and (b). We note that we have shown slightly more than the desired theorem, namely also the following proposition.

COROLLARY. *Condition (b) [of the definition] is a consequence of Condition (a).*

If ϕ defines an orthogonality, then we shall call *vectors* v and w *orthogonal* [with respect to ϕ], if there exists a subspace S such that v is in S and w in S^ϕ . Naturally this is equivalent to the fact that w belongs to $(Fv)^\phi$ and also to the fact that v belongs to $(Fw)^\phi$.

2. Free mobility. If P is a subgroup of index 2 of the multiplication group of the field F , and if -1 does not belong to P , then we term P a *domain of positivity* [in the weak sense]; and the letter P shall always designate such domains. We note that P is a domain of positivity in the customary [or strict] sense, if it is closed under addition and that E. Sperner has termed "Halbordnung" what we called here a domain of positivity in the weak sense.

The group ϕ of linear transformations of the n -dimensional vector space V has the property of n -dimensional free mobility with respect to P , if it meets the following requirement:

(P.n) If b'_1, \dots, b'_n and b''_1, \dots, b''_n are bases of V , then there exists one and only one transformation τ in ϕ such that

$$\left[\sum_{j=1}^{i-1} Fb'_j + Pb'_i \right] \tau = \sum_{j=1}^{i-1} Fb''_j + Pb''_i \quad \text{for } i = 1, \dots, n.$$

PROPOSITION 1. A group ϕ with Property (P.n) has Property (E) (of §1, Theorem) and the following property:

(J) The transformation τ in ϕ is an involution, if there exists a basis b_1, \dots, b_n of V such that $\left[\sum_{j=1}^i Fb_j \right] \tau = \sum_{j=1}^i Fb_j$ for $i = 1, \dots, n$.

Proof. If τ leaves invariant the subspaces $\sum_{j=1}^i Fb_j$, then τ^2 leaves invariant the sub-half-spaces $\sum_{j=1}^{i-1} Fb_j + Pb_i$, since the square of any number, not 0, in F , belongs to P . Now it is clear that (J) is a consequence of the uniqueness statement contained in (P.n). From (P.n) one deduces furthermore the existence of a transformation η in ϕ and of numbers p_i in P such that

$$b_i \eta \equiv \begin{cases} + p_i b_i \\ - p_i b_i \end{cases} \text{ modulo } \sum_{j=1}^{i-1} Fb_j \quad \text{for } \begin{cases} i \leq k \\ k < i \end{cases}.$$

It follows from (J) that $\eta^2 = 1$; and this implies $p_i^2 = 1$. Since p_i belongs to P whereas -1 does not belong to P , we see that $p_i = 1$; and this shows the validity of (E).

PROPOSITION 2. Property (J) implies Property (U) (of §1, Theorem).

Proof. Assume that τ in ϕ has the property $b_i \tau \equiv b_i$ modulo $\sum_{j=1}^{i-1} Fb_j$ for $i = 1, \dots, n$. It follows from (J) that τ is an involution. It is clear that b_1 belongs to $J(\tau)$, and thus we may make the inductive hypothesis that b_1, \dots, b_{i-1} belong to $J(\tau)$. By hypothesis $b_i \tau - b_i$ belongs to $\sum_{j=1}^{i-1} Fb_j$, which by our inductive hypothesis belongs to $J(\tau)$. Since τ is an involution, we have therefore

$$b_i\tau - b_i = (b_i\tau - b_i)\tau = b_i - b_i\tau$$

or $b_i = b_i\tau$, since the characteristic of F is different from 2. This completes our inductive argument and shows that $\tau = 1$, as we claimed.

An immediate consequence of Propositions 1 and 2 and of §1, Theorem, is the following

PROPOSITION 3. *A group with property (P.n) defines an orthogonality relation (§1, Definition).*

PROPOSITION 4. *If ϕ has Property (P.n), then there exists to every pair of orthogonal lines an involution interchanging them.*

Proof. Suppose that L' and L'' are lines orthogonal with respect to the orthogonality relation defined by ϕ . Then we have

$$V = L' \oplus L'' \oplus (L' \oplus L'')^\phi, \quad L''^\phi = L' \oplus (L' \oplus L'')^\phi.$$

There exists a basis b_1, \dots, b_n of V such that $(L' \oplus L'')^\phi = \sum_{i=1}^{n-2} Fb_i$, $L' = Fb_{n-1}$, $L'' = Fb_n$. We infer from (P.n) the existence of a transformation σ in ϕ such that

$$\begin{aligned} \left[\sum_{j=1}^{i-1} Fb_j + Pb_i \right] \sigma &= \sum_{j=1}^{i-1} Fb_j + Pb_i & \text{for } i = 1, \dots, n-2, \\ \left[\sum_{j=1}^{n-2} Fb_j + Pb_{n-1} \right] \sigma &= \sum_{j=1}^{n-2} Fb_j + Pb_n, \\ \left[\sum_{j=1}^{n-1} Fb_j + Pb_n \right] \sigma &= \sum_{j=1}^{n-2} Fb_j + Fb_n + Pb_{n-1}. \end{aligned}$$

Since σ leaves invariant the subspace $(L' \oplus L'')^\phi$, it follows from §1, (f) that σ leaves invariant also the subspace $L' \oplus L''$. Thus the last two formulas defining σ reduce to $[Pb_{n-1}]\sigma = Pb_n$ and $[Pb_n]\sigma \leq Fb_n + Pb_{n-1}$. But $[Fb_{n-1}]\sigma$ and $[Fb_n]\sigma$ are orthogonal too; and thus it follows from the last inequality that $[Pb_n]\sigma = Pb_{n-1}$. Consequently σ^2 leaves invariant every half-subspace $\sum_{j=1}^{i-1} Fb_j + Pb_i$; and the uniqueness part of (P.n) shows that $\sigma^2 = 1$. Hence σ is the desired involution interchanging L' and L'' .

PROPOSITION 5. *If ϕ has Property (P.n), and if $2 < n$, then*

(T) *there exists to every pair of lines L', L'' in V a product σ of involutions in ϕ such that $L'\sigma = L''$.*

This is an almost immediate consequence of Proposition 4, since because of $2 < n$ there exists a line L orthogonal to both L' and L'' .

3. The form of a group.

THEOREM. *If the group ϕ of linear transformations of the vector space V over F has Properties (J), (E), (T), and if the dimension n of V is at least 3, then*

the field F is Pythagorean and there exists a symmetrical, positive definite bilinear form $f(x, y)$ [from V to F] such that ϕ consists of all the linear transformations preserving f .

Proof. We infer from §2, Proposition 2, the validity of (U). Thus conditions (U) and (E) of §1, Theorem are satisfied by ϕ ; and this shows that ϕ defines an orthogonality relation S^ϕ . Since $2 < n$, there exists an involutorial anti-automorphism α of F and a bilinear form $f(x, y)$ from V to F with the following properties:

$$(1) f(cx, y) = cf(x, y), f(x, cy) = f(x, y)c^\alpha \text{ for } x, y \text{ in } V, c \text{ in } F.$$

$$(2) f(x, y) = f(y, x)^\alpha \text{ for } x, y \text{ in } V.$$

$$(3) f(x, x) = 0 \text{ implies } x = 0.$$

$$(4) f(e, e) = 1 \text{ for some } e \text{ in } V.$$

(5) If S is a subspace of V , then S^ϕ is the totality of solutions v of the equation $f(S, v) = 0$.

