COMPOSITIO MATHEMATICA

REINHOLD BAER

The group of motions of a two dimensional elliptic geometry

Compositio Mathematica, tome 9 (1951), p. 241-288

<http://www.numdam.org/item?id=CM_1951__9__241_0>

The group of motions of a two dimensional elliptic geometry

by

Reinhold Baer

Urbana, Illinois

If Φ is the group of motions of a two dimensional elliptic geometry, then it is possible to reconstruct within Φ by purely group theoretical means the original geometry. This phenomenon, not uncommon in geometry in general, makes it possible and convenient to use as postulates for such a geometry group theoretical properties of its motion group Φ. This has been done with great success. An extremely neat and straightforward set of postulates for plane elliptic geometry has been obtained in just this fashion by A. Schmidt [1] where further references may be found.

One of the tools used in the development of plane elliptic geometry from its group theoretical basis is Reidemeister's construction of the motion space [Reidemeister—Podehl [1], § 5—8]. This may be applied to any abstract group G in the following fashion: The derived geometrical structure $D(G)$ of G has for its points as well as for its hyperplanes just the elements in G; and incidence is defined in $D(G)$ by the rule that the point p is on the hyperplane h if, and only if, the product ph is an element of order 2 in G. The question arises to find criteria for $D(G)$ to be a projective space, a question that has a rather surprising answer: The derived geometrical structure $D(G)$ of the group G is a projective space of dimension greater than one if, and only if, G is isomorphic to the motion group of a plane elliptic geometry.

The motion group of a plane elliptic geometry may be considered as an abstract group, as a group of linear transformations, as a group of planar auto-projectivities or we may consider its derived geometrical structure. Each of these points of view leads to a definite characterization of our class of groups; and the proof of the equivalence of these four characterizations is the principal objective of this investigation. We shall arrange the argument as follows. In § 1.C we consider a group G whose derived geometrical structure is a projective space of dimension greater than

one; and we construct in a natural way a representation of G as a group Λ of linear transformations with the following two properties: $(L.1)$. If $\nu \neq 1$ is a linear transformation in Λ, then its space of fixed elements has rank 1. $(L.2)$ To every subspace Q of rank 1 there exists an involution σ in Λ with Q for its space of fixed elements. In § 2,3 we prove that a group Λ of linear transformations has these properties (L) if, and only if, it is the motion group of an elliptic plane; and that Λ induces isomorphically a group of planar auto-projectivities satisfying three conditions (E) on its reflections. In § 4 we show that every group of planar auto-projectivities with these properties (E) meets a set of four abstract group theoretical requirements (G) which deal almost exclusively with the involutions in the group; and in § 6 we close the circle by proving that $D(G)$ is a three dimensional projective space whenever G satisfies the conditions (G). [See § 7, Theorem 1 for a summary of these results.]

It is only to be expected that the representations of groups as L-groups of linear transformations or as E-groups of planar auto-projectivities are essentially uniquely determined; and the proofs of these uniqueness theorems [together with some implications for the foundations of elliptic geometry] may be found in § 7. It is clear that groups in our class may be represented in many different ways as groups of linear transformations; and thus one may be tempted to ask whether the L-groups are at least the only groups of linear transformations which induce isomorphically an E-group of planar auto-projectivities. Strangely enough this is not the case; and we discuss in § 8 the class of motion groups of elliptic planes with this additional uniqueness property. They may be variously characterized by the „Pythagorean" character of the underlying elliptic plane, the possibility of bisecting all right angles, the fact that every group element is a square and by the transitivity of the induced group of planar auto-projectivities.

1. Projective group spaces.

The present section has two principal objectives. Firstly we want to give a survey of the low dimensional projective group spaces; and secondly we shall show that every higher dimensional projective group space may be represented in a natural way as a group of linear transformations.

The definition of a projective group space will be preceded by

the definition of the derived geometrical structure which may be attached to every group.

1.A. The derived geometrical structure of a group.

If G is any group whatsoever, then the derived geometrical structure $D(G)$ is defined as follows. Both the set of points and the set of hyperplanes in $D(G)$ are equal to the set of elements in G. The point p is on the hyperplane h [in symbols: $p < h$] if, and only if, their product ph in G is an involution [= element of order 2].

The structure $D(G)$ is homogeneous. For if g is some fixed element in the group G, and if we map the point p in $D(G)$ upon the point pg and at the same time the hyperplane h onto the hyperplane $g^{-1}h$, then we obtain an incidence preserving, one to one and exhaustive transformation of $D(G)$. This family of transformations is a group isomorphic to G; and it is simply transitive on the points and on the hyperplanes of $D(G)$.

The structure $D(G)$ is self-dual. To prove this fact we construct *the canonical polarity* of which use will be made quite often. This canonical polarity is obtained by interchanging the point g and the hyperplane g. That this interchange preserves incidence, follows from the easily verified equivalence of the following four properties:

(i) $p < h$;
(ii) ph is an involution;
(iii) $hp = h(ph)h^{-1}$ is an involution;
(iv) $h < p$.

Linear dependence in $D(G)$ is defined as follows: If S is a set of points in $D(G)$, and if the point p is on every hyperplane which passes through every point in S, then p is said to depend on S. In other words: p depends on S if ph is an involution whenever Sh is a set of involutions.

Point subspaces of $D(G)$ are sets M of points such that p belongs to M whenever p depends linearly on M. If S is a set of points in $D(G)$, and if $M = M(S)$ is the totality of points linearly dependent on S, then it is easily seen that $M(S)$ is a point subspace of $D(G)$. We shall refer to $M(S)$ as to *the point subspace spanned by S.*

Linear dependence and subspaces may be defined for hyperplanes too [by duality]. We shall make little use of it; and thus we shall usually say subspace instead of point subspace.

S-groups [or *projective group spaces*] may now be defined as groups G whose derived geometrical structure $D(G)$ meets the following requirements.

(a) If the point p depends on the point q, then $p = q$.

(b) If p and q are different points, then there exists a third point r dependent on the set (p, q) [in other words: lines carry at least three points].

(c) If the point p depends on the set S, then p depends on a finite subset of S.

(d) The totality of subspaces of $D(G)$ is a complete, complemented, modular lattice.

These conditions may be restated shortly as requiring that the subspaces of $D(G)$ form a projective space whose points are the points of $D(G)$. As we shall make little use of the above properties, but only of various well known derived properties, a further analysis of them is out of place.

1.B. The low dimensional projective group spaces.

Low dimensional means for us dimension less than three.

THEOREM 1: *The group G is a projective group space of dimension 1 if, and only if, G contains one and only one involution and is of order greater than two.*

PROOF: The group G is a projective group space of dimension one if, and only if, there exist at least three points and if every hyperplane carries one and only one point. The first of these conditions is satisfied if, and only if, the order of G is greater than two. It follows from the homogeneity of $D(G)$ [see 1.A] that the second of these conditions is satisfied if, and only if, the hyperplane 1 carries one and only one point. But a point p is on the hyperplane 1 if, and only if, $p1 = p$ is an involution; and so the second condition is equivalent to the requirement that there exists one and only one involution.

REMARK 1: The class of groups with the properties of Theorem 1 is extremely large. We mention a few examples only. The quaternion group; the direct product of any group with the above properties and of a group without involutions etc.

PROPOSITION 1: *Projective group spaces do not have dimension 2.*

PROOF: Assume by way of contradiction that $D(G)$ is a projective plane. Then G contains at least seven elements; and the „hyperplanes" are lines with the property that any two different lines

have one and only one point in common. Consider an element $g \neq 1$ in G. Then 1 and g represent different lines; and these have one and only one common point p. From $p < 1$ we infer that p is an involution; and from $p < g$ we deduce that pg is an involution too. Naturally $g^{-1}pg$ and $g^{-1}(pg)g = (g^{-1}pg)g$ are involutions too so that the point $g^{-1}pg$ is likewise on the two lines 1 and g. Hence $p = g^{-1}pg$ or $pg = gp$. But pg is an involution; and so it follows that $1 = (pg)^2 = p^2g^2 = g^2$.

Hence every element, not 1, in G is an involution. If a and b are different elements, then ab is an involution; and this shows that every point p is on every line not p. It follows that any two distinct lines have at least five common points; and this is the desired contradiction.

PROPOSITION 2: *The following properties of the S-group G are equivalent.*

(i) *The dimension of $D(G)$ is greater than one.*
(ii) *Every element in G is a product of two involutions.*
(iii) *The center of G does not contain involutions.*
(iv) *The center of G equals* 1.

PROOF: Assume the validity of (i). Then we deduce from Proposition 1 that the dimension of $D(G)$ is at least three. Consider an element $g \neq 1$ in G. Then the points 1 and g span a line which is on at least one hyperplane. There exists therefore a hyperplane h such that $1 < h$ and $g < h$ hold at the same time. But $1 < h$ implies that h is an involution; and $g < h$ implies that $gh = j$ is an involution. Hence $g = jh$ is the product of the two involutions j and h, proving that (i) implies (ii).

Assume next the validity of (ii). Then we infer from $G \neq 1$ the existence of at least two different involutions in G; and it follows from Theorem 1 that the dimension of $D(G)$ is greater than one. Thus we see the equivalence of (i) and (ii).

Assume now the validity of the equivalent properties (i) and (ii); and suppose, by way of contradiction, the existence of an element $c \neq 1$ in the center of G. Then $c = j'j''$ where j' and j'' are different involutions [by (ii)]. Since c belongs to the center of G, $cj' = j'c$; and this implies $j'j'' = j''j'$ so that c is an involution. It is clear now that $1 < c$ and $j' < c$. Hence the line through 1 and j' is on the hyperplane c. This line carries at least a third point p; and this point is necessarily on c too. Hence pc is an involution; and this implies that p is an involution different from c, since c is an involution in the center of G. Con-

sequently $j' < 1$ and $p < 1$ so that the two different points p, j' of the line from 1 to j' are on the hyperplane 1. Hence the point 1 is on 1, an impossibility since 1 is not an involution. Thus we have shown that (iv) is a consequence of the equivalent properties (i), (ii).

It is clear that (iii) is a consequence of (iv). — Assume finally the validity of (iii). Then it is impossible that G contains just one involution, since an only involution would be equal to all its conjugates in G and would therefore belong to the center of G. Thus it follows from Theorem 1 that the dimension of G is not one. This shows that (i) is a consequence of (iii); and this completes the proof.

REMARK 2. In the presence of the equivalent conditions (i) to (iv) of Proposition 2 the element 1 is the only element in G which commutes with every involution, since elements commuting with every involution belong to the center [by (ii)] and since the center equals 1 [by (iv)].

1.C. The canonical representation of G as a group of linear transformations.

We shall call the group G an *S^*-group, if $D(G)$ is a projective space of dimension greater than one.* It follows from Proposition 1 [of 1.B] that the dimension of $D(G)$ is at least three; and this implies among other things that the Theorem of Desargues holds in $D(G)$ and in all its subspaces.

We denote by J the totality of involutions in G. This is just the totality of points on the hyperplane 1 so that the projective space J has at least dimension 2. We note that the point 1 is not on this hyperplane J so that the whole space is spanned by the hyperplane J and the point 1. Since the Theorem of Desargues holds in J, it is possible to represent J by means of „coordinates" from a [not necessarily commutative] field. But this field and this representation are only essentially uniquely determined; and it will be convenient for us to obtain a canonical representation. It will then be possible to obtain a representation of G as a group of linear transformation, again in a natural way. We precede our discussion by the introduction of two symbols.

1. If $g \neq 1$ is an element in the S^*-group G, then the points 1 and g determine a line in $D(G)$ which meets the hyperplane J in one and only one point which we shall denote throughout by g^*. Thus g^* is *a well determined involution for every* $g \neq 1$

2. If the element g in the S^*-group G is neither 1 nor an involution, then we infer from the validity of the Theorem of Desargues in $D(G)$ the existence of one and only one *perspectivity* $\bar{g}$ *with axis* J *and center* g^* *which maps* 1 *onto* g [we recall that $\bar{g}$ leaves invariant every point in J and every line through g^*]. It will be convenient to let $\bar{1}$ be the identity transformation.

The natural representation of the hyperplane J. We denote by A the totality of all elements in the S^*-group G which do not belong to J. Then we may introduce an addition in A by the following rule.

$$a + b = a^{\bar{b}} \tag{3}$$

[is the image of a under the perspectivity $\bar{b}$].

We note that the null-element for this addition is just the identity element in the group G; and thus we shall denotate this element by either of the symbols 0 and 1 according as we discuss addition in A or multiplication in G.

It is easily seen [and well known] that mapping a in A upon the perspectivity $\bar{a}$ is an isomorphism of the additive system A upon the multiplicative group of all the perspectivities with axis J and center on J. Thus A is an additive abelian group, since $\overline{A}$ is a multiplicative abelian group.

If we note that $a = 1^{\bar{a}}$ for every a in A, then we may restate (3) as follows.

$$a + b = 1^{\bar{a}\,\bar{b}} \text{ for } a, b \text{ in } A. \tag{3'}$$

Consider now a perspectivity f with center 1 and axis J. If a is any element in A, then f maps a upon a well determined element in A which we shall denote by fa. One verifies that

$$\overline{fa} = f^{-1}\bar{a}f; \tag{4}$$

and this implies that

$$f(a + b) = fa + fb \text{ for } a, b \text{ in } A. \tag{4'}$$

It is well known that the ring F of endomorphisms of the additive group A which is generated by these transformations is a [not necessarily commutative] field; and that 0 is the only element in F which is not a perspectivity f with center 1 and axis J.

(5) The subset U of A is an F-admissible subgroup of A if, and only if, the totality U^* of all the u^* with $u \neq 0$ in U is a subspace of J; and mapping U onto U^* constitutes a projectivity between the partially ordered set of F-subgroups of A and the partially ordered set of subspaces of J.

This well known theorem asserts that the F-subgroups of A constitute a representation of the subspaces of J; and this is the desired *natural representation of the hyperplane* J by means of the subspaces of the linear manifold (F, A).

The relation between addition in A and multiplication in G is somewhat obscure. We noted already that the null-element 0 in A and the identity-element 1 in G are identical. Upon this result we can improve a little by proving the following useful statement.

LEMMA 1: $-a = a^{-1}$ *for every* a *in* A.

PROOF: To prove this we consider the following mapping σ of the derived geometry $D(G)$. If g is a point [hyperplane] in $D(G)$, then g^σ is the point [hyperplane] g^{-1}. If the point p is on the hyperplane h, then $ph = j$ is an involution. Hence $h^{-1}p^{-1} = j^{-1} = j$ is an involution too; and consequently $p^\sigma h^\sigma = p^{-1}h^{-1} = h(h^{-1}p^{-1})h^{-1}$ is likewise an involution. Consequently p^σ is on h^σ; and thus we see that σ is an involutorial auto-projectivity of the derived geometry $D(G)$. But σ leaves invariant the point 1 and every point on the hyperplane J. Consequently σ is an involutorial perspectivity with center 1 and axis J; and σ is therefore an element in F which maps a in A upon $\sigma a = a^{-1}$ in A. Now σ is involutorial; and the field F contains only one involutorial element, namely -1. Hence σ in F is just -1; and we see that $-a = a^{-1}$ for every a in A. Since G contains elements which are different from their inverses, $-1 \neq 1$ in F; and thus we have shown incidentally the following fact.

COROLLARY 1: *The characteristic of* F *is not* 2.

Now we are ready to establish the desired

Natural representation of G *as group of linear transformations of* (F, A).

If we map the element g in G upon the inner automorphism $x^g = g^{-1}xg$, then we obtain an isomorphic mapping of G upon the group of inner automorphisms of G [by Proposition 2 of 1.B]. If we map the point p upon the point p^g and at the same time the hyperplane h upon the hyperplane h^g, then we obtain an auto-projectivity of $D(G)$, since ph is an involution if, and only if, $(ph)^g = p^g h^g$ is an involution; and this auto-projectivity g^π preserves the canonical polarity, the point 1 and the hyperplane J. Mapping the element a in A upon the element a^g we obtain clearly a permutation of the elements in A which we denote by g^+; and it is clear that mapping g upon g^+ constitutes a homomor-

phism of the group G upon a group G^+ of permutations of A.

Before stating our principal result we introduce some *notations*. If v is a linear transformation of the linear manifold (F, A), then we denote by $P(v)$ the totality of elements x in A such that $xv = x$ and by $N(v)$ the totality of elements x in A such that $xv = -x$. Clearly $P(v)$ and $N(v)$ are subspaces of A.

The group Φ of linear transformations of the linear manifold (F, A) will be termed an *L-group of linear transformations*, if it has the following two properties.

(L.1) *$P(v)$ is a point in (F, A) for every $v \neq 1$ in Φ.*

(L.2) *To every point Q in (F, A) there exists an involution ω in Φ such that $Q = P(\omega)$.*

Now we are ready to state the principal result of this section.

THEOREM 2: *If G is an S^*-group, then mapping g onto g^+ constitutes an isomorphism of G upon the L-group G^+ of linear transformations.*

The proof of this theorem will be effected in a number of steps.

(6) $$(x^y)^* = (x^*)^y \text{ for } x \neq 1 \text{ and } y \text{ in } G.$$

PROOF: If $x \neq 1$, then there exists one and only one line L in $D(G)$ which connects the points 1 and x; and L meets the hyperplane J in the uniquely determined point x^*. The inner automorphism of G which is induced by the element g maps the line L upon the line L^g which connects the points 1 and x^g and which meets in J in the point $(x^g)^*$. But our transformation maps the point x^* of intersection of L and J upon the point $(x^g)^*$ of intersection of L^g and J so that $(x^g)^* = (x^*)^g$, as we claimed.

(7) *The mapping of g upon g^+ constitutes an isomorphism of G upon G^+.*

PROOF: Suppose that $g^+ = 1$. If $a \neq 0$ is an element in A, then we deduce from (6) that

$$a^* = (a^{g^+})^* = (a^g)^* = (a^*)^g.$$

Hence g commutes with every involution in G. But every element in G is a product of involutions in G [§ 1.B, Proposition 2] so that g belongs to the center of G. But the center of G is 1 [by § 1.B, Proposition 2]; and so $g^+ = 1$ implies $g = 1$.

(8) $$\overline{(a^g)} = (g^\pi)^{-1}\bar{a}g^\pi \text{ for } a \text{ in } A \text{ and } g \text{ in } G.$$

PROOF: We note first that $\overline{(a^g)}$ is the uniquely determined perspectivity with axis J and center $(a^g)^*$ which maps 1 onto a^g.

Secondly we note that $(g^\pi)^{-1}\bar{a}g^\pi$ is the uniquely determined perspectivity with axis J and center $(a^*)^g$ which maps 1 upon $1^{(g^\pi)^{-1}\bar{a}g^\pi}$. But $(a^*)^g = (a^g)^*$ by (6) and $1^{(g^\pi)^{-1}\bar{a}g^\pi} = 1^{\bar{a}g^\pi} = a^{g^\pi} = a^g$. Thus the two perspectivities under consideration are equal, proving (8).

(9) $(a + b)^{g^+} = a^{g^+} + b^{g^+}$ *for* a *and* b *in* A, g *in* G.

PROOF: This follows from (8), if we note that

$$x^g = x^{g^+} = x^{g^\pi} \text{ for } x \text{ in } A \text{ and } g \text{ in } G,$$

and that therefore [by (3′)]

$$(a + b)^{g^+} = (1^{\bar{a}\,\bar{b}})^{g^+} = 1^{(g^\pi)^{-1}\bar{a}\,\bar{b}g^\pi} = 1^{\overline{a^g}\,\overline{b^g}}$$
$$= a^g + b^g = a^{g^+} + b^{g^+}.$$

(10) *If* j *is an involution in* G, *then* j^+ *is an involutorial linear transformation of* (F, A) *with the following properties.*

(a) $P(j^+)^*$ *consists of* j *alone.*

(b) $N(j^+)^*$ *is the totality* $J(j)$ *of involutions* u *in* G *such that* uj *is an involution.*

(c) $A = P(j^+) \oplus N(j^+)$.

PROOF: The involution j in G commutes with itself and with the involutions in $J(j)$ and with no further involution. But $J(j)$ is clearly the intersection of the hyperplane j and the hyperplane J [of all involutions]. Since the point j is not on the hyperplane j, the whole space is spanned by the point j and the points on the hyperplane j. Since j is on the hyperplane of all involutions, it follows that J is spanned by the point j and its submanifold $J(j)$. We deduce from (5) the existence of uniquely determined subspaces U and V of (F, A) such that $U^* = j$ and $V^* = J(j)$; and it follows from (5) [and the fact that J is spanned by $J(j)$ and the point j not on $J(j)$] that

(10.1) $$A = U \oplus V.$$

Suppose now that $a \neq 0$ is an element in U. Then we deduce from the definition of U that $a^* = j$. Since G is an S^*-group, there exist involutions a', a'' in G such that $a = a'a''$ [by § 1.B, Proposition 2]. Since $aa' = a'a''a'$ and $aa'' = a'$ are clearly involutions in G, it follows that the point a is on the two different hyperplanes a' and a''. These two hyperplanes carry 1; and so the whole line from 1 to a is on them. But the point $a^* = j$ is on the line from 1 to a so that j is on the hyperplanes a' and a''. Since j, a', a'' and ja', ja'' are therefore involutions, it follows that j commutes with a' and with a''. But this implies $ja = aj$

or $a = a^{j^+}$ belongs to the totality $P(j^+)$ of fixed elements of j^+. Hence

$$U \leqq P(j^+). \tag{10.2}$$

Consider next an element $a \neq 0$ in V. Then a^* is a well determined element in $J(j)$ so that a^* and a^*j are involutions. Consequently the points 1 and a^* are on the hyperplane j. Since 1, a, a^* are collinear points, it follows that a too is on the hyperplane j. Hence aj is an involution; and we deduce from Lemma 1 that

$$a^{j^+} = j^{-1}aj = jaja\,a^{-1} = a^{-1} = -a.$$

Hence a belongs to the totality $N(j^+)$ of elements in A such that $a^{j^+} = -a$; and we have shown that

$$V \leqq N(j^+). \tag{10.3}$$

It follows from (9) [and (7)] that j^+ is an involutorial automorphism of the additive group A. Hence $P(j^+)$ and $N(j^+)$ are certainly subgroups of A. If these subgroups were equal, then it would follow from (10.1) to (10.3) that they are equal to A so that $j^+ = 1$ which is impossible by (7). But once $P(j^+)$ and $N(j^+)$ are different, they have only 0 in common; and now it follows from (10.1) to (10.3) that

$$U = P(j^+) \text{ and } V = N(j^+). \tag{10.4}$$

Since U and V are F-admissible subspaces with direct sum A, it is now an almost immediate consequence of (10.4) that the involutorial automorphism j^+ of the additive group A is a linear transformation of A over F; and this completes the proof of (10).

(11) *Every transformation in G^+ is linear.*

Proof: If g is in G, then there exist involutions h, k in G such that $g = hk$ [§ 1.B, Proposition 2]. It follows from (10) that h^+ and k^+ are linear transformations; and consequently $g^+ = h^+k^+$ is linear too.

Verification of (L.1): Suppose that $g \neq 1$ is an element in G. If g happens to be an involution, then it follows from (5) and (10) that $P(g^+)$ is a point in (F, A). Assume now that $g^2 \neq 1$. Then g is an element, not 0, in A too. Consider now an element $a \neq 0$ in $P(g^+)$. Then $a = a^g$ so that 1, a and consequently the line from the point 1 to the point a are left invariant by the autoprojectivity g^π. Since g^π leaves also the hyperplane J invariant, the point a^* [in which the line from 1 to a meets J] is a fixed

point of g^{π}. Hence $a^*g = ga^*$ or $g = g^{a^*}$ so that g is an element, not 0, in $P[(a^*)^+]$. Since $P[(a^*)^+]$ is a point [by (10)], we have $P[(a^*)^+] = Fg$; and it follows from [(5) and] (10) that $(Fg)^* = P[(a^*)^+] = a^*$. Thus we see that $a^* = g^*$ whenever $a \neq 0$ is in $P(g^+)$. Since g itself certainly belongs to $P(g^+)$, it follows now that $P(g^+)^* = g^*$; and it follows from (5) that $P(g^+)$ is a point in (F, A). This shows the validity of (L.1).

Verification of (L.2): If Q is a point in (F, A), then it follows from (5) that $Q^* = j$ is an involution in G. We deduce from (10) that j^+ is a linear transformation in G^+, satisfying $P(j^+)^* = j = Q^*$; and it follows from (5) that $P(j^+) = Q$, showing the validity of (L.2).

Combining (7), (11) with these last two verifications we see the validity of Theorem 2.

2. L-groups of linear transformations.

Throughout this section we consider a linear manifold (F, A) and an L-group Φ of linear transformations of (F, A) [as defined in § 1.C]. It is our principal objective in this section to show that such a group is the group of motions of an elliptic plane. Thus there will be no danger of confusion, if we abstain from restating this hypothesis (L) in the course of this section.

Proposition 1: *The characteristic of F is not 2 and the rank of (F, A) is 3.*

Proof: Since $A \neq 0$, there exists a point Q. We infer from (L.2) the existence of an involution v such that $Q = P(v)$. Since $v \neq 1$, $Q \neq A$ so that the rank of A is at least 2.

Assume now by way of contradiction that the characteristic of F is 2. If a is an element in A, then $a + av$ belongs to $P(v) = Q$, since v is an involution. If $a + av = 0$, then $av = -a = a$, since the characteristic of F is 2. Hence $a + av \neq 0$ for every a in A, not in Q; and this implies

$$Q = F(a + av) \text{ for } a \text{ in } A, \text{ not in } Q.$$

If a and b are elements, not in Q, then it follows that there exists a number $c \neq 0$ in F such that $b + bv = c(a + av)$ or

$$(b + ca)v = b + ca,$$

since the characteristic of F is 2. Hence b is in $Q + Fa$; and we have shown that $A = Q + Fa$ is a line.