(For a proof of this theorem, see Birkhoff-von Neumann [1, Appendix, pp. 837-843]). It is important to note that this is the only application of the hypothesis $2 < n$ which we are going to make in the course of this proof.

The linear transformation τ of V preserves f , if $f(x, y) = f(x\tau, y\tau)$ for every x and y in V . The following easily verified and presumably well known fact will be convenient to use.

(3.1) The linear transformation τ of V preserves f , if $f(x, x) = f(x\tau, x\tau)$ for every x in V .

Next we prove:

(3.2) The involution σ belongs to ϕ if, and only if, σ preserves f .

If σ is an involution in ϕ , then we have $R(\sigma) = J(\sigma)^\phi$ [see §1]; and it follows from (2) and (5) that

$$f(u, v) = f(v, u) = 0 \quad \text{for } u \text{ in } J(\sigma) \text{ and } v \text{ in } R(\sigma).$$

From $V = J(\sigma) \oplus R(\sigma)$ it follows that every vector z has the form $z = z' + z''$ with z' in $J(\sigma)$ and z'' in $R(\sigma)$. Consequently

$$\begin{aligned} f(x\sigma, y\sigma) &= f(x' - x'', y' - y'') = f(x', y') + f(x'', y'') \\ &= f(x' + x'', y' + y'') = f(x, y), \end{aligned}$$

so that σ preserves f .

If conversely σ preserves f , and if u is in $J(\sigma)$ and v in $R(\sigma)$, then $f(u, v) = f(u\sigma, v\sigma) = f(u, -v) = -f(u, v)$, so that $f(u, v) = 0$, since the characteristic of F is different from 2. It follows from (5) that $R(\sigma) \leq J(\sigma)^\phi$; and this implies $R(\sigma) = J(\sigma)^\phi$, since $V = J(\sigma) \oplus R(\sigma)$. Hence we have, in the notation of §1, $\sigma = \sigma[J(\sigma)]$ so that σ belongs to ϕ .

(3.3) To every vector v in V there exists a number r in F such that $f(v, v) = rr^\alpha$.

If $v \neq 0$ is a vector in V , then Fv is a line. We infer from (T) the existence of a product τ of involutions in ϕ such that $Fe = (Fv)\tau$. It follows from (3.2)

that τ preserves f ; and it follows from our choice of τ that $v\tau = re$ with r in F . Now it follows from (1) and (4) that $f(v, v) = f(v\tau, v\tau) = f(re, re) = rf(e, e)r^\alpha = rr^\alpha$, as we claimed.

$$(3.4) \quad \alpha = 1.$$

Since Fe is a line, $E = (Fe)^\phi$ is a hyperplane which contains naturally a vector $w \neq 0$. We infer from (3.3) the existence of a number r in F such that $f(w, w) = rr^\alpha$, and $r \neq 0$ by (3). Then $v = r^{-1}w$ is a vector in E which satisfies $f(v, v) = 1$, $f(e, v) = f(v, e) = 0$. From $f(e-v, e+v) = f(e, e) - f(v, v) = 0$ and (5) we infer that the hyperplane $[F(e-v)]^\phi$ contains the hyperplane $F(e+v) + (Fe + Fv)^\phi$. Hence $[F(e-v)]^\phi = F(e+v) + (Fe + Fv)^\phi$ and consequently there exists an involution σ in ϕ such that

$$J(\sigma) = F(e+v) + (Fe + Fv)^\phi, \quad R(\sigma) = F(e-v).$$

From $2e\sigma = (e+v)\sigma + (e-v)\sigma = e+v - (e-v) = 2v$ we infer $e\sigma = v$, so that $v\sigma = e$.

Consider now a number j in F which satisfies $jj^\alpha = 1$. Then we have $f(e-jv, e+jv) = f(e, e) - jf(v, v)j^\alpha = 1 - jj^\alpha = 0$. As before we see that $[F(e-jv)]^\phi = F(e+jv) + (Fe + Fv)^\phi$ and that there exists an involution σ' in ϕ such that

$$J(\sigma') = F(e+jv) + (Fe + Fv)^\phi, \quad R(\sigma') = F(e-jv).$$

From $2e\sigma' = (e+jv)\sigma' + (e-jv)\sigma' = e+jv - (e-jv) = 2jv$ we infer $e\sigma' = jv$ and $v\sigma' = j^{-1}e = j^\alpha e$.

Since σ and σ' belong to ϕ , so does $\sigma\sigma'$. We have clearly $x\sigma\sigma' = x$ for x in $(Fe + Fv)^\phi$, $e\sigma\sigma' = v\sigma' = j^\alpha e$, $v\sigma\sigma' = e\sigma' = jv$. Since $V = Fe \oplus Fv \oplus (Fe + Fv)^\phi$, it follows from (J) that $\sigma\sigma'$ is an involution. Hence $v = v(\sigma\sigma')^2 = j^2v$ or $j^2 = 1$. But F is a field; and thus we have shown that

$$(*) \quad jj^\alpha = 1 \quad \text{if, and only if,} \quad j = \pm 1.$$

If z is any element in F , then let $c = z - z^\alpha$. From $\alpha^2 = 1$ we infer $c^\alpha = -c$. Since the characteristic of F is not 2, this implies that c is neither $+1$ nor -1 . Thus we may form $j = (1+c)(1-c)^{-1}$. Since the elements $1+c$, $1-c$ and their inverses commute with each other, it follows that

$$jj^\alpha = (1+c)(1-c)^{-1}(1-c^\alpha)^{-1}(1+c^\alpha) = 1.$$

Hence $j = \pm 1$ by (*). If j were -1 , then we would have $1+c = c-1$, which is impossible, since the characteristic of F is not 2. Hence $j = 1$, so that $1+c = 1-c$ or $0 = c = z - z^\alpha$. Hence $z = z^\alpha$ for every z in F or $\alpha = 1$, as we intended to show.

(3.5) *F is Pythagorean.*

Since $\alpha = 1$ is an anti-automorphism of F , F is a commutative field. In the proof of (3.4) we showed the existence of vectors e and v such that $f(e, e) = f(v, v) = 1$, $f(e, v) = f(v, e) = 0$. If t is a number in F , then we infer from (3.3) and (3.4) the existence of a number r in F such that

$$r^2 = rr^\alpha = f(e + tv, e + tv) = f(e, e) + tf(v, v)t^\alpha = 1 + t^2;$$

and from (3) we deduce that $r \neq 0$. Now it is quite easy to show that the field F is formally real [no sum of squares equals -1] and therefore possesses at least one algebraical ordering; and this completes the proof of the Pythagorean character of the field F .