We infer from (L.2) the existence of an involution ω in Φ such

that $P(\omega)$ is some point different from Q. Hence $A = P(\nu) \oplus P(\omega)$, since A is a line. Since $\nu\omega$ belongs to Φ, and since $P(\nu) \neq P(\omega)$, ν and ω are different involutions so that $\nu\omega \neq 1$. It follows from (L.1) that $P(\nu\omega)$ is a point. Hence there exists an element $b \neq 0$ in $P(\nu\omega)$; and we infer from $A = P(\nu) \oplus P(\omega)$ the existence of elements s and t in $P(\nu)$ and $P(\omega)$ respectively such that $b = s + t$. Then

$$s + t = b = b\nu\omega = s\nu\omega + t\nu\omega = s\omega + t\nu\omega.$$

Remembering that the characteristic of F is supposed to be two it follows that

$$(s + s\omega) + (t\nu + t\nu\omega) = t + t\nu$$

is an element in the intersection 0 of $P(\nu)$ and $P(\omega)$. Hence $t + t\nu = 0$ or $t\nu = t$ so that t belongs to the intersection 0 of $P(\nu)$ and $P(\omega)$. Consequently $t = 0$; and this implies $s + s\omega = 0$ or $s\omega = s$ so that s belongs to the intersection 0 of $P(\nu)$ and $P(\omega)$. Hence $s = 0$ so that $0 \neq b = s + t = 0$, the desired contradiction. This shows that the characteristic of F is not 2.

If the linear transformation ν of (F, A) is an involution, then it follows [as usual] that $A = P(\nu) \oplus N(\nu)$. We have already pointed out that the rank of (F, A) is at least 2. Assume now by way of contradiction that A is a line. Then $N(\nu)$ is a point, since $P(\nu)$ is a point. Thus there exists by (L.2) an involution ω such that $P(\omega) = N(\nu)$. Clearly $\nu\omega \neq 1$; and it follows from (L.1) that there exists an element $a \neq 0$ in $P(\nu\omega)$. From $A = P(\nu) \oplus N(\nu)$ we deduce the existence of elements p, n in $P(\nu)$ and $N(\nu)$ respectively such that $a = p + n$. Then

$$p + n = a = a\nu\omega = (p + n)\nu\omega = (p - n)\omega = p\omega - n,$$

since $N(\nu) = P(\omega)$. Hence $2n = p\omega - p$ is in the intersection 0 of $P(\omega)$ and $N(\omega)$; and this implies $n = 0$ and $p\omega = p$, since the characteristic of F is not 2. But then p itself is in the intersection 0 of $P(\nu)$ and $N(\nu)$ so that $p = 0$. Hence $0 \neq a = p + n = 0$ is the desired contradiction which shows that the rank of A is at least 3.

If ν is any involution in Φ, then $P(\nu)$ is a point [by (L.1)] so that $N(\nu)$ has rank not less than 2. We deduce from (L.2) the existence of an involution ω such that $P(\omega)$ is some point on $N(\nu)$. It is clear that

$$N(\nu) \cap N(\omega) \leqq P(\nu\omega).$$

Since ν and ω are different involutions, $\nu\omega \neq 1$; and it follows from (L.1) that $P(\nu\omega)$ is a point. It follows from (L.1) that $P(\nu)$

and $P(\omega)$ are points; and we have $A = P(\nu) \oplus N(\nu) = P(\omega) \oplus N(\omega)$, since the characteristic of F has been shown to be different from 2. The rank of A consequently exceeds the rank of $N(\nu) \cap N(\omega)$ at most by two. But we have shown already that the rank of $N(\nu) \cap N(\omega)$ cannot exceed one; and thus we see that the rank of A cannot exceed three. Since we have shown in the preceding paragraph of this proof that the rank of A is at least three, it follows that the rank of A over F is exactly three; and this completes the proof.

COROLLARY 1: *If ν is an involution in Φ, then $A = P(\nu) \oplus N(\nu)$ where $P(\nu)$ is a point and $N(\nu)$ a line.*

This is a fairly obvious consequence of Proposition 1 and (L.1) and has actually been verified in the course of its proof.

LEMMA 1: *If ν is an involution in Φ, and if $P(\nu)$ is a fixed point of the transformation τ in Φ, then $\tau\nu = \nu\tau$.*

PROOF: Clearly $\omega = \tau^{-1}\nu\tau$ is an involution in Φ; and it follows from our hypothesis that $P(\omega) = P(\nu)\tau = P(\nu)$. The intersection of the lines $N(\nu)$ and $N(\omega)$ has at least rank 1. Since obviously

$$P(\nu) \oplus [N(\nu) \cap N(\omega)] \leqq P(\nu\omega),$$

it follows that $P(\nu\omega)$ has at least rank two. We deduce from (L.1) that $\nu\omega = 1$ or $\nu = \omega = \tau^{-1}\nu\tau$ or $\tau\nu = \nu\tau$, as we intended to show.

LEMMA 2: *To every line L in A there exists an involution in Φ such that $L = N(\nu)$.*

PROOF: We infer from (L.2) the existence of an involution α in Φ such that $P(\alpha) \leqq L$. Then the lines L and $N(\alpha)$ are necessarily different so that they meet in a point $Q = L \cap N(\alpha)$, since A is by Proposition 1 a plane. There exists by (L.2) an involution β in Φ such that $Q = P(\beta)$. Since Q is a fixed point of α, it follows from Lemma 1 that $\alpha\beta = \beta\alpha$ to that $\nu = \alpha\beta = \beta\alpha$ is an involution. From $P(\alpha) = P(\beta^{-1}\alpha\beta) = P(\alpha)\beta$ it follows that $P(\alpha)$ is a fixed point of β which is different from $P(\beta) = Q = L \cap N(\alpha)$. But all these fixed points of β are on $N(\beta)$. From $P(\alpha) \leqq N(\beta)$ and $P(\beta) \leqq N(\alpha)$ we infer

$$L = P(\alpha) \oplus P(\beta) \leqq N(\alpha\beta);$$

and this implies $L = N(\alpha\beta)$, since $N(\alpha\beta)$ is a line by Corollary 1.

LEMMA 3: *The following properties of the transformation $\tau \neq 1$ in Φ are equivalent.*

(i) $N(\tau) \neq 0$.
(ii) *τ is an involution.*
(iii) *τ possesses at least two fixed points.*

PROOF: If $N(\tau) \neq 0$, then $P(\tau) \oplus N(\tau) \leqq P(\tau^2)$ implies that $P(\tau^2)$ has at least rank 2. It follows from (L.1) that $\tau^2 = 1$. Hence (ii) is a consequence of (i).

If (ii) is true, then $N(\tau)$ is a line [Corollary 1] all of whose points are fixed points so that τ possesses at least three fixed points. Hence (iii) is a consequence of (ii).

Assume finally the validity of (iii). Since $P(\tau)$ is a [fixed] point by (L.1), it follows that there exists a fixed point $Q \neq P(\tau)$. We deduce from Lemma 2 the existence of an involution ν in Φ such that $N(\nu) = Q \oplus P(\tau)$. Clearly $P(\tau) \leqq N(\tau\nu)$ so that $N(\tau\nu) \neq 0$. We have already verified that (i) implies (ii); and so it follows that $\tau\nu$ is an involution. Clearly Q is a fixed point of $\tau\nu$ [as a fixed point of τ and of ν]. Suppose now that $Q \leqq N(\tau\nu)$. Since $Q \leqq N(\nu)$, this would imply $Q \leqq P(\tau\nu\,\nu) = P(\tau)$; and this is impossible, since Q and $P(\tau)$ are different points. But the only fixed point of the involution $\tau\nu$ which is not on $N(\tau\nu)$ is $P(\tau\nu)$ [by Corollary 1]. Hence $P(\tau\nu) = Q \leqq N(\nu)$ so that $Q \leqq N(\tau\nu\,\nu) = N(\tau)$. Consequently $N(\tau) \neq 0$ so that (i) is a consequence of (iii). This completes the proof.

COROLLARY 2: *Every transformation in Φ is the product of two involutions in Φ.*

PROOF: Suppose that $\tau \neq 1$ is a transformation in Φ. Then $P(\tau)$ is a point [by (L.1)]; and we infer from Lemma 2 the existence of an involution ν in Φ such that $P(\tau) \leqq N(\nu)$. Then $P(\tau) \leqq N(\tau\nu)$ so that $N(\tau\nu) \neq 0$. It follows from Lemma 3 that $\tau\nu = \omega$ is an involution and $\tau = \omega\nu$ is the product of two involutions.

PROPOSITION 2: *A polarity is defined in the plane (F, A) by the following rule.*
(2.P) *The point Q is the pole of the line L and the line L is the polar of the point Q if, and only if, there exists an involution ν such that $Q = P(\nu)$ and $L = N(\nu)$.*

We shall refer to this polarity as to the Φ-polarity.

PROOF: It follows from (L.2) that every point Q is the pole of at least one line. If ν and ω are involutions in Φ such that $Q = P(\nu) = P(\omega)$, then $Q \oplus [N(\nu) \cap N(\omega)]$ has rank not less than two and is on $P(\nu\omega)$ [by Corollary 1]. It follows from (L.1)

that $\nu\omega = 1$ or $\nu = \omega$. Thus every point is the pole of one and only one line.

It follows from Lemma 2 that every line L is the polar of at least one point. If ν and ω are involutions in Φ such that $L = N(\nu) = N(\omega)$, then $L \leqq P(\nu\omega)$; and it follows from (L.1) that $\nu\omega = 1$ or $\nu = \omega$. Thus every line is the polar of one and only one point.

Assume now that the point Q is on the line L; and denote by ν and ω the uniquely determined involutions in Φ such that $Q = P(\nu)$ and $L = N(\omega)$. Then $Q \leqq N(\nu\omega)$ so that $N(\nu\omega) \neq 0$; and it follows from Lemma 3 that $\nu\omega$ is an involution. Hence $\nu\omega = \omega\nu$ so that $P(\omega) = P(\nu^{-1}\omega\nu) = P(\omega)\nu$ is a fixed point of the involution ν. Since $P(\omega)$ is not on $N(\omega)$, it follows that $P(\omega) \neq P(\nu)[= Q < L = N(\omega)]$. But all the other fixed points of ν are on $N(\nu)$; and this implies $P(\omega) < N(\nu)$. Thus we have shown that the pole $P(\omega)$ of L is on the polar $N(\nu)$ of Q whenever the point Q is on the line L; and this completes the proof of the fact that rule (2.P) defines a polarity.

COROLLARY 3: *No point is on its polar [with respect to the Φ-polarity].*

This is an almost immediate consequence of Corollary 1 and the rule (2.P).

COROLLARY 4: *L-groups of linear transformations are infinite.*

PROOF: It follows from Corollary 3 that the projective plane (F, A) carries an infinity of points [see Baer [1], p. 82, Theorem 5]. Hence it follows from (L.2) that L-groups contain an infinity of involutions and are consequently infinite.

It is well known that every polarity of the projective plane (F, A) may be represented by a „Generalized Hermitean Form" [see, for instance, Birkhoff-von Neumann [1], p. 837—843]. Consequently there exists an anti-automorphism σ of F and an F-valued function $f(x, y)$ of the elements x and y in A, meeting the following requirements.

$(F.a)$ $\sigma^2 = 1$.

$(F.b)$ $f(x, y)^\sigma = f(y, x)$.

$(F.c)$ $f(a + b, y) = f(a, y) + f(b, y)$.

$(F.d)$ $f(cx, y) = cf(x, y)$.

$(F.e)$ *y is on the Φ-polar of the point Q if, and only if,* $f(Q, y) = 0$.

Applying $(F.b)$ onto $(F.c)$ and $(F.d)$ one deduces that

$(F.c')$ $f(x, a + b) = f(x, a) + f(x, b)$;

$(F.d')$ $f(x, cy) = f(x, y)c^{\sigma}$.

On the basis of $(F.e)$ it follows that Corollary 3 is essentially equivalent to the property

$(F.f)$ $\quad f(x, x) = 0$ *implies* $x = 0$.

The form f is not uniquely determined by the Φ-polarity. But because of $(F.f)$ it is possible to impose always the following normalizing condition.

$(F.g)$ $\quad f(e, e) = 1$ *for some* [*preassigned*] $e \neq 0$ *in* A.

A linear transformation ν is said to preserve f, if $f(x\nu, y\nu) = f(x, y)$ for every x and y in A.

LEMMA 4: *The transformations in* Φ *preserve* f.

PROOF: Because of Corollary 2 it suffices to prove this for involutions ν in Φ. If x is an element in A, then there exist uniquely determined elements x', x'' in $P(\nu)$ and $N(\nu)$ respectively such that $x = x' + x''$. We notice furthermore that $f[P(\nu), N(\nu)] = 0$ as a consequence of $(F.e)$ and the definition of the Φ-polarity. Now we find that

$$f(a\nu, b\nu) = f(a' - a'', b' - b'') = f(a', b') + f(a'', b'') = \\ = f(a' + a'', b' + b'') = f(a, b),$$

as we claimed.

REMARK: The converse of Lemma 4 is false, as the linear transformation -1 does not belong to Φ, but preserves f. — Later we shall be able to prove a kind of converse.

LEMMA 5: *The following properties of the three distinct involutions* α, β, γ *in* Φ *are equivalent.*

(i) $\alpha\beta\gamma$ *is an involution.*

(ii) $P(\alpha)$, $P(\beta)$ *and* $P(\gamma)$ *are collinear points.*

(iii) $N(\alpha)$, $N(\beta)$ *and* $N(\gamma)$ *are copunctual lines.*

PROOF: The equivalence of properties (ii) and (iii) is an immediate consequence of the definition of the Φ-polarity and the general properties of polarities.

Assume the validity of (iii). Then the point $Q = N(\alpha) \cap N(\beta) \cap N(\gamma)$ is clearly on $N(\alpha\beta\gamma)$ so that $N(\alpha\beta\gamma) \neq 0$. It follows from Lemma 3 that $\alpha\beta\gamma$ is an involution in Φ.

If ν and ω are distinct involutions in Φ, then it follows from (L.1) and the fact that distinct lines in a plane meet in a point that $P(\nu\omega) = N(\nu) \cap N(\omega)$. If now $\alpha\beta\gamma$ is an involution, then α, β and $\alpha\beta\gamma$, γ are pairs of distinct involutions so that

$$N(\alpha) \cap N(\beta) = P(\alpha\beta) = P[(\alpha\beta\gamma)\gamma] = N(\alpha\beta\gamma) \cap N(\gamma)$$

is the common point of the three lines $N(\alpha)$, $N(\beta)$ and $N(\gamma)$. Thus (i) and (iii) are equivalent too; and this completes the proof.

PROPOSITION 3: $\sigma = 1$.

COROLLARY 4: *The field F is commutative and f is an ordinary symmetrical bilinear form.*

It is clear that Corollary 4 is an immediate consequence of the fundamental Proposition 3, since the identity is an anti-automorphism of the field F if, and only if, F is commutative. We note that this latter fact is known to be equivalent to the validity of the Theorem of Pappus in the projective plane (F, A). Proposition 3 is a much stronger statement which in a way may be likened to the Theorem of Pascal. We note the fact, interesting for the foundations of geometry, that the commutativity of F is obtained as a trivial consequence of $\sigma = 1$; and is not used in its proof.

PROOF: According to $(F \,.\, g)$ there exists a point e such that $f(e, e) = 1$. Denote by d some element, not 0, on the polar of the point Fe. Then the points Fe and Fd span a line $L = Fe \oplus Fd$. We note that $f(e, d) = f(d, e) = 0$, since Fe is on the polar of Fd and Fd on the polar of Fe. We let $k = f(d, d)$; and note that $0 \neq k = k^\sigma$ by $(F.b)$ and $(F.f)$. If t is some number in F, then $F(e + td)$ is a point on the line L; and there exists one and only one involution $\nu(t)$ such that $P[\nu(t)] = F(e + td)$ [by (L.2) and Proposition 2]. It will be convenient to let $\nu = \nu(0)$ and $\upsilon = \nu(1)$.

If t is neither 0 nor 1, then Fe, $F(e + d)$ and $F(e + td)$ are three distinct collinear points. It follows from (L.1) and the definition of the involutions $\nu(t)$ that ν, υ and $\nu(t)$ are three distinct involutions; and it follows from Lemma 5 that $\nu\upsilon\nu(t)$ is an involution. This implies that

(t.1) *$\nu\upsilon\nu(t) = \nu(t)\upsilon\nu$ is an involution for every $t \neq 0, 1$ in F.*

The lines L and $N[\nu(t)]$ meet in a point which we are going to determine next. From $P[\nu(t)] = F(e + td)$ and

$$f(-kt^\sigma e + d, e + td) = -kt^\sigma f(e, e) + f(d, d)t^\sigma = 0$$

it follows that $L \cap N[\nu(t)] = F(-kt^\sigma e + d)$. Consequently $\nu(t)$ meets the following two requirements.

$$(e + td)\nu(t) = e + td.$$
$$(-kt^\sigma e + d)\nu(t) = -(-kt^\sigma e + d).$$

From these formulae it follows by elimination that

$$(1 + tkt^\sigma)e\nu(t) = (1 - tkt^\sigma)e + 2td$$
$$(1 + tkt^\sigma)td\nu(t) = 2tkt^\sigma e + (tkt^\sigma - 1)td.$$

It is clear that $1 + tkt^\sigma \neq 0$.

We note furthermore that $ev = e$, $dv = -d$ and

$$(1 + k)ev = (1 - k)e + 2d$$
$$(1 + k)dv = 2ke + (k - 1)d.$$

Noting that the numbers tkt^σ, $1 + tkt^\sigma$, $1 - tkt^\sigma$, $(1 + tkt^\sigma)^{-1}$ commute with each other one verifies now by direct computation that

$$evvv(t) = (1 + k)^{-1}[(1 - k)(1 - tkt^\sigma) + 4t^{-1}(tkt^\sigma)](1 + tkt^\sigma)^{-1}e + \\ + 2(1 + k)^{-1}[(1 - k) + t^{-1}(tkt^\sigma - 1)](1 + tkt^\sigma)^{-1}td;$$

$$ev(t)vv = (1 + tkt^\sigma)^{-1}[(1 - tkt^\sigma)(1 - k) + 4tk](1 + k)^{-1}e - \\ - 2(1 + tkt^\sigma)^{-1}[(1 - tkt^\sigma) + t(k - 1)](1 + k)^{-1}d.$$

If $t \neq 0, 1$, then we may apply $(t.1)$; and because of the independence of e and d we may equate corresponding coefficients. Thus we obtain the following two equations which are valid for every $t \neq 0, 1$.

$(t.2)$ $(1 + k)^{-1}[(1 - k)(1 - tkt^\sigma) + 4kt^\sigma](1 + tkt^\sigma)^{-1} =$
$= (1 + tkt^\sigma)^{-1}[(1 - tkt^\sigma)(1 - k) + 4tk](1 + k)^{-1};$

$(t.3)$ $(1 + k)^{-1}[(1 - k) + t^{-1}(tkt^\sigma - 1)](1 + tkt^\sigma)^{-1}t =$
$= (1 + tkt^\sigma)^{-1}[(tkt^\sigma - 1) + t(1 - k)](1 + k)^{-1}.$

With the equations $(t.2)$ and $(t.3)$ we have also the equations $(-t.2)$ and $(-t.3)$. Adding and subtracting these equations and remembering that the characteristic of the field F is not 2 [Proposition 1] we find the following equations.

$(t.2')$ $(1 + k)^{-1}(1 - k)(1 - tkt^\sigma)(1 + tkt^\sigma)^{-1} =$
$= (1 + tkt^\sigma)^{-1}(1 - tkt^\sigma)(1 - k)(1 + k)^{-1};$

$(t.2'')$ $(1 + k)^{-1}kt^\sigma(1 + tkt^\sigma)^{-1} = (1 + tkt^\sigma)^{-1}tk(1 + k)^{-1};$

$(t.3')$ $(1 + k)^{-1}t^{-1}(tkt^\sigma - 1)(1 + tkt^\sigma)^{-1}t =$
$= (1 + tkt^\sigma)^{-1}(tkt^\sigma - 1)(1 + k)^{-1};$

$(t.3'')$ $(1 + k)^{-1}(1 - k)(1 + tkt^\sigma)^{-1}t = (1 + tkt^\sigma)^{-1}t(1 - k)(1 + k)^{-1}$

[The equation $(t.3')$ is trivially satisfied.] From $(t.3'')$ we deduce that

$$(1 - k)(1 + tkt^\sigma)^{-1}t(1 + k) = (1 + k)(1 + tkt^\sigma)^{-1}t(1 - k)$$

or

$$-k(1 + tkt^\sigma)^{-1}t + (1 + tkt^\sigma)^{-1}tk = k(1 + tkt^\sigma)^{-1}t - (1 + tkt^\sigma)^{-1}tk.$$

But the characteristic of the field F is not 2 [Proposition 1]; and so it follows that

$(t.4)$ $$k[(1 + tkt^\sigma)^{-1}t] = [(1 + tkt^\sigma)^{-1}t]k.$$

Applying $(t.4)$ onto $(t.2'')$ we find that

$$t^\sigma(1 + tkt^\sigma)^{-1} = (1 + tkt^\sigma)^{-1}t$$

or

$$(t.5) \qquad (1 + tkt^\sigma)t^\sigma = t(1 + tkt^\sigma).$$

Combine $(t.4)$ and $(t.5)$ to find that

$$(1 + tkt^\sigma)k = tkt^{-1}(1 + tkt^\sigma) = tk(1 + tkt^\sigma)t^{-\sigma}$$

or

$$(t.6) \qquad (1 + tkt^\sigma)kt^\sigma = tk(1 + tkt^\sigma).$$

From $(t.2')$ we deduce now successively that

$$\begin{aligned}&(1 - k)(1 - tkt^\sigma)(1 + tkt^\sigma)^{-1}(1 + k) = \\ &\quad = (1 + k)(1 - tkt^\sigma)(1 + tkt^\sigma)^{-1}(1 - k), \\ &-k(1 - tkt^\sigma)(1 + tkt^\sigma)^{-1} + (1 - tkt^\sigma)(1 + tkt^\sigma)^{-1}k = \\ &\quad = k(1 - tkt^\sigma)(1 + tkt^\sigma)^{-1} - (1 - tkt^\sigma)(1 + tkt^\sigma)^{-1}k.\end{aligned}$$

But the characteristic of F is not two [Proposition 1]; and so it follows that

$$k(1 - tkt^\sigma)(1 + tkt^\sigma)^{-1} = (1 + tkt^\sigma)^{-1}(1 - tkt^\sigma)k$$

or

$$(1 + tkt^\sigma)k(1 - tkt^\sigma) = (1 - tkt^\sigma)k(1 + tkt^\sigma)$$

or

$$tkt^\sigma k - ktkt^\sigma = -tkt^\sigma k + ktkt^\sigma.$$

But this implies

$$(tkt^\sigma)k = k(tkt^\sigma),$$

since the characteristic of F is not two. If we apply this on $(t.6)$ and use $(t.5)$, then we find that

$$(1 + tkt^\sigma)kt^\sigma = tk(1 + tkt^\sigma) = t(1 + tkt^\sigma)k = (1 + tkt^\sigma)t^\sigma k$$

or

$$(t.7) \qquad kt^\sigma = t^\sigma k \text{ for every } t \text{ in } F,$$

since $1 + tkt^\sigma \neq 0$. But $F = F^\sigma$; and so $(t.7)$ implies that

$$(7) \qquad k \text{ belongs to the center of } F.$$

If σ were not 1, then there would exist an element $w \neq 0$ in F such that $w \neq w^\sigma$. Let $z = w - w^\sigma$. Then $z \neq 0$ and $z^\sigma = -z$. Clearly therefore $z \neq 1$; and so we may apply $(z.5)$ and (7). It follows that

$$-(1 - zkz)z = z(1 - zkz) = (1 - zkz)z.$$

But $1 - zkz = 1 + zkz^{\sigma} \neq 0$; and so it follows that $z = -z$ or $z = 0$, since the characteristic of F is not two. This is a contradiction which proves that $\sigma = 1$, as we desired to show.

Since the field F is commutative, every linear transformation of (F, A) has a well determined determinant.

COROLLARY 5: *Every linear transformation in Φ has determinant $+1$.*

Because of Corollary 2 it suffices to prove this for the involutions in Φ; and the involutions in Φ have determinant $+1$ because of Corollary 1.

PROPOSITION 4: *If G is an S^*-group, then $D(G)$ is a three dimensional projective space, the Theorem of Pappus is true in $D(G)$ and the canonical polarity may be represented by means of an ordinary symmetrical bilinear form.*

PROOF: It is a consequence of § 1.C, Theorem 2 that G is essentially the same as an L-group of linear transformations of the linear manifold (F, A) which is projectively equivalent [by § 1.G, (5)] to the hyperplane J in $D(G)$. It follows from § 2, Proposition 1 that (F, A) has rank 3 so that J is a plane and $D(G)$ is a three dimensional projective space. It follows from Corollary 4 that F is commutative; and this is equivalent to the validity of the Theorem of Pappus in the projective plane J. But if the Theorem of Pappus holds in one plane, it holds everywhere. Finally it is possible to represent the canonical polarity in $D(G)$ by means of a generalized Hermitean form which may be restricted to a generalized Hermitean form in J. But the latter is an ordinary symmetrical bilinear form [by Corollary 4] so that the former is an ordinary symmetrical bilinear form too.

3. Motion groups of elliptic planes.

The triplet (F, A, f) is termed *an elliptic plane, if*

(a) *F is a commutative field of characteristic different from 2,*
(b) *A has rank 3 over F,*
(c) *$f(x, y)$ is an ordinary symmetrical bilinear form over (F, A) such that*

(c^*) $$f(x, x) = 0 \text{ implies } x = 0.$$

The question arises [and seems to be open] which fields F may be the fields of coordinates of an elliptic plane. It is a consequence of a well known theorem on polarities of projective planes [see

Baer [1], p.82, Theorem 5] that F must be infinite. Whenever F is a commutative field, there exists a projective plane (F, A) over F and there exist non-trivial symmetrical bilinear forms f over (F, A). But these may or may not meet requirement (c^*). If P is a commutative field of any characteristic, and if the commutative field F is obtained by adjoining to P two algebraically independent elements u and v, then the form $x_0y_0 + x_1uy_1 + x_2vy_2$ is symmetrical, bilinear and meets requirement (c^*). Thus F may have any characteristic; and this example shows incidentally the indispensability of the requirement that F be of characteristic different from 2.