(3.6) *If L' and L'' are lines in V , then there exists an involution σ in ϕ which interchanges L' and L'' and which satisfies $(L' + L'')^\phi \leq J(\sigma)$.*

From (3.3) we deduce the existence of vectors v', v'' such that $f(v', v') = f(v'', v'') = 1$ and $L' = Fv', L'' = Fv''$. From (2) and $\alpha = 1$ we infer that

$$f(v' + v'', v' - v'') = f(v', v') + f(v'', v'') - f(v', v'') - f(v'', v') = 0.$$

Consequently $[F(v' - v'')]^\phi$ contains $F(v' + v'') + (L' + L'')^\phi$. If—as we may assume without loss in generality— $L' \neq L''$, then $[F(v' - v'')]^\phi$ and $F(v' + v'') + (L' + L'')^\phi$ are hyperplanes, and this implies $[F(v' - v'')]^\phi = F(v' + v'') + (L' + L'')^\phi$. Consequently there exists an involution σ in ϕ such that

$$J(\sigma) = F(v' + v'') + (L' + L'')^\phi, \quad R(\sigma) = F(v' - v''),$$

and it is fairly obvious that σ interchanges v' and v'' and therefore meets all the requirements.

(3.7) *If L'_1, \dots, L'_n and L''_1, \dots, L''_n are two sets of mutually orthogonal lines in V , then there exists a product τ of involutions in ϕ such that $L'_i \tau = L''_i$ for $i = 1, \dots, n$.*

This one deduces from (3.6) by an obvious inductive procedure.

(3.8) *The following three properties of the linear transformation τ of V are equivalent.*

- (i) τ is in ϕ .
- (ii) τ is a product of involutions in ϕ .
- (iii) τ preserves f .

Let us assume first that τ belongs to ϕ . There exists a set of n mutually orthogonal lines L_1, \dots, L_n in V , as follows by the usual argument from $V = S \oplus S^\phi$. Since τ belongs to ϕ , the lines $L_i \tau$ are mutually orthogonal too (§1, (f)). There exists by (3.7) a product τ' of involutions in ϕ such that $L_i = L_i \tau \tau'$ for every i . It follows from Property (J) that the transformation $\tau \tau'$ in ϕ is an involution in ϕ . Hence τ itself is a product of involutions in ϕ . Thus (i) implies (ii).

That (ii) implies (iii) is a consequence of (3.2).

Assume finally that τ preserves f . If the lines L_i are mutually orthogonal, so are the lines $L_i \tau$, since $0 = f(L_i, L_j) = f(L_i \tau, L_j \tau)$ for $i \neq j$. Consequently there exists by (3.7) a product τ' of involutions in ϕ such that $L_i = L_i \tau \tau'$ for every i . It follows from (3.2) that τ' and hence $\tau \tau'$ preserves f . If $L_i = Fv_i$, then $v_i \tau \tau' = k_i v_i$ for $k_i \neq 0$ in F , and

$$f(v_i, v_i) = f(v_i \tau \tau', v_i \tau \tau') = k_i^2 f(v_i, v_i) \quad \text{or} \quad k_i^2 = 1$$

because of (3) and (3.5). Hence $k_i = \pm 1$; and this shows that $\tau\tau'$ is an involution preserving f . It follows from (3.2) that $\tau\tau'$ and therefore τ is in ϕ ; and this completes the proof of (3.8).

Because of their importance, two special cases of (3.9) should be mentioned: ϕ is generated by the involutions in ϕ , and ϕ is the totality of linear transformations of V which preserve f .

(3.9) f is a symmetrical, positive definite bilinear form.

That f is a symmetrical bilinear form is a consequence of (2) and (3.4). There exist n mutually orthogonal lines L_i , and from (3.3) we deduce the existence of vectors v_i such that $L_i = Fv_i$ and $f(v_i, v_i) = 1$. The vectors v_i form a basis of V ; and every vector x has the form $x = \sum_{i=1}^n x_i v_i$. Clearly $f(x, x) = \sum_{i=1}^n x_i^2$. It follows from (3.5) that a sum of squares, not all 0, is a square not 0. Hence $f(x, x)$ is positive definite, as we claimed.

This completes the proof of our theorem.

4. The group of a form.

THEOREM. *If the field F is Pythagorean, if f is a symmetrical, positive definite bilinear form [from the n -dimensional vector space V over F to F], and if P is a domain of positivity of F [in the weak sense], then the group Γ of all the linear transformations of V which preserve f has Property (P.n).*

Proof. To every basis b_1, \dots, b_n of V there exists one and only one basis b'_1, \dots, b'_n of V such that

$$f(b'_i, b'_j) = \begin{cases} 1 & \text{for } i = j \\ 0 & \text{for } i \neq j \end{cases} \text{ and } \sum_{i=1}^{i-1} Fb_i + Pb_i = \sum_{i=1}^{i-1} Fb'_i + Pb'_i$$

for $i = 1, \dots, n$,

as one sees by a fairly obvious inductive argument [E. Schmidt's orthogonalization procedure]. The validity of (P.n) may now be derived by fairly obvious arguments.

We note here without proof the fact that the existence of a symmetrical, positive definite bilinear form from V to F implies the Pythagorean character of F .

5. Characterization of the full orthogonal group. The results of the preceding considerations show the equivalence of the following properties of the group ϕ of linear transformations of the n -dimensional vector space V over the field F , provided the characteristic of F is not 2 and $2 < n$:

- (1) F possesses a domain of positivity and ϕ satisfies (P.n) for every domain P of positivity.
- (2) There exists a domain P of positivity of F such that ϕ satisfies (P.n).
- (3) ϕ meets requirements (E), (J), (T).
- (4) ϕ defines an orthogonality relation and satisfies (J), (T).
- (5) F is Pythagorean and there exists a symmetrical, positive definite

bilinear form f such that ϕ consists of all the linear transformations of V preserving f .

If ϕ is a group of linear transformations of V which satisfies these equivalent conditions (1) to (5), then we shall term ϕ a *full orthogonal group* of V . As long as the equivalence of properties (1) to (5) has not been verified for $n=2$, we shall refrain from using this term for groups of linear transformations of the plane. Whenever F is Pythagorean, it is possible to construct a symmetrical, positive definite bilinear form; and thus the Pythagorean character of F is necessary and sufficient for the existence of a full orthogonal group of V . It is clear that every symmetrical, positive definite bilinear form may be brought into the form $f(x, y) = \sum_{i=1}^n x_i y_i$ by an appropriate choice of a basis of V ; and consequently any two full orthogonal groups of V are conjugate in the group of all linear transformations of V . Thus we see that Theorem A and its corollaries as stated in the introduction are consequences of the preceding theorems.

6. Euclidean fields of coordinates. A field F may be termed *Euclidean*, if it is commutative, formally real, and has the further property that one and only one of the numbers x and $-x$, for $x \neq 0$, is a square in F . Clearly every Euclidean field is Pythagorean and every real closed field is Euclidean. Thus vector spaces over Euclidean fields form a particularly important special case of our discussion; and in this special case we shall be able to remove some of the more obnoxious restrictions from our principal results.

PROPOSITION 1. *If V is an n -dimensional vector space over the Euclidean field F , if $2 < n$, and if the group ϕ of linear transformations of V defines an orthogonality relation, then*

(T*) *there exists to any two lines in V an involution in ϕ which interchanges them.*

Proof. As in the proof of §3, Theorem there exists an involutorial automorphism α of F and a bilinear form $f(x, y)$ from V to F which satisfies the rules (1) to (5) of §3. We prove

$$(1.1) \quad \alpha = 1.$$

If this were not true, then α would be an automorphism of order 2. Denote by D the totality of elements in F invariant under α . It follows from Galois theory that $[F:D]=2$ and that therefore $F=D(q)$ where q^2 is in D , though q is not. Since F is Euclidean, and since we may substitute $-q$ for q , we may assume without loss in generality that q is a square of an element in F . Hence there exist elements d', d'' in D such that $q=(d'+d''q)^2$. From $[F:D]=2$ it follows now that $2d'd''=1$ and $d'^2+q^2d''^2=0$. Since F is formally real, $d'=0$, which is impossible. Hence $\alpha=1$.

(1.2) *f is a symmetrical, positive definite bilinear form.*

From (1.1) and §3, (2) it follows that f is a symmetrical bilinear form.

Suppose now that the vector v is orthogonal to the vector e with $f(e, e) = 1$ (§3, (4)). If $f(v, v)$ were not a square in F , then it would follow from the Euclidean character of F that $f(v, v) = -c^2$ for c in F ; and this would imply $f(ce+v, ce+v) = 0$, which contradicts §3, (3). Thus $f(v, v)$ is a square in F for every v in $(Fe)^\phi$. If x is any vector in V , then $x = te + v$ with v in $(Fe)^\phi$. Hence $f(x, x) = t^2 + f(v, v)$ is the sum of two squares and therefore a square since F is Euclidean and hence Pythagorean. Now it follows from §3, (3) that f is positive definite.

Because of (1.2), any two lines in V have the form Fs' , Fs'' with $f(s', s') = f(s'', s'') = 1$. Then $f(s' + s'', s' - s'') = 0$, and it follows as usual that $[F(s' - s'')]^\phi = F(s' + s'') + (Fs' + Fs'')^\phi$, provided $Fs' \neq Fs''$. Consequently ϕ contains an involution σ such that $J(\sigma) = F(s' + s'') + (Fs' + Fs'')^\phi$, $R(\sigma) = F(s' - s'')$. Clearly $s'\sigma = s''$ and $s''\sigma = s'$, and this completes the proof.

REMARK 1. Proposition 1 would cease to be true without some hypothesis of the type considered here. Consider for instance the full orthogonal group of the n -dimensional vector space with rational coefficients. This group certainly has Properties (U), (E), (J), but if it also had Property (T) or the sharper property (T*), then it would follow from §3, Theorem that the field of rational numbers were Pythagorean, which certainly is not the case.

REMARK 2. That Condition (J) cannot be deduced from (U), (E), (T*) may be seen from the group of all orthogonality preserving linear transformations.

PROPOSITION 2. *The following properties of the group ϕ of linear transformations of the two-dimensional vector space V over the Euclidean field F are equivalent.*

- (i) ϕ has Property (P.2) where P is the set of all squares not 0.
- (ii) ϕ has Properties (E), (J), (T*).
- (iii) There exists a symmetrical, positive definite bilinear form $f(x, y)$ [from V to F] such that ϕ is the totality of linear transformations preserving f .

Proof. Assume the validity of (i). Then we infer the validity of (E), (J) from §2, Proposition 1. Consider two different lines Fa and Fb in V . Then $V = Fa \oplus Fb$; and we deduce from (P.2) the existence of one and only one transformation σ in ϕ such that $Pa\sigma = Pb$, $[Fa + Pb]\sigma = Fb + Pa$. Hence $a\sigma = pb$, $b\sigma = tb + qa$ where p and q are in P [are squares, not 0, in F]. Then $t^2 + 4pq$ belongs to P and is consequently a square, not 0, in F . The equation $qy^2 - ty - p = 0$ has therefore a solution y in F . The vector $v = a + yb$ satisfies $v\sigma = yqv$ so that $Fv = (Fv)\sigma$. Since $v \neq 0$, we may apply Property (J) so that σ is an involution. Hence $a = a\sigma^2 = p(tb + qa)$, so that $t = 0$. Consequently $Fa\sigma = Fb$ and $Fb\sigma = Fa$, and this proves (T*). Thus (ii) is a consequence of (i).

Assume next the validity of (ii). We infer from §2, Proposition 2 and §1, Theorem that ϕ defines an orthogonality relation. Select at random a vector $e \neq 0$ in V . Then we prove:

(ii.1) To every vector v in V there exists one and only one number v^2 in F with the following properties:

(a) If σ is in ϕ and $v = te\sigma$, then $t^2 = v^2$, and ϕ contains such transformations σ .

(b) $v^2 = (v\tau)^2$ for τ in ϕ .

(c) $(cv)^2 = c^2v^2$ for c in F .

Clearly $0^2 = 0$; and thus we may assume $v \neq 0$. From (T*) we deduce the existence of an involution σ in ϕ such that $(Fe)\sigma = Fv$. If σ' and σ'' are transformations in ϕ such that $v = t'e\sigma'$ and $v = t''e\sigma''$, then $(Fe)\sigma'\sigma''^{-1} = Fe$. It follows from (J) that $\sigma'\sigma''^{-1}$ is an involution and that therefore $e\sigma'\sigma''^{-1} = \pm e$. Hence $t' = \pm t''$ or $t'^2 = t''^2$; now it is fairly obvious how to complete the proof of (ii.1).

(ii.2) If $a \neq 0$ and b are vectors in V , then there exists one and only one number $g(b, a)$ in F such that a and $b - g(b, a)a$ are orthogonal vectors.

This is an immediate consequence from $V = Fa \oplus (Fa)^\phi$.

If σ is the uniquely determined involution in ϕ such that $Fa = J(\sigma)$, then $b + b\sigma = 2g(b, a)a$; and one verifies easily the following properties of the function $g(b, a)$:

$$\begin{aligned} g(b' + b'', a) &= g(b', a) + g(b'', a), \\ g(cb, a) &= cg(b, a), \quad g(b, ca) = g(b, a)c^{-1}, \\ g(b\tau, a\tau) &= g(b, a) \quad \text{for } \tau \text{ in } \phi. \end{aligned}$$

Now we define

$$f(b, a) = \begin{cases} g(b, a)a^2 & \text{for } a \neq 0, \\ 0 & \text{for } a = 0. \end{cases}$$

This function $f(b, a)$ has clearly the following properties:

$$\begin{aligned} f(b' + b'', a) &= f(b', a) + f(b'', a), \quad f(cb, a) = cf(b, a), \\ f(b\tau, a\tau) &= f(b, a) \quad \text{for } \tau \text{ in } \phi, \end{aligned}$$

the vectors b and a are orthogonal if, and only if, $f(b, a) = 0$.