Suppose now that (F, A, f) is an elliptic plane. *A motion of (F, A, f) is a linear transformation ν of (F, A) which has determinant $+1$ and which preserves f.* It is clear that the totality of motions of (F, A, f) is a group, *the motion group of* (F, A, f); and we note that the motion group does not change, if we substitute for f any form which defines the same polarity as f, since such a form is necessarily a multiple fc of f. We note that f defines a polarity. It follows from (c^*) that no point is on its polar [with respect to this polarity].

THEOREM: *The group Φ of linear transformations of the linear manifold (F, A) has Properties* (L.1) *and* (L.2) *if, and only if, Φ is the motion group of an elliptic plane (F, A, f).*

PROOF: Assume first that Φ is the motion group of the elliptic plane (F, A, f). We begin by proving the following property of Φ.

(L.1′) *If $\alpha \neq 1$ is in Φ, then the rank of $P(\alpha)$ does not exceed* 1.

Suppose that α is in Φ and that $P(\alpha)$ contains a line L. The pole Q of L is characterized by the equation $f(L, Q) = 0$; and is a fixed point of α, since L is a fixed line of α and α preserves f. If $q \neq 0$ is in Q, then there exists a number $t \neq 0$ in F such that $q\alpha = tq$. From $A = L \oplus Q$ and $L < P(\alpha)$ we infer that the determinant of α is t. But α is a motion and has therefore determinant $+1$. Hence $t = 1$ so that $\alpha = 1$.

(L.1″) *If ν is an involution in Φ, then $P(\nu)$ is a point and $N(\nu)$ a line.*

We have $A = P(\nu) \oplus N(\nu)$. Since the determinant of ν is $+1$, $N(\nu)$ has even rank which cannot be 0, as $\nu \neq 1$. Hence $N(\nu)$ is a line and $P(\nu)$ a point, since the rank of A is three.

(L.2′) *If Q is a point, then there exists an involution ν in Φ such that $Q = P(\nu)$ and such that $N(\nu)$ is the polar of Q.*

We note first that the polar of Q is the line L defined by the equation $f(Q, L) = 0$; and that Q is not on L[by (c^*)]. Hence $A = Q \oplus L$. Since the characteristic of F is not 2, there exists one and only one involutorial linear transformation ν such that $P(\nu) = Q$ and $N(\nu) = L$. It is clear that ν has determinant $+1$. If x is an element in A, then there exist uniquely determined elements x' and x'' in Q and L respectively such that $x = x' + x''$. Hence

$$f(a\nu, b\nu) = f(a' - a'', b' - b'') = f(a', b') + f(a'', b'') = \\ = f(a' + a'', b' + b'') = f(a, b)$$

so that ν preserves f. Hence ν is a motion and consequently an element in Φ.

(L.3) *If $f(a, a) = f(b, b)$, then there exists an involution in Φ which interchanges a and b.*

This is an immediate consequence of (L.2′) in case $a = \pm b$. If $a \neq \pm b$, then $F(a + b)$ and $F(a - b)$ are points; and it follows from the symmetry of f that

$$f(a + b,\ a - b) = f(a, a) + f(b, a) - f(a, b) - f(b, b) = 0$$

so that $F(a - b)$ is on the polar of $F(a + b)$. We infer from (L.2′) the existence of an involution ν in Φ such that $P(\nu) = F(a + b)$ and $N(\nu)$ is the polar of $F(a + b)$. Hence $F(a - b)$ is on $N(\nu)$. Thus $(a + b)\nu = a + b$ and $(a - b)\nu = b - a$; and this implies $a\nu = b$ so that the involution ν interchanges a and b.

(L.4) *If ν is in Φ and $N(\nu) \neq 0$, then ν is an involution.*

There exists an element $a \neq 0$ such that $a\nu = -a$. Since Fa is a fixed point of ν, the polar L of Fa is a fixed line of ν. If $b \neq 0$ is on L, then $b\nu$ is on L too. If Fb is a fixed point of ν, then $b\nu = eb$; and we have $f(b, b) = f(b\nu, b\nu) = e^2 f(b, b)$, since ν preserves f. Hence $e^2 = 1$; and one verifies that $Fa + Fb \leqq P(\nu^2)$ so that $\nu^2 = 1$ by (L.1′). If Fb is not a fixed point, then $f(b, b) = f(b\nu, b\nu)$, since ν preserves f; and we may deduce from (L.3) the existence of an involution ω in Φ which interchanges b and $b\nu$. It is clear that $L = Fb + Fb\nu$ is a fixed line of L, that $P(\omega) = F(b + b\nu) = F(b + b\omega)$ is on L, and that the pole Fa of L is a fixed point of ω. From this last remark it follows that Fa is on $N(\omega)$; and now one verifies that $Fa + Fb \leqq P(\nu\omega)$. But then it follows from (L.1′) that $\nu\omega = 1$. Hence $\nu = \omega$ is an involution.

(L.1''') $P(v) \neq 0$ *for every* v *in* Φ.

If $a \neq 0$ is in A, then $f(-a, -a) = f(a, a) = f(av, av)$, since v preserves f. There exists by (L.3) an involution ω in Φ which interchanges $-a$ and av. Then $av\omega = -a$ so that $a \neq 0$ is in $N(v\omega)$. It follows from (L.4) that $v\omega = v$ is an involution. It follows from (L.1'') that $N(v)$ and $N(\omega)$ are lines in the plane (F, A). Their intersection is certainly not 0; and it is clear that

$$0 < N(v) \cap N(\omega) \leqq P(v\omega) = P(v),$$

as we intended to show.

(L.1) is an immediate consequence of (L.1') and (L.1''') whereas (L.2) is contained in (L.2'). Thus we have shown that every motion group of an elliptic plane is an L-group of linear transformations.

Assume now that Φ is an L-group of linear transformations. Then we deduce from § 2, Proposition 1 and § 2, Corollary 4 that F is a commutative field of characteristic different from 2 and that A has rank 3 over F. There exists by § 2, Proposition 2, § 2, Corollary 4 and § 2, Lemma 4 an ordinary symmetrical bilinear form f over (F, A) which meets requirement (c^*) and which is preserved by every transformation in Φ. It follows from § 2, Corollary 5 that every transformation in Φ has determinant $+1$; and thus we have shown that Φ is a subgroup of the motion group Φ_0 of the elliptic plane (F, A, f). We have shown in the first part of this proof that Φ_0 is an L-group too. If v is an involution in Φ_0, then $P(v)$ is a point by (L.1); and there exists by (L.2) an involution ω in the L-group Φ such that $P(v) = P(\omega)$. It follows from § 2, Proposition 2 that the L-group Φ_0 contains only one involution σ with given point $P(\sigma)$. Hence $v = \omega$ so that Φ contains every involution in Φ_0. It follows from § 2, Corollary 2 that the L-group Φ_0 is generated by its involutions. Since these are all contained in Φ, we have $\Phi = \Phi_0$. Thus Φ is the motion group of the elliptic plane (F, A, f), as we intended to show.

We consider now the motion group Φ of the elliptic plane (F, A, f). Because of the preceding theorem Φ is an L-group of linear transformations so that the results of § 2 may be used freely.

If v is a linear transformation of (F, A), then an auto-projectivity is obtained by mapping the subspace S upon the subspace Sv. We shall denote this induced auto-projectivity by v^{π}.

PROPOSITION 1: *If Φ is an L-group of linear transformations, then mapping ν in Φ upon the auto-projectivity ν^π constitutes an isomorphism.*

PROOF: It is clear that π is a homomorphism. If ν is in Φ and $\nu^\pi = 1$, then every point is a fixed point of ν; and $\nu^2 = 1$ may be inferred from § 2, Lemma 3. We deduce from § 2, Corollary 1 that the fixed points of an involution are just the points on a certain line and one point off this line. Thus ν is not an involution. Hence $\nu = 1$, as we wanted to show.

To describe a number of characteristic properties of the group Φ^π of auto-projectivities we need two definitions.

DEFINITION 1: *The auto-projectivity ϱ of the projective plane Π is a reflection with center $C(\varrho)$ and axis $a(\varrho)$, if ϱ has order 2, if every line through $C(\varrho)$ and every point on $a(\varrho)$ is left invariant by ϱ, and if the point $C(\varrho)$ is not on the line $a(\varrho)$.*

In other words: reflections are involutorial perspectivities whose center and axis are not incident.

DEFINITION 2: *The group Λ of auto-projectivities of the projective plane Π is elliptic, if it meets the following requirements.*

(E.1) *Every element in Λ is the product of two reflections in Λ.*

(E.2) *To every point Q there exists one and only one reflection with center Q in Λ.* *To every line L there exists one and only one reflection with axis L in Λ.*

(E.3) *The product of three different reflections in Λ is a reflection, if their centers are collinear.* *The product of three different reflections in Λ is a reflection, if their axes are copunctual.*

The postulates (E) have been stated in a convenient, self-dual form. They are redundant; and it would be easy to state them in such a form that the planar character would be a provable fact.

The justification for the term „elliptic" is contained in the following

PROPOSITION 2: *If Φ is an L-group of linear transformations, then Φ^π is an elliptic group of planar auto-projectivities.*

PROOF: (F, A) is a projective plane by § 2, Proposition 1. It follows from § 2, Corollary 1 that ν^π is a reflection with center $P(\nu)$ and axis $N(\nu)$ whenever ν is an involution in Φ. It follows from Proposition 1 that ν in Φ is an involution if, and only if, ν^π is a reflection. Now one deduces (E.1) from § 2, Corollary 2, (E.2) from § 2, Proposition 2 and (E.3) from § 2, Lemma 5.

4. Elliptic groups of planar auto-projectivities.

Throughout this section we consider a projective plane Π [in which the Theorem of Desargues may or may not hold] and an *elliptic* group Λ of auto-projectivities of Π [in the sense of § 3, Definition 2]. It is our objective to derive a number of purely group theoretical properties of the group Λ. The ellipticity hypothesis need not be restated and much use will be made of its self-dual character.

LEMMA 1: *The following properties of the reflections α and β in Λ are equivalent.*

(i) $\alpha\beta = \beta\alpha$ *is an involution.*
(ii) $C(\alpha)$ *is on* $a(\beta)$.
(iii) $C(\beta)$ *is on* $a(\alpha)$.

PROOF: For reasons of symmetry it suffices to prove the equivalence of (i) and (iii). If (i) is true, then α and β are different reflections in Λ so that $C(\alpha) \neq C(\beta)$ by (E.2). One deduces from (i) and the definition of center that $C(\beta) = C(\alpha\beta\alpha) = C(\beta)\alpha$. But every fixed point of α with the exception of $C(\alpha)$ is on the axis $a(\alpha)$; and so the fixed point $C(\beta)$ of α is on $a(\alpha)$. Hence (iii) is a consequence of (i). — Assume conversely the validity of (iii). Since $C(\beta)$ is on $a(\alpha)$ and $C(\alpha)$ is not, $C(\alpha) \neq C(\beta)$ and consequently $\alpha \neq \beta$. Next we note that $C(\beta)$ is a fixed point of α, as a point on the axis $a(\alpha)$. Hence $C(\beta) = C(\beta)\alpha = C(\alpha^{-1}\beta\alpha)$. Consequently the reflections β and $\alpha^{-1}\beta\alpha$ have the same center; and it follows from (E.2) that $\beta = \alpha^{-1}\beta\alpha$ or $\alpha\beta = \beta\alpha$. This implies (i), since α and β are different involutions.

LEMMA 2: *The following properties of the element ϱ in Λ are equivalent.*

(i) ϱ *is an involution.*
(ii) ϱ *is a reflection.*
(iii) $\varrho \neq 1$ *possesses at least two fixed points.*
(iv) $\varrho \neq 1$ *possesses at least two fixed lines.*

PROOF: Assume first that ϱ is an involution. We deduce from (E.1) the existence of reflections ϱ' and ϱ'' such that $\varrho = \varrho'\varrho''$; and we deduce from (E.1) the existence of reflections α, β in Λ such that $\varrho' = \alpha\beta$. Thus $\varrho = \alpha\beta\varrho''$ is a product of three reflections; and ϱ is trivially a reflection, if two of the three reflections α, β, ϱ'' are equal. Thus we may assume that they are all different. Since α, β and $\alpha\beta = \varrho'$ are reflections, it follows that α, β and ϱ'

are three different commuting reflections; and it follows from Lemma 1 that $C(\varrho')$ is on $a(\alpha)$ and $a(\beta)$. Since ϱ' and ϱ'' are two different and commuting reflections [as ϱ is an involution], it follows from Lemma 1 that $C(\varrho')$ is also on $a(\varrho'')$. The three axes $a(\alpha)$, $a(\beta)$ and $a(\varrho'')$ have therefore the common point $C(\varrho')$; and now it follows from (E.3) that $\alpha\beta\varrho'' = \varrho'\varrho'' = \varrho$ is a reflection. Hence (ii) is a consequence of (i).