Suppose now that neither of the vectors a and b is 0. Then there exists by (T*) an involution σ in ϕ interchanging the lines Fa and Fb . Clearly $a\sigma = sb$, $b\sigma = s^{-1}a$, $a^2 = (a\sigma)^2 = s^2b^2$. Consequently

$$\begin{aligned} f(b, a) &= f(b\sigma, a\sigma) = g(s^{-1}a, sb)(a\sigma)^2 = s^{-1}g(a, b)s^{-1}a^2 \\ &= g(a, b)b^2 = f(a, b), \end{aligned}$$

since F is commutative; and thus we have shown:

(ii.3) $f(x, y)$ is a symmetrical bilinear form such that the vectors a and b are orthogonal if, and only if, $f(a, b) = 0$ and such that every transformation in ϕ preserves f .

The validity of (iii) is now a consequence from the proof of §3, Theorem, since the hypothesis $2 < n$ had been used there only to prove the existence of f , which we showed here independently.

That (iii) implies (i) is shown now as in §4.

REMARK 3. The hypothesis that F be Euclidean has been used fully only when proving that (i) implies (ii). When proving that (ii) implies (iii), we needed the commutativity of F , and our argument would have sufficed then to show that F is Pythagorean.

REMARK 4. The method of proof used when deducing (iii) from (ii) and (ii) from (i) is very similar to a method used by Pickert [1, p. 496] when dealing with the proper orthogonal group of three-dimensional space. Results of Iyanaga-Abe [1] could have been used too.

CHAPTER II. THE PROPER ORTHOGONAL GROUP

7. The general free mobility condition. If V is an n -dimensional vector space over F , and if P is a domain of positivity of F [in the weak sense of §2], then i -dimensional free mobility of the group ϕ of linear transformations of V is expressed by the following property.

(P.i) If b'_1, \dots, b'_i and b''_1, \dots, b''_i are two sets of i independent vectors in V , then there exists one and only one transformation τ in ϕ such that $[\sum_{j=1}^{i-1} Fb'_j + Pb'_i]\tau = \sum_{j=1}^{i-1} Fb''_j + Pb''_i$ for $k=1, \dots, i$.

THEOREM. If ϕ has Property (P.i), and if $i < n-1$, then $i=1$.

Proof. It is clear that (P.i) implies the following property.

(U*) If τ in ϕ leaves invariant every vector in some i -dimensional subspace of V , then $\tau=1$.

Consider now some i -dimensional subspace S of V ; and denote by θ the totality of transformations τ in ϕ such that $S=S\tau$. It is clear that θ is a subgroup of ϕ ; and it follows from (U*) that θ is essentially the same as the group of linear transformations which it induces in S . This induced group has likewise Property (P.i), and thus it follows from §2, Proposition 3 that

(0) θ defines an orthogonality relation in S .

Consider now an $(i-1)$ -dimensional subspace T' of S . Then there exists one and only one involution σ' in θ such that $T'=S \cap J(\sigma')$ [since, by (U*), transformations are involutions, if they induce involutions in S]. Since $\sigma' \neq 1$, it follows from (U*) that $J(\sigma')$ has dimension less than i ; and since T' has dimension $i-1$, this implies $T'=J(\sigma')$. From $V=J(\sigma') \oplus (R\sigma')$ we deduce that $S=J(\sigma') \oplus L'$, where $L'=S \cap R(\sigma')$ is a line in S .

Assume now that $1 < i$. Then there exists an $(i-2)$ -dimensional subspace N of T' , and we may form the $(i-1)$ -dimensional subspace $T''=N \oplus L'$ of S . As before there exists an involution σ'' in θ such that $T''=J(\sigma'')$, $S=J(\sigma'') \oplus L''$, where $L''=S \cap R(\sigma'')$ is a line in S . If we denote the orthogonality relation which θ defines in S by the exponent θ , then we have $T'^\theta=L'$,

$T''^\theta = L''$, and it follows from $L' \leq T''$ that $L'' = T''^\theta \leq L'^\theta = T'$. Since L'' is not part of T'' , L'' is not part of N either; and it follows that

$$T'' = L' \oplus N, \quad N = T' \cap T'', \quad T'' = L' \oplus N, \quad S = L' \oplus L'' \oplus N.$$

If we remember that $T' = J(\sigma')$, $T'' = J(\sigma'')$, $L' \leq R(\sigma')$, $L'' \leq R(\sigma'')$, it follows that σ' and σ'' commute on S , and that their product is an involution on S . It follows from (U*) that $\sigma'\sigma'' = \sigma''\sigma'$ is an involution in θ and ϕ . From $\sigma' \neq \sigma''$ we deduce furthermore $\sigma'\sigma'' \neq 1$. From $\sigma'\sigma'' = \sigma''\sigma'$ one deduces easily that

$$R(\sigma'\sigma'') = [J(\sigma') \cap R(\sigma'')] \oplus [J(\sigma'') \cap R(\sigma')] \leq L'' \oplus L'.$$

Hence the dimension of $R(\sigma'\sigma'')$ is at most 2, and it follows from (U*) and $V = J(\sigma'\sigma'') \oplus R(\sigma'\sigma'')$ that

$$n - 2 \leq \text{dimension of } J(\sigma'\sigma'') \leq i - 1 \quad \text{or} \quad n - 1 \leq i,$$

as we intended to prove.

REMARK 1. In the proof of the preceding theorem we used, apart from (U*), only the following property of ϕ .

There exists an i -dimensional subspace S of V in which ϕ defines an orthogonality relation.

REMARK 2. Property (P. n) is just the property characteristic for the full orthogonal group which we discussed in Chapter 1. The property (P. $n-1$) is satisfied by all the proper orthogonal groups; and will be our object of investigation in the remainder of Chapter II. Concerning (P.1) we make the following observations. A nontrivial example is provided by the real quaternions of absolute value 1 which by post-multiplication produce in the four-dimensional real space of real quaternions just a group of linear transformations with this property (P.1). It appears furthermore that the determination of all groups of linear transformations with this property leads to interesting problems in the theory of non-distributive fields.

8. Mutual determination of full and proper orthogonal groups. If V is vector space over F of dimension not less than 3, and if ϕ is a full orthogonal group of V , then F is a Pythagorean field (§5) and consequently commutative. Thus every transformation in ϕ has a uniquely determined determinant which is either $+1$ or -1 , since ϕ is generated by its involutions [§3, (3.8)]; and the transformations of determinant $+1$ form a subgroup of index 2 which is called the *proper orthogonal group* ϕ_+ . The relation between ϕ and ϕ_+ is even closer than this and may be described in purely group theoretical terms. This we are going to do now.

PROPOSITION 1. *A full orthogonal group possesses one and only one subgroup of index 2.*

Proof. If ϕ is a full orthogonal group of V , then ϕ has the properties (1)

to (5) of §5; and that ϕ then possesses a subgroup of index 2 has already been mentioned. We show next:

(8.1) *If the normal subgroup θ of ϕ contains an involution σ with one-dimensional $R(\sigma)$, then $\phi = \theta$.*

ϕ is certainly transitive on the lines in V . Consequently any two involutions in ϕ with one-dimensional R are conjugate in ϕ . It follows therefore from our hypotheses that θ contains all involutions in ϕ whose R is one-dimensional; and this implies that θ contains all the involutions in ϕ . But ϕ is generated by its involutions [§3, (3.8)]. Hence $\theta = \phi$, as we claimed.

Suppose now that θ is a subgroup of index 2 of ϕ . Then θ is normal in ϕ , but different from ϕ ; and so it follows from (8.1) that θ does not contain the involutions with one-dimensional R . Noting that every transformation in ϕ is the product of involutions with one-dimensional R and that the involutions with one-dimensional R have determinant -1 , it is now easy to verify that the subgroup θ of index 2 consists exactly of those transformations in ϕ whose determinant is $+1$. Hence $\theta = \phi_+$; this completes the proof.

PROPOSITION 2. *A proper orthogonal group is the subgroup of index 2 of one and only one full orthogonal group.*

Proof. Suppose that the full orthogonal groups ϕ' and ϕ'' have a common subgroup θ of index 2. Then they define orthogonality relations $S^{\phi'}$ and $S^{\phi''}$. Suppose now that the vectors x and y in V are orthogonal with respect to ϕ' . We may assume that neither x nor y is 0. Then x belongs to the hyperplane $(Fy)^{\phi'}$ and y belongs to the hyperplane $(Fx)^{\phi'}$. If we let $N = (Fx)^{\phi'} \cap (Fy)^{\phi'} = (Fx + Fy)^{\phi'}$, then N has the positive dimension $n-2$ and $(Fx)^{\phi'} = Fy \oplus N$, $(Fy)^{\phi'} = Fx \oplus N$. Denote by $z \neq 0$ some vector in N . Then $Fx \oplus Fz$ has dimension 2, and there exists one and only one involution σ in ϕ' such that $R(\sigma) = Fx + Fz$. Clearly

$$\begin{aligned} Fy &\leq [Fx]^{\phi'} \cap [Fx + Fy] = [Fx]^{\phi'} \cap N^{\phi'} \leq [Fx]^{\phi'} \cap [Fz]^{\phi'} \\ &\leq (Fx + Fz)^{\phi'} = J(\sigma). \end{aligned}$$

Since σ has determinant $+1$, it follows from Proposition 1 that σ is in θ . But θ is part of ϕ'' . Since σ belongs to ϕ'' , and since y is in $J(\sigma)$ and x in $R(\sigma)$, it follows that x and y are also orthogonal with respect to ϕ'' . By reasons of symmetry we see now that ϕ' and ϕ'' define the same orthogonality relation in V . But this last fact shows that ϕ' and ϕ'' contain the same involutions. Since full orthogonal groups are generated by their involutions [§3, (3.8)], this implies $\phi' = \phi''$; this completes the proof.

9. The odd-dimensional case. Throughout this section we shall assume that the dimension n of the vector space V over F is at least 3.

PROPOSITION 1. *If θ is a proper orthogonal group of V , then F possesses domains of positivity and θ satisfies (P. $n-1$) for every domain P of positivity.*

Proof. θ is the subgroup of index 2 of one and only one full orthogonal group ϕ of V [§8, Proposition 2]. Consequently there exist domains of positivity in F , and ϕ satisfies (P. n) for each of them. If C' and C'' are two $(n-1)$ -dimensional chains of incident sub-half-spaces of V , then there exist exactly two transformations σ', σ'' in ϕ such that $C'\sigma' = C'' = C'\sigma''$. It is easily seen that $\sigma'\sigma''^{-1}$ is an involution with $J(\sigma'\sigma''^{-1})$ a hyperplane. Thus $R(\sigma'\sigma''^{-1})$ is a line and $\sigma'\sigma''^{-1}$ does not belong to θ [§8, (8.1)]. Hence one and only one of the transformations σ', σ'' belongs to θ and, consequently, (P. $n-1$) is satisfied by θ .

PROPOSITION 2. *A group θ with property (P. $n-1$) for some domain P of positivity has properties (J), (T) (of §2) and the following properties.*

(U*) *If σ in θ leaves invariant every vector of a hyperplane, then $\sigma = 1$.*

(E*) *If S is a subspace of a hyperplane H of V , then there exist involutions σ', σ'' in θ such that $S = H \cap J(\sigma') = H \cap R(\sigma'')$.*

Proof. (U*) is an immediate consequence of the uniqueness assertion in (P. $n-1$). If H is a hyperplane in V , then the group $\theta(H)$ of all the transformations in θ which transform H into itself is essentially the same as the group of transformations it induces in H [by (U*)], and this latter group has property (P. $n-1$) too. Applying §2, Propositions 1 and 3 and §1, Theorem on the group induced by $\theta(H)$ in H , we deduce the validity of (J) and (E*), whereas §2, Proposition 5 gives the validity of (T) in case $3 < n$. To treat the remaining case $3 = n$ we deduce from §2, Proposition 4 the validity of the following condition:

(T₀) *If L', L'' are different lines, and if there exists an involution σ in θ such that $L' \leq J(\sigma)$, $L'' \leq R(\sigma)$, then there exists an involution in θ which interchanges L' and L'' .*

Consider now two different lines A and B in the three-dimensional space V . Then $A \oplus B = D$ is a plane, and we infer from (E*) the existence of involutions σ', σ'' in θ such that $A = D \cap J(\sigma')$, $B = D \cap J(\sigma'')$. It follows from (U*) that $J(\sigma')$, $J(\sigma'')$ cannot be planes, and thus it follows from $\sigma' \neq 1$, $\sigma'' \neq 1$ that $A = J(\sigma')$, $B = J(\sigma'')$. Consequently $R(\sigma')$ and $R(\sigma'')$ are planes in the three-dimensional space V , and as such they have a line L in common. Now we deduce from (T₀) the existence of involutions in θ which interchange A and L , L and B so that θ contains a product of involutions which maps A upon B . Thus (T) has been verified in every case.

LEMMA. *If θ has properties (U*), (E*), (J), then $R(\sigma)$ has even dimension for every involution σ in θ .*

Proof. It is a consequence of (U*) that $R(\sigma)$ cannot be one-dimensional. Consider now an involution σ in θ such that $R(\sigma)$ has at least dimension 2. From $V = J(\sigma) \oplus R(\sigma)$ we deduce the existence of a basis b_i of V such that $J(\sigma) = \sum_{i=1}^{h-1} Fb_i$, $R(\sigma) = \sum_{i=h}^n Fb_i$. We deduce from (E*) the existence of an

involution σ' in θ such that $\sum_{i=1}^{n-2} Fb_i = J(\sigma') \cap [\sum_{i=1}^{n-1} Fb_i]$. Since $\sigma' \neq 1$, and since $R(\sigma')$ cannot be one-dimensional [by (U*)], though $J(\sigma')$ has at least dimension $n-2$, we infer $J(\sigma') = \sum_{i=1}^{n-2} Fb_i$. From $h < n$ we deduce $J(\sigma) \leq J(\sigma')$.