If ϱ is a reflection, then every point on the axis $a(\varrho)$ is a fixed point; and so ϱ possesses at least three fixed points. Hence (iii) is a consequence of (ii).

Assume next the validity of (iii). We deduce from (E.1) the existence of reflections ϱ' and ϱ'' in Λ such that $\varrho = \varrho'\varrho''$. From $\varrho \neq 1$ we infer $\varrho' \neq \varrho''$; and it follows from (E.2) that $a(\varrho') \neq a(\varrho'')$ The two different lines $a(\varrho')$ and $a(\varrho'')$ meet therefore in a point Q which is a fixed point of ϱ' and ϱ'' and consequently of $\varrho = \varrho'\varrho''$. But ϱ possesses at least two fixed points by (iii); and so there exists a fixed point $R \neq Q$ of ϱ. We deduce now from (E.2) the existence of one and only one reflection τ in Λ whose axis is the line $Q + R$. Then $a(\varrho')$, $a(\varrho'')$ and $a(\tau)$ have the common point Q; and one deduces from (E.3) that $\varrho\tau = \varrho'\varrho''\tau = \nu$ is likewise a reflection. Since the points Q and R are fixed points of ϱ [by construction] and fixed points of τ [as points on the axis $a(\tau)$], they are also fixed points of the reflection $\varrho\tau = \nu$. But $\varrho \neq 1$ implies $\tau \neq \nu$; and it follows from (E.2) that $a(\tau) \neq a(\nu)$. Hence it is impossible that both Q and R are on $a(\nu)$; and it follows from the properties of reflections that one of them is the center of ν [since the center and the points on the axis are all the fixed points of a reflection]. The center of ν is therefore on the axis of τ; and it follows from Lemma 1 that $\tau\nu = \nu\tau = \varrho$ is an involution. Hence (i) is a consequence of (iii). This completes the proof of the equivalence of properties (i) to (iii); and the equivalence of property (iv) with these properties follows by duality.

REMARK: Using (E.2) and Lemmas 1, 2 one may define a Λ-polarity by the rule:

The point Q and the line L are in the pole-polar-relation if, and only if, there exists a reflection with center Q and axis L in Λ.

That in this way a polarity is defined, is fairly easy to see; we omit the details of the argument, as no use will be made of this fact.

Naturally the transformations in Λ preserve this Λ-polarity. The question may be asked which groups of planar auto-pro-

jectivities preserving a polarity are elliptic. In the presence of such an invariant polarity one could certainly omit „half" of the postulates (E.2) and (E.3). But then we would have instead of self-dual postulates totally undual postulates.

LEMMA 3: *Assume that α and β are two different reflections in Λ.*

(a) *If $\alpha\beta$ is a reflection, then $C(\alpha\beta) = a(\alpha) \cap a(\beta)$ and $a(\alpha\beta) = C(\alpha) + C(\beta)$.*

(b) *If $\alpha\beta$ is not a reflection, then $a(\alpha) \cap a(\beta)$ is the one and only one fixed point of $\alpha\beta$ and $C(\alpha) + C(\beta)$ is the one and only one fixed line of $\alpha\beta$.*

PROOF: If $\alpha\beta$ is a reflection, then $\beta = \alpha(\alpha\beta)$ is the product of the two different reflections α and $\alpha\beta$; and $\alpha(\alpha\beta) = (\alpha\beta)\alpha$ is itself a reflection. It follows from Lemma 1 that $C(\alpha\beta)$ is on $a(\alpha)$; and that $C(\alpha\beta)$ is on $a(\beta)$, is seen likewise. From $\alpha \neq \beta$ and (E.2) we deduce $a(\alpha) \neq a(\beta)$; and as distinct lines meet in a point, we see that $C(\alpha\beta) = a(\alpha) \cap a(\beta)$. — The equation $a(\alpha\beta) = C(\alpha) + C(\beta)$ follows by duality.

Assume next that $\alpha\beta$ is not a reflection. We infer from Lemma 2 that $\alpha\beta$ possesses at most one fixed point. It follows from (E.2) and $\alpha \neq \beta$ that $a(\alpha) \neq a(\beta)$; and so these lines meet in one and only one point. This point is a fixed point of $\alpha\beta$, since as a point on $a(\alpha)$ it is a fixed point of α and as a point on $a(\beta)$ it is a fixed point of β. — That $C(\alpha) + C(\beta)$ is the one and only one fixed line of $\alpha\beta$, follows by duality.

NOTATION 1: If ν is an element in Λ, $\nu^2 \neq 1$, then it follows from (E.1) and Lemma 3, (b) that ν possesses one and only one fixed point which we denote by $C(\nu)$; and ν possesses one and only one fixed line which we denote by $a(\nu)$. — It follows from Lemma 3 that this choice of notation is in accordance with the corresponding notations for reflections.

NOTATION 2: If Σ is a subset of the group Λ, then $J(\Sigma)$ is the totality of involutions ν in Λ such that every $\nu\sigma$ for σ in Σ is an involution in Λ.

This concept $J(\Sigma)$ is defined for every abstract group. It is an extension of a concept introduced in § 1.C, (9). — We note furthermore that $J = J(1)$ is just the totality of involutions in the group Λ.

PROPOSITION 1: *The following properties of the reflection ϱ and the element $\sigma \neq 1$ in Λ are equivalent.*

(i) *ϱ belongs to $J(\sigma)$.*

(ii) *$C(\varrho)$ is on $a(\sigma)$.*

(iii) *$C(\sigma)$ is on $a(\varrho)$.*

PROOF: Assume first that ϱ belongs to $J(\sigma)$. Then $\varrho\sigma = \tau$ is an involution and $\sigma = \tau\varrho$. Applying Lemma 2—3 and Notation 1 we find that $a(\sigma) = C(\tau) + C(\varrho)$; and this shows that (ii) is a consequence of (i). Assume conversely that $C(\varrho)$ is on $a(\sigma)$. We deduce from (E.1) the existence of reflections σ', σ'' in Λ such that $\sigma = \sigma'\sigma''$; and it follows from Lemma 3 and Notation 1 that $a(\sigma) = C(\sigma') + C(\sigma'')$. If ϱ equals σ' or σ'', then $\varrho\sigma$ equals σ'' or $\sigma''\sigma'\sigma''$ each of which is a reflection so that ϱ belongs to $J(\sigma)$. If on the other hand ϱ is different from σ' and σ'', then it follows from [(E.2) and] (ii) that $C(\varrho)$, $C(\sigma')$ and $C(\sigma'')$ are three different points on the line $a(\sigma)$; and it follows from (E.3) that $\varrho\sigma'\sigma'' = \varrho\sigma$ is a reflection; and ϱ belongs again to $J(\sigma)$. This completes the proof of the equivalence of (i) and (ii); and the equivalence of (i) and (iii) follows by duality.

PROPOSITION 2: *The following properties of the reflection τ and the element $\sigma \neq 1$ in Λ are equivalent.*

(i) *τ belongs to $J[J(\sigma)]$.*

(ii) $C(\tau) = C(\sigma)$.

(iii) $a(\tau) = a(\sigma)$.

PROOF: Suppose first that τ belongs to $J[J(\sigma)]$. Consider two distinct points S and T on $a(\sigma)$. There exist [by (E.2)] uniquely determined reflections α, β in Λ such that $S = C(\alpha)$ and $T = C(\beta)$. It follows from Proposition 1 that α and β are in $J(\sigma)$, since $C(\alpha)$ and $C(\beta)$ are on $a(\sigma)$. It follows from (i) that τ belongs to $J(\alpha)$ and $J(\beta)$; and hence it follows from Proposition 1 that $a(\tau)$ passes through $C(\alpha)$ and $C(\beta)$. Consequently
$a(\tau) = C(\alpha) + C(\beta) = a(\sigma)$ so that (iii) is a consequence of (i).

Assume next the validity of (iii). Consider a reflection ϱ in $J(\sigma)$. It follows from Proposition 1 that $C(\varrho)$ is on $a(\sigma) = a(\tau)$ and again from Proposition 1 that τ belongs to $J(\varrho)$. Thus τ is in every $J(\varrho)$ with ϱ in $J(\sigma)$ so that τ is in $J[J(\sigma)]$. Hence (i) is a consequence of (iii). — The equivalence of (i) and (ii) follows by duality.

THEOREM: *Every elliptic group Λ of planar auto-projectivities has the following properties.*

(G.1) *$J[J(\sigma)]$, for $\sigma \neq 1$ in Λ, consists of one and only one involution which we denote by σ^*.*

(G.2) *$\alpha^* = \beta^*$ implies $J(\alpha) = J(\beta)$ whenever α and β are elements, not 1, in Λ.*

(G.3) *If α and β are two different involutions in Λ, then $(\alpha\beta)^* = J(\alpha) \cap J(\beta)$.*

(G.4) *The center of the group Λ is 1.*

PROOF: An element in Λ is an involution if, and only if, it is a reflection [Lemma 2]. Now (G.1) is a consequence of (E.2) and Proposition 2; and (G.2) is a consequence of Propositions 1 and 2.

Suppose next that α and β are different involutions in Λ. Then they are different reflections in Λ; and it follows from Proposition 1 that the reflection τ belongs to $J(\alpha) \cap J(\beta)$ if, and only if, $a(\tau) = C(\alpha) + C(\beta)$. It follows from Lemma 3, Notation 1 and Proposition 2 that $a(\tau) = C(\alpha) + C(\beta) = a(\alpha\beta) = a[(\alpha\beta)^*]$. Henc $\tau = (\alpha\beta)^*$ by (E.2); and this proves the validity of (G.3).

If the transformation σ in Λ commutes with the reflection ϱ in Λ, then the center $C(\varrho)$ of ϱ is clearly a fixed point of σ. It follows from (E.2) that a center element of Λ leaves invariant every point in Π. Hence the center of Λ is 1 so that (G.4) is true too.

REMARK 2: If (G.1) is satisfied by the group Λ, then one verifies without difficulty that (G.2) is equivalent with the following condition.

(G.2′) *If* $\sigma \neq 1$ *is an element in* Λ, *then* $J(\sigma) = J(\sigma^*)$.

Remembering the definition of σ^* [in (G.1)] we see that this is equivalent to requiring.

(G.2″) *If* $\sigma \neq 1$ *is an element in* Λ, *then* $J(\sigma) = J(J[J(\sigma)])$.

This condition is trivially satisfied whenever σ is an involution. But in case $\sigma^2 \neq 1$ it does not seem possible to derive this condition from the other conditions.

5. The incidence groups of A. SCHMIDT.

We want to prove in the present section that the class of groups which is characterized by the properties (G.1) to (G.4) of § 4 is identical with a class of groups introduced by A. Schmidt [1] under the name „Inzidenzgruppe". To do this we need the following fact which will also be used later in another context.

LEMMA: *If a group* G *has properties* (G.1) *and* (G.4), *the every element in* G *is the product of two involutions in* G.

PROOF: Suppose that $g \neq 1$ is an element in G. If the set $J(g)$ were vacuous, then $J[J(g)]$ would be the set of all involutions in G; and it would follow from (G.1) that g^* is the one and only one involution in G. But then g^* would belong to the center of G, since $x^{-1}g^*x$ is an involution for every x in G. It follows from (G.4) that this is impossible. Hence there exists an involution j in $J(g)$. Consequently $jg = k$ is an involution and $g = kj$ is the product of two involutions.

A. Schmidt [1] has defined an *incidence group* as a group G with the following properties.

(I.1) *G is generated by its involutions.*

(I.2) *To every involution j in G there exists an involution j' in G such that jj' is not an involution.*

(I.3) *It is possible to assign to every pair of distinct involutions a and b in G an involution $a \circ b$ in G meeting the following requirements.*

(a) $a \circ b = b \circ a$.

(b) *Suppose that a, b, c are involutions in G and $a \neq b$.*

(b') *abc is an involution if, and only if, $(a \circ b)c$ is an involution.*

(b'') *If ac and bc are involutions, then $c = a \circ b$.*

Now we prove the announced result.

THEOREM: *A group G has properties (G.1) to (G.4) if, and only if, G is an incidence group.*

PROOF: Assume first the validity of (G.1) to (G.4). Then every element in G is the product of two involutions [Lemma 1], proving the validity of (I.1). If the involution j in G would commute with every involution in G, then j would belong to the center of G, contradicting (G.4). Thus (I.2) is true.

If a and b are distinct involutions in G, then $(ab)^* = J[J(ab)]$ is a well determined involution by (G.1); and we may let

$$a \circ b = (ab)^*.$$

It is easy to see that $J(ab) = J[(ab)^{-1}] = J(ba)$. Hence $a \circ b = b \circ a$. If c is some involution, then $(a \circ b)c = (ab)^*c$ is an involution if, and only if, c belongs to $J[(ab)^*]$. But $J[J((ab)^*)] = (ab)^*$; and it follows from (G.2) that $J(ab) = J[(ab)^*]$. Thus $(a \circ b)c$ is an involution if, and only if, $c(ab)$ is an involution; and this is the case if, and only if, abc is an involution. Hence (b') is true. — If ac and bc are both involutions, and if c is an involution, then c belongs to $J(a)$ and to $J(b)$; and it follows from (G.3) that $c = J(a) \cap J(b) = (ab)^* = a \circ b$. Thus (b'') is true too. Hence G is an incidence group.

Assume conversely that G is an incidence group. Then every element in G is the product of two involutions [for a proof, see A. Schmidt [1], 3, Satz, p. 233]. One deduces from (b) that $(ab)^* = J[J(ab)] = a \circ b$ whenever a and b are different involutions. This proves (G.1), since every element in G is the product of two involutions. One deduces (G.2) from (b'), (G.3) from (b''). — If finally z belongs to the center of G, then $z = z'z''$ where z' and z'' are involutions. Since z commutes with z' and

z'', it follows that z is 1 or an involution. But it follows from (I.2) that an involution cannot be in the center. Hence $z = 1$; and this proves (G.4).

REMARK: It becomes apparent form the proof that Schmidt's composition $a \circ b$ of the involutions is not a second and independent operation on the group elements, but is completely determined by the multiplicative properties of the group G.

6. The characteristic properties of projective space groups.

It is the purpose of this section to show that groups with properties (G.1) to (G.4) [of § 4, Theorem] are S^*-groups i.e. projective space groups of dimension not less than two. Using § 5, Theorem we could do this simply by reference to a result of A. Schmidt [1, § 5, p. 237]. We shall, however, offer a direct proof, somewhat different from the one due to A. Schmidt and more appropriate in the present context. We begin by proving the following result.

PROPOSITION 1: *If the group G meets requirements (G.1) to (G.4), and if collinearity of the three involutions a, b, c in G is defined by the rule:*

(C) *a, b, c are collinear involutions if, and only if, abc is an involution;*

then the totality J of involutions in G forms a projective plane.

PROOF: Considering that abc is an involution if, and only if cab is an involution — assuming that a, b, c are involutions — it follows that $J(ab)$ is exactly the set of all involutions collinear with a and b. Consequently we may term the sets $J(g)$ for $g \neq 1$ *the lines in* J, if we only remember that by § 5, Lemma every element, not 1, in G is the product of two distinct involutions.

(1.a) *Two distinct involutions belong to one and only one line.*

If a and b are distinct involutions, then they certainly belong to the line $J(ab)$. Suppose next that they also belong to the line $J(g)$. Then g^* is different from, and commutes with, a and b. Hence $g^* = J(a) \cap J(b) = (ab)^*$ by (G.3); and it follows from (G.2) that $J(g) = J(ab)$. This proves (1.a).

(1.b) *Two distinct lines have one and only one involution in common.*

Suppose that g and h are elements, not 1, in G and that $J(h) \neq J(g)$. It follows from (1.a) that $J(h)$ and $J(g)$ possess at most one common involution. From $J(h) \neq J(g)$ and (G.2) we infer that g^* and h^* are different involutions. Hence $g^*h^* \neq 1$ and we may form the involution $j = (g^*h^*)^*$ by (G.1). Now g^*

and h^* belong to $J(g^*h^*) = J(j)$; and thus j is different from, and commutes with, g^* as well as with h^*. Consequently j belongs to $J(g^*) = J(g)$ [by (G.2)] as well as to $J(h^*) = J(h)$, as we intended to show.

(1.c) *The two distinct involutions a and b determine the line $J(ab)$ and the two distinct lines $J(g)$ and $J(h)$ meet in $(g^*h^*)^*$.*

The proof of this fact is contained in the proofs of (1.a), (1.b).

(1.d) *There exist three involutions which are not collinear.*

Since $G \neq 1$, there exists an element $g \neq 1$ in G. By § 5, Lemma there exist involutions a, b such that $g = ab$. These are both on the line $J(ab) = J(g^*)$ whereas the involution g^* is not on this line.

(1.e) *Every line carries at least three involutions.*

Every line has the form $J(ab)$ where a and b are different involutions [§ 5, Lemma]; and the two involutions a and b are certainly on $J(ab)$. Suppose by way of contradiction that the line $J(ab)$ does not carry a third involution. Since a is not on the line $J(a)$, the lines $J(a)$ and $J(ab)$ meet in exactly one involution which of necessity is b; and likewise we see that $J(b)$ and $J(ab)$ meet in a. It follows that a and b are commuting, but different involutions. Hence ab itself is an involution so that in particular $ab = (ab)^*$. It follows from (G.4) that a does not commute with every element in G; and since every element in G is a product of two involutions [§ 5, Lemma] there exists an involution a' which does not commute with a. Since a is not on $J(a')$, the lines $J(a')$ and $J(ab)$ meet in b. But then b is on $J(a')$ and this is equivalent to the fact that a' is on $J(b)$. Since a and a' do not commute, a' is different from the involutions a and ab on $J(b)$. Likewise there exists an involution b' on $J(a)$ which is different from ab and b. The line $J(a'b')$ carries a' and b' neither of which is on $J(g)$, since otherwise one of the lines $J(a)$ or $J(b)$ would be equal to $J(g)$ [use (1.a)]. This line likewise cannot carry a or b, but meets the line $J(ab)$ through a and b in some involution w which would be different from a and b. This contradiction proves (1.e). The statements (1.a) to (1.e) just contain the contention of Proposition 1.

PROPOSITION 2: *If the group G satisfies conditions (G.1) to (G.4), then the derived geometrical structure $D(G)$ [see §1.A] is a three-dimensional projective space.*

PROOF: It will be convenient to adopt the following terminology which is in essential agreement with the terminology of § 1, the homogeneity of $D(G)$ and Proposition 1. The elements in G will

be termed *points*; if g is an element in G, then $P(g)$ is the totality of elements x in G such that xg is an involution, and $P(g)$ is the *plane* [determined by] g; if $a \neq 1$ is in G, and if b is a random element in G, then the points of $J(a)b$ form a *line*.

We note that $P(1) = J$ is the plane of all the involutions.

(2.1) $P(g) = Jg^{-1}$.

(2.2) $P(g) \cap P(h) = J(g^{-1}h)g^{-1} = J(h^{-1}g)h^{-1}$ *for* $g \neq h$.

These two facts are easily verified. (2.2) asserts that two different planes meet in a line; and (2.1) implies that the plane $P(g)$ has the same geometrical structure as the [by Proposition 1] projective plane of all the involutions.

(2.3) *The two different points g and h determine one and only one line, namely $J(h^{-1}g)(g^*h^*)^*$.*

It follows from (1.c) that $(g^*h^*)^*$ is the uniquely determined common involution of the lines $J(g)$ and $J(h)$. Hence $(g^*h^*)^*g$ and $(g^*h^*)^*h$ are involutions so that $a = g(g^*h^*)^*$ and $b = h(g^*h^*)^*$ are two distinct involutions. We have $ab = ab^{-1} = gh^{-1} \neq 1$; and it is clear now that a and b belong to the line $J(ab) = J(gh^{-1})$. Hence $g = a(g^*h^*)^*$ and $h = b(g^*h^*)^*$ belong to the line $J(gh^{-1})(g^*h^*)^*$.

Suppose now that g and h are both on the line $J(u)v$ where $u \neq 1$. Then $g' = gv^{-1}$ and $h' = hv^{-1}$ are distinct involutions on the line $J(u)$; and it follows from (1.c) that $J(u) = J(g'h') = J(gh^{-1})$. If x is any element in $J(u)v$, then xv^{-1} is an involution in $J(u)$. It follows from (1.c) that $J(u) = J(j'j'')$ whenever j' and j'' are distinct involutions in $J(u)$; and this implies that

the product of three involutions in $J(u)$ is likewise an involution in $J(u)$.

However, we have shown that xv^{-1}, vg^{-1} and $g(g^*h^*)^*$ are involutions in $J(u)$. Hence their product $(xv^{-1})(vg^{-1})(g(g^*h^*)^*) = x(g^*h^*)^*$ is in $J(u)$; and this shows that $J(u)v = J(gh^{-1})(g^*h^*)^*$, as we claimed.

(2.4) *Every plane carries with any two different points the whole line through them.*

If a and b are two distinct points in the plane $P(g) = Jg^{-1}$, then ag and bg are distinct involutions. They determine by (1.c) the line $J[(ag)(bg)] = J(ab^{-1})$ of involutions; and so a and b both belong to the line $J(ab^{-1})g^{-1}$ in $P(g) = Jg^{-1}$. It follows from (2.3) that this is the only line carrying a and b.

(2.5) *If two planes pass through a point p, then their line of intersection passes through p.*

Obvious.

(2.6) *A line $J(a)b$ and a plane $P(g)$, not through $J(a)b$, meet in a point.*

Because of (2.4) we need only show that $J(a)b$ and $P(g)$ possess a common point. Now $P(g) = Jg^{-1}$ so that $b = g^{-1}$ would imply that $J(a)b$ is on $P(g)$. Hence $bg \neq 1$. It follows from Proposition 1 that the lines $J(a)$ and $J(bg)$ possess a common involution j. Then jb is certainly on $J(a)b$; and $jb = (jbg)g^{-1}$ is in $Jg^{-1} = P(g)$, since j is in $J(bg)$ so that jbg is an involution. Thus jb is the desired point of intersection of $J(a)b$ and $P(g)$.

(2.7) *A line and a point, not on the line, determine one and only one plane.*

Since two distinct planes meet in a line by (2.2), we need only show the existence of at least one plane through the point p and the line $J(a)b$, not through p. Denote by p', p'' two different points on the line $J(a)b$; and consider the three planes $P(p)$, $P(p')$ and $P(p'')$. The last two meet in a line by (2.2); and a line and a plane have always a common point by (2.6). Thus there exists a common point g on the planes $P(p')$, $P(p'')$ and $P(p)$. Then gp', gp'' and gp are involutions; and this implies also that pg, $p'g$ and $p''g$ are involutions. Hence p, p' and p'' are points on the plane $P(g)$; and it follows from (2.4) that this plane $P(g)$ carries the whole line $J(a)b$.

Remembering that every plane $P(g)$ is a projective plane in the strict sense of the word [by (2.1) and Proposition 1] we deduce now from (2.2) to (2.7) that the points, lines and planes which we defined in the beginning of this proof just constitute a three-dimensional projective space [see, for instance, Menger [1]]. Hence $D(G)$ is a three-dimensional projective space, as we claimed.

REMARK: The principle of duality could not be used in the proof in its explicite form, since lines had been defined as intersections of planes, not self-dually. However, an analysis of the proof of (2.7) will show that we have used the principle of duality at least implicite.

7. The representations and their uniqueness.

We begin by stating a theorem that summarizes part of the results obtained sofar and that will permit us to put the problem of this section into proper focus.

THEOREM 1: *The following properties of the group G are equivalent.*

(i) *G is an S*-group.*
(ii) *G is isomorphic to an L-group of linear transformations.*
(iii) *G is isomorphic to the group of all motions of an elliptic plane.*
(iv) *G is isomorphic to an elliptic group of planar auto-projectivities.*
(v) *G has Properties* (G.1) *to* (G.4).
(vi) *The derived geometrical structure $D(G)$ is a three dimensional projective space.*

The proof of this theorem is effected by reference to the preceding results in the following fashion. We recall that the group G has been termed an S^*-group, if the derived geometrical structure is a projective space of dimension greater than 1. That every S^*-group is isomorphic to an L-group of linear transformations is the content of § 1.C, Theorem 2. We deduce from § 3, Theorem that a group of linear transformations is an L-group if, and only if, it is the group of all motions of an elliptic plane; and § 3, Propositions 1 and 2 show that the group of all motions of an elliptic plane induces isomorphically an elliptic group of planar auto-projectivities. It is a consequence of § 4, Theorem that elliptic groups of planar auto-projectivities have the properties (G); and (v) implies (vi) by § 6, Proposition 2 whereas it is trivial that (vi) implies (i).

We note that properties (ii) to (iv) assert the existence of certain representations of S^*-groups; and we have already pointed out that the representations as L-groups of linear transformations are the same as those as motion groups of elliptic planes. We recall that the representations constructed in § 1.C and § 3 were natural ones. But we have not shown yet that these are the only possible representations; and in particular we have not yet shown that all representations as elliptic groups of planar auto-projectivities are isomorphically induced by L-groups of linear transformations. With these questions [and related ones] we want to concern ourselves in the present section.

We shall use the name S^*-group to indicate any group with the equivalent properties (i) to (vi) of the above theorem; and we recall that because of § 1.B, Proposition 2 such groups have the following often used property.

(G.0) *Every element in G is the product of two involutions in G.*

That (G.0) is actually a consequence of (G.1) and (G.4), is the content of § 5, Lemma.