The transformation $\sigma\sigma'$ belongs to θ and has the following properties: $b_i\sigma\sigma' = \pm 1$ for $i \leq n-2$, $b_i\sigma\sigma' - b_i = -(b_i\sigma' + b_i)$ belongs to $J(\sigma') = \sum_{i=1}^{n-2} Fb_i$ for $n-2 < i$. It follows from (J) that $\sigma\sigma'$ is an involution so that in particular $\sigma\sigma' = \sigma'\sigma$. From $J(\sigma) \leq J(\sigma')$ we deduce now $R(\sigma') \leq R(\sigma)$ and $R(\sigma\sigma') = \sum_{i=1}^{n-2} Fb_i$. Thus we have found an involution $\sigma\sigma'$ in θ such that $R(\sigma\sigma')$ has a dimension exactly two less than the dimension of $R(\sigma)$. Now it is clear how to complete the proof of the evenness of the dimension of $R(\sigma)$.

PROPOSITION 3. *If θ has properties (U*), (J), (E*), (T), then the following properties are equivalent:*

- (i) *The dimension of V is odd.*
- (ii) *θ does not contain the reflection $vp = -v$.*
- (iii) *The group obtained by adjoining the reflection ρ to θ is a full orthogonal group, and θ is a proper orthogonal group.*

Proof. That (i) implies (ii) is a consequence of the preceding lemma. Assume now that the reflection ρ does not belong to θ . Denote by ϕ the group obtained by adjoining ρ to θ . Then ϕ is the direct product of θ and of the cyclic group of order 2, generated by ρ . Thus θ has index 2 in ϕ , and it is fairly clear that ϕ satisfies conditions (J) and (T). If H is some hyperplane, then we infer from (E*) the existence of an involution σ in θ such that $H \leq R(\sigma)$. From $V \neq R(\sigma)$ —otherwise σ would be ρ which by hypothesis is not in θ —we deduce $H = R(\sigma)$. Consequently $\sigma\rho$ is an involution in ϕ such that $H = J(\sigma\rho)$. Consider next some subspace S of H . We infer from (E*) the existence of an involution σ' in θ such that $S = J(\sigma') \cap H$. Either $S = J(\sigma')$ or else we consider $\sigma'\sigma\rho$. Since $\sigma'\sigma$ is an involution on H , and since $\sigma'\sigma$ belongs to θ , it follows from (U*) that $\sigma'\sigma$ is an involution in θ . Now we see that $\sigma'\sigma\rho$ is an involution in ϕ such that $S = J(\sigma'\sigma\rho)$. We deduce from §1, Corollary that an orthogonality relation is defined by ϕ , and now it follows from the principal result of §5 that ϕ is a full orthogonal group. Hence (iii) is a consequence of (ii). If (iii) is true, then ρ cannot be in θ , since θ because of (U*) cannot be the full orthogonal group. It follows from (E*) that θ contains an involution such that $R(\sigma)$ has dimension at least $n-1$. From $\sigma \neq \rho$ it follows that $R(\sigma)$ is a hyperplane; and now it follows from the preceding lemma that the dimension of hyperplanes is even and that of V is therefore odd. This completes the proof.

THEOREM. *If the dimension of V is odd, then the following properties of the group θ of linear transformations of V are equivalent:*

- (1) *θ is a proper orthogonal group.*
- (2) *There exists a domain of positivity of F , and θ satisfies (P. $n-1$) for domains P of positivity.*

(3) θ satisfies conditions (U^*) , (J) , (E^*) , (T) .

This is an almost immediate consequence of Propositions 1 to 3.

REMARK. It is easy to show by use of §6, Proposition 1 that condition (T) may be omitted from (3), in case the field F is euclidean. It is furthermore easy to see that condition (E^*) is a consequence of (U^*) and the following condition.

If S is a subspace of the hyperplane H , then there exists an involution σ in θ such that $S = H \cap R(\sigma)$.

10. The case of dimension greater than 3.

THEOREM. *If the dimension of the vector space V over F is greater than 3, then the following properties of the group θ of linear transformations of V are equivalent.*

- (i) θ is a proper orthogonal group.
- (ii) There exist domains of positivity of F , and θ satisfies $(P.n-1)$ for a domain P of positivity.
- (iii) If H is a hyperplane in V , and if $\theta(H)$ is the group of all transformations in θ which transform H into itself, then $\theta(H)$ is essentially the same as a full orthogonal group of H .

It is a consequence of §9, Proposition 1 that (i) implies (ii). If (ii) is true, then we infer from §9, Proposition 2 that $\theta(H)$ is essentially the same as the group of linear transformations it induces in H . Naturally this latter group satisfies $(P.n-1)$. But the dimension of the hyperplane H is at least 3, since $3 < n$, and thus it follows from the main result of Chapter I (§5) that $\theta(H)$ induces in H a full orthogonal group. Thus (iii) is a consequence of (ii).

Assume finally the validity of (iii). Since hyperplanes in V have dimension not less than 3, we may use all the results of §5. Applying in particular §5, (5) we obtain the validity of the following facts:

- (1) The field F is Pythagorean.
- (2) If H is a hyperplane in V , then there exists a symmetrical, positive definite bilinear form $f_H(x, y)$ from H to F such that $\theta(H)$ is essentially the same as the group of all linear transformations of H which preserve f_H .

We note that f_H is not uniquely determined, since $t^2 f_H$ with $t \neq 0$ in F has likewise all the required properties. As a matter of fact our main problem is to pick these forms "coherently."

- (3) If L is a line in V , then the group $\theta(L)$ of all the transformations in θ which transform L into itself is essentially the same as a full orthogonal group of V/L .

It is clear that $\theta(L)$ induces a group of linear transformations in V/L . Consider now a transformation σ in $\theta(L)$ which induces the identity in V/L . Then $v\sigma - v$ belongs to L for every v in V , and σ maps onto itself every subspace containing L . Apply this in particular onto some hyperplane H con-

taining L . Then σ belongs to $\theta(H)$, which is essentially the same as a full orthogonal group of H . Hence (J) is satisfied by this group of transformations of H , and it follows that σ is an involution. Since every $v\sigma - v$ is in L , it follows that $R(\sigma) \leq L$. Since $J(\sigma)$ cannot be a hyperplane—for otherwise a transformation, not 1, would be the identity on a hyperplane—it follows that $J(\sigma) = V$ or $\sigma = 1$. Thus we have shown that $\theta(L)$ is essentially the same as the group of transformations it induces in V/L .

Any two lines in V/L are represented by distinct planes B', B'' which both contain L . Their sum $B' + B''$ has dimension $3 < n$ and is consequently contained in some hyperplane H . It follows from (iii) that $\theta(H)$ defines an orthogonality in H , and $B' = L \oplus L', B'' = L \oplus L''$ where L' and L'' are lines orthogonal to L [in H]. Consequently there exists an involution in $\theta(H)$ which interchanges L' and L'' and which maps L upon itself, and thus we have found an involution in $\theta(L)$ which interchanges B' and B'' . Hence (T) is satisfied by the group $\theta(L)$ of transformations of V/L . It is fairly easy to see that (J) is satisfied by θ and consequently also by the group $\theta(L)$ of transformations of V/L .

From (iii) one deduces immediately that θ satisfies conditions (U*), (E*), (J) [see §9]; and thus it follows from §9, Lemma that $R(\sigma)$ is even-dimensional for every involution σ in θ .

Next we want to show that to every subspace T containing L there exists an involution σ in $\theta(L)$ such that $T = L + J(\sigma)$. To do this we may assume that T is part of some hyperplane H . If dimension V minus dimension T is even, then we consider the uniquely determined involution σ in $\theta(H)$ such that $T = H \cap J(\sigma)$. Since $R(\sigma)$ cannot have odd dimension, it follows that $J(\sigma) = T$ so that σ is a desired transformation in $\theta(L)$. If dimension V minus dimension T is odd, then we remember first that $\theta(H)$ defines an orthogonality relation in H and that therefore $T = L \oplus S$ where S is orthogonal to L in H . Next we consider the uniquely determined involution σ' in $\theta(H)$ such that $S = J(\sigma') \cap H$. Since dimension V minus dimension S is even, it follows as before that $J(\sigma') = S$. Since S and L are orthogonal in H , it follows that $L \leq R(\sigma')$ and that therefore σ' belongs to $\theta(L)$. Thus σ' is a desired transformation.

Using §1, Corollary we see now that $\theta(L)$ defines an orthogonality relation in V/L . Since the dimension of V/L is not less than 3, it follows now from §5, (4) that $\theta(L)$ induces a full orthogonal group in V/L . This completes the proof of (3).

(4) If σ is a transformation in θ , and if $v \neq 0$ is a vector in V such that $v\sigma = mv$, then $m = \pm 1$.

It is a consequence of (3) that $\theta(Fv)$ is essentially the same as the full orthogonal group of V/Fv . But this group is generated by its involutions (§3, (3.8)). Hence $\theta(Fv)$ is generated by the involutions in $\theta(Fv)$. It is clear

that every involution in $\theta(Fv)$ maps v upon $\pm v$, and these last two facts clearly imply (4).

If H is a hyperplane, if f is a symmetrical, positive definite bilinear form from H to F , and if $\theta(H)$ induces in H just the transformations which preserve f , then we term f a θ -admissible form of H . Proposition (2) asserts the existence of such forms.

(5) If H' and H'' are hyperplanes in V , if f' and f'' are θ -admissible forms of H' and H'' respectively, and if there exists a vector $e \neq 0$ in $H' \cap H''$ such that $f'(e, e) = f''(e, e)$, then

$$f'(x, y) = f''(x, y) \quad \text{for } x, y \text{ in } H' \cap H''.$$

Since the groups $\theta(H)$ induce in H groups with property (T), there exist to every $x \neq 0$ in $H' \cap H''$ transformations σ' and σ'' in $\theta(H')$ and $\theta(H'')$ respectively such that $F\sigma' = Fx = F\sigma''$. Hence $e\sigma' = z'x$ and $e\sigma'' = z''x$. Clearly $e\sigma'\sigma''^{-1} = z'z''^{-1}e$, and it follows from (4) that $z'z''^{-1} = \pm 1$ or $z'^2 = z''^2$. But then $f'(x, x) = z'^{-2}f'(e\sigma', e\sigma') = z'^{-2}f'(e, e) = z''^{-2}f''(e, e) = z''^{-2}f''(e\sigma'', e\sigma'') = f''(x, x)$, and now (5) is an immediate consequence of the well known identity

$$(*) \quad f(x, y) = 2^{-1}[f(x+y, x+y) - f(x, x) - f(y, y)]$$

which holds for all symmetrical bilinear forms.

(6) There exists a symmetrical, positive definite bilinear form f from V to F which induces θ -admissible forms f_H in all hyperplanes H .

We note first that because of $3 < n$ the intersection of three hyperplanes is not 0. Using (2) and (5) we can find easily θ -admissible forms f_H from H to F such that $f_{H'}$ and $f_{H''}$ coincide on $H' \cap H''$. There exists one and only one function $f(x, y)$ from V to F which coincides on every hyperplane H with f_H . This function f is the desired form, since because of $3 < n$ any three vectors are contained in some hyperplane.

(7) Every transformation in θ preserves f .

Consider a vector $v \neq 0$ and a transformation σ in θ . Then v and $v\sigma$ belong to some hyperplane H , and as usual there exists a transformation σ' in $\theta(H)$ such that $Fv\sigma = Fv\sigma'$. It follows from (4) that $v\sigma = \pm v\sigma'$; consequently we find that

$$f(v\sigma, v\sigma) = f(v\sigma', v\sigma') = f_H(v\sigma', v\sigma') = f_H(v, v) = f(v, v),$$

and (7) follows now from the identity (*).

Denote now by ϕ the group of all linear transformations of V which preserve the form f . It follows from (1) and §5, (5) that ϕ is a full orthogonal group of V , and it follows from (7) that θ is a subgroup of ϕ . From the properties of the full orthogonal group we infer now the existence of an involution ω in ϕ such that $R(\omega)$ is a line. Then $J(\omega)$ is a hyperplane and x belongs to

$J(\omega)$ if, and only if, $f(R(\omega), x) = 0$. Consider now some transformation σ in ϕ . Since θ has property (T), there exists a transformation σ' in θ such that $R(\omega) = R(\omega)\sigma\sigma'$. Since σ , σ' , and $\sigma\sigma'$ preserve f , it follows that $\sigma\sigma'$ maps the hyperplane $J(\omega)$ onto itself. Since $\theta[J(\omega)]$ induces the full orthogonal group in $J(\omega)$, and since $\sigma\sigma'$ induces a transformation in the hyperplane $J(\omega) = H$ which preserves f and therefore f_H , there exists a transformation σ'' in $\theta(H)$ such that $\sigma\sigma'\sigma''$ induces the identity in H . But then $\sigma\sigma'\sigma''$ is as an element in the full orthogonal group ϕ either 1 or ω ; and now one verifies easily that θ has index 2 in ϕ . Thus θ is a proper orthogonal group of V ; this completes the proof of our theorem.

REMARK. It is worth noting that we have used the hypothesis $3 < n$ at least three times in an essential way when deriving (i) from (iii). That the two-dimensional proper orthogonal group is not characterized by the property (P.1) has been shown by Pickert [1, p. 498], who gave an example of a group of two by two matrices with real coefficients satisfying (P.1), though it does not leave invariant any symmetrical, positive definite bilinear form. This is still more remarkable in the light of §6, Proposition 2.

BIBLIOGRAPHY

G. BIRKHOFF and J. VON NEUMANN

1. *The logic of quantum mechanics*, Ann. of Math. vol. 37 (1936) pp. 823–843.

S. IYANAGA and M. ABE

1. *Über das Helmholtzsche Raumproblem*, Proc. Imp. Acad. Tokyo vol. 19 (1943) pp. 174–180 and 540–543.

G. PICKERT

1. *Elementare Behandlung des Helmholtzschen Raumproblems*, Math. Ann. vol. 120 (1948) pp. 492–501.

H. WEYL

1. *Mathematische Analyse des Raumproblems*, Berlin, 1923.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.