PROPOSITION 1: *If Λ is an elliptic group of auto-projectivities of the projective plane Π, then mapping the reflection σ in Λ upon its center $C(\sigma)$ constitutes a projectivity of the plane of involutions in $D(\Lambda)$ upon Π such that $C(\sigma)\alpha = C(\alpha^{-1}\sigma\alpha)$ for every α in Λ.*

PROOF: It is a consequence of § 4, Lemma 2 that every involution in Λ is a reflection; and thus it is a consequence of Property (E.2) that mapping σ upon $C(\sigma)$ constitutes a one to one mapping of the totality J of involutions in Λ upon the totality of points in Π. Suppose that α, β, γ are three different reflections in Λ. If the points $C(\alpha)$, $C(\beta)$, $C(\gamma)$ are collinear, then it follows from (E.3) that $\alpha\beta\gamma$ is a reflection. If conversely $\alpha\beta\gamma = \delta$ is a reflection, then it follows from § 4, Lemma 3 and § 4, Notation 1 that $C(\alpha) + C(\beta) = a(\alpha\beta) = a(\delta\gamma) = C(\delta) + C(\gamma)$, proving the collinearity of $C(\alpha)$, $C(\beta)$, $C(\gamma)$. But three points in the plane J in $D(\Lambda)$ are collinear if, and only if, their product belongs to J [see, for instance, § 6, Proposition 1]; and thus we have shown that $C(\alpha)$, $C(\beta)$, $C(\gamma)$ are collinear points in Π if, and only if, α, β, γ are collinear points in the plane J [in $D(\Lambda)$]. This proves Proposition 1 as $C(\sigma)\alpha = C(\alpha^{-1}\sigma\alpha)$ is an almost immediate consequence of the definition of the center.

THEOREM 2: *Every isomorphism between elliptic groups of planar auto-projectivities is induced by one and only one projectivity between the underlying projective planes.*

PROOF: Suppose that Λ is an elliptic group of auto-projectivities of the projective plane Π; and suppose that the auto-projectivity α of Π induces the identity automorphism in Λ. Then α commutes with every element in Λ and in particular with every reflection σ in Λ. Thus we find that $C(\sigma) = C(\alpha^{-1}\sigma\alpha) = C(\sigma)\alpha$ holds for every reflection σ in Λ. But every point in Π is the center of a reflection in Λ [by (E.2)] so that α leaves invariant every point in Π. Hence $\alpha = 1$; and this implies that an isomorphism of Λ upon some group of planar auto-projectivities is induced by at most one projectivity of Π.

Assume now that Θ is an elliptic group of auto-projectivities of the projective plane T; and that β is an isomorphism of Λ upon Θ. If Q is a point in Π, then there exists [by (E.2)] one and only one reflection $\sigma(Q)$ with center Q in Λ; and it follows from Proposition 1 that mapping Q onto $\sigma(Q)$ constitutes a projectivity of Π upon the plane J of involutions in $D(\Lambda)$. It is clear that β induces a projectivity of the plane J in $D(\Lambda)$ upon the plane J' of all involutions in Θ; and it follows from Proposition 1 that mapping the reflection ν in Θ upon its center $C(\nu)$ in T constitutes

a projectivity of the plane J' in $D(\Theta)$ upon the plane T. Mapping Q onto $Q\alpha = C[\sigma(Q)^\beta]$ constitutes therefore a projectivity of Π upon T. One verifies easily that, for every involution σ in Λ,

$$C(\alpha^{-1}\sigma\alpha) = C(\sigma)\alpha = C[\sigma(C[\sigma])^\beta] = C(\sigma^\beta).$$

Since $\alpha^{-1}\sigma\alpha$ and σ^β are both reflections in Θ [§ 4, Lemma 2], we infer $\alpha^{-1}\sigma\alpha = \sigma^\beta$ for every involution σ in Λ. Since every element in Λ and in Θ is a product of two reflections [by (E.1)], one verifies now that the isomorphism β is induced by the projectivity α, completing the proof.

COROLLARY 1: *An S^*-group possesses one and essentially only one representation as an elliptic group of planar auto-projectivities.*

This is an obvious consequence of Theorems 1 and 2.

COROLLARY 2: *Every elliptic group of planar auto-projectivities is isomorphically induced by the group of all motions of an elliptic plane.*

PROOF: Suppose that Λ is an elliptic group of auto-projectivities of the projective plane Π. Then Λ is an S^*-group [Theorem 1] and consequently isomorphic to the group Φ of all motions of an elliptic plane (F, A, f). Every element ν in Φ induces an auto-projectivity ν^π in the projective plane (F, A); and it follows from § 3, Propositions 1 and 2 that π is an isomorphism of Φ upon the elliptic group $\Theta = \Phi^\pi$ of auto-projectivities of (F, A). Now Corollary 2 is an immediate consequence of Corollary 1.

COROLLARY 3: *The Theorems of Desargues and Pappus hold in projective planes possessing elliptic groups of auto-projectivities.*

PROOF: If (F, A, f) is an elliptic plane, then F is a commutative field [see § 3, Theorem] so that the Theorems of Desargues and Pappus hold in the projective plane $(F.A.)$. Now Corollary 3 is an immediate consequence of Corollary 2.

THEOREM 3: *Isomorphisms between L-groups of linear transformations are induced by essentially uniquely determined semi-linear transformations between the underlying linear manifolds.*

PROOF: Suppose that Φ is an L-group of linear transformations of the linear manifold (F, A); and suppose that the semi-linear transformation τ of (F, A) commutes with every element in Φ [induces the identity automorphism in Φ]. If Q is a point in (F, A), then there exists an involution ν in Φ such that $Q = P(\nu)$ [by (L.2)]. Clearly $Q\tau = P(\nu)\tau = P(\tau^{-1}\nu\tau) = P(\nu) = Q$ so that every point is a fixed point. It is well known that τ is then a multiplication by a number in F; and this implies that isomorphisms

between L-groups are induced essentially by at most one semi-linear transformation.

Suppose now that Φ and Φ' are L-groups of linear transformations of the linear manifolds (F, A) and (F', A') respectively; and that $\varkappa$ is an isomorphism of Φ upon Φ'. We deduce from § 3, Theorem that Φ and Φ' are the groups of all motions of elliptic planes (F, A, f) and (F', A', f') respectively. It follows from § 3, Propositions 1 and 2 that Φ induces isomorphically the elliptic group Λ of auto-projectivities of the projective plane (F, A) and that Φ' induces isomorphically the elliptic group Λ' of auto-projectivities of the projective plane (F', A'). If ν is an element in Λ, then there exists one and only one transformation ν^{ξ} in Φ which induces ν; and we denote, as usual, by ω^{π} the auto-projectivity in Λ' which is induced by the transformation ω in Φ'. Since ξ, $\varkappa$ and π are isomorphisms, $\xi\varkappa\pi$ is an isomorphism of Λ upon Λ'. It is a consequence of Theorem 2 that the isomorphism $\xi\varkappa\pi$ is induced by a projectivity η of (F, A) upon (F', A'); and it is the content of the Fundamental Theorem of Projective Geometry that η is induced by some semi-linear transformation τ of (F, A) upon (F', A'). One verifies easily that τ induces $\varkappa$, as we claimed.

COROLLARY 4: *An S^*-group possesses one and essentially only one representation as an L-group of linear transformations.*

This is an immediate consequence of Theorems 1 and 3.

REMARK 1: If Φ is the group of all motions of the elliptic plane (F, A, f) and if c is a number, not 0, in F, then Φ is also the group of all motions of the elliptic plane (F, A, cf). — Conversely if Φ is the group of all motions of the elliptic planes (F, A, f) and (F, A, g), then it is not difficult to prove the existence of a number $c \neq 0$ in F such that $g = cf$. Thus the elliptic plane underlying such a group of motions is essentially uniquely determined.

REMARK 2: If the group Φ of linear transformations of the linear manifold (F, A) is an S^*-group, then Φ need not be an L-group, as is seen from easily constructed examples. [The rank of A may be too big or the field F may be chosen "too large", for instance]. — The situation changes somewhat, if we require that Φ induces an elliptic group of planar auto-projectivities, as may be seen from the next result.

PROPOSITION 2: *The group Φ of semi-linear transformations of the linear manifold (F, A) induces isomorphically an elliptic group of planar auto-projectivities if, and only if, there exists an L-group Θ of linear transformations of (F, A) such that $\Phi \otimes \{-1\} = \Theta \otimes \{-1\}$.*

Here as always $\otimes$ indicates the direct product.

PROOF: Assume first the existence of an L-group Θ of linear transformations of (F, A) such that $\Phi \otimes \{-1\} = \Theta \otimes \{-1\} = \Xi$. Then Ξ consists of linear transformations only. We map the element τ in Ξ upon the auto-projectivity τ^π which it induces. This mapping π is a homomorphism with kernel $\{-1\}$ such that $\Phi^\pi = \Theta^\pi = \Xi^\pi = \Lambda$ is an elliptic group of planar auto-projectivities [§ 3, Propositions 1 and 2] and now it is clear that Φ induces isomorphically an elliptic group of planar auto-projectivities.

Conversely we assume now that Φ is a group of semi-linear transformations of (F, A) and that mapping the transformation τ in Φ upon the induced auto-projectivity τ^π constitutes an isomorphism of Φ upon the elliptic group $\Lambda = \Phi^\pi$ of planar auto-projectivities. It is implicite in these hypotheses that A has rank 3 over F; and it follows from Corollary 3 that F is a commutative field. We note furthermore that [by Theorem 1] Φ and Λ are isomorphic S^*-groups.

(1) *If ν is an involution in Φ, then ν is linear, $A = P(\nu) \oplus N(\nu)$ and one of the subspaces $P(\nu)$, $N(\nu)$ is a point, the other one a line.*

To prove this, we note first that ν^π is an involution in Λ, since π is an isomorphism and ν an involution. It follows from § 4, Lemma 2 that ν^π is a reflection whose center Q is a point and whose axis L is a line in (F, A) satisfying $A = Q \oplus L$, since the center of a reflection is not on its axis. Since every point on L is a fixed point of ν, there exists a number $e \neq 0$ in F such that $x\nu = ex$. This implies already the linearity of ν, since L has rank 2, and since F is commutative. We infer now $e^2 = 1$ or $e = \pm 1$ from $\nu^2 = 1$. From the linearity of ν and $\nu^2 = 1$ we deduce furthermore the existence of a number f in F such that $x\nu = fx$ for x in Q and $f = \pm 1$. From $\nu^\pi \neq 1$ we deduce $e \neq f$; and this implies $e = -f$. It is clear now that Q is $P(\nu)$ or $N(\nu)$ and that L is accordingly $N(\nu)$ or $P(\nu)$; and this completes the proof of (1).

(2) *Every element in Φ is a linear transformation of determinant ± 1.*

By (G.0) every element in the S^*-group Φ is a product of two involutions. Involutions are by (1) linear transformations whose determinant is clearly ± 1. This proves (2). — We note that the commutativity of F makes it possible to speak of the determinant of linear transformations.

It is clear that -1 does not belong to Φ. Thus we may form the direct product $\Xi = \Phi \otimes \{-1\}$. It is clear that all the linear transformations in Ξ have determinant ± 1, since the same holds for Φ; and that the mapping π of transformations in Ξ upon the

induced auto-projectivities is a homomorphism of Ξ upon $\Lambda = \Phi^\pi$ with kernel $\{-1\}$. The totality Θ of transformations in Ξ with determinant $+1$ is clearly a subgroup of Ξ such that $\Xi = \Phi \otimes \{-1\} = \Theta \otimes \{-1\}$ and such that π induces an isomorphism of Θ upon Λ.

(3) *If ν is an involution in Θ, then $P(\nu)$ is a point and $N(\nu)$ is a line.*

Since the determinant of the involution ν is $+1$, the rank of $N(\nu)$ is even. Since the rank of A is 3, and since $\nu \neq 1$, it follows that $N(\nu)$ has rank 2; and $P(\nu)$ is consequently a point.

(4) *Θ is an L-group of linear transformations.*

Suppose that $\sigma \neq 1$ is an element in Θ. If σ is an involution, then $P(\sigma)$ is a point by (3). Suppose therefore that $\sigma^2 \neq 1$. It follows from (G.0) [which may be applied, since Θ is isomorphic to the S^*-group Λ] that there exist involutions α, β in Θ such that $\sigma = \alpha\beta$. Since π is an isomorphism, we may deduce from § 4, Lemma 2 that α^π and β^π are reflections in Λ whereas σ^π is not a reflection in Λ [nor is it 1]. We deduce from § 4, Lemma 3 that $a(\alpha^\pi) \cap a(\beta^\pi)$ is the one and only one fixed point of σ^σ; and it follows from (3) that $a(\alpha^\pi) = N(\alpha)$ and $a(\beta^\pi) = N(\beta)$. This makes it obvious that the one and only one fixed point of σ is $a(\alpha^\pi) \cap a(\beta^\pi) \leqq P(\alpha\beta) = P(\sigma)$. Since every point on $P(\sigma)$ is a fixed point of σ, it is clear now that $P(\sigma)$ is a point. Thus (L.1) is satisfied by Θ.

It follows from (E.2) that there exists to every point Q in (F, A) one and only one reflection ϱ in Λ with center Q. There exists one and only one involution ν in Θ such that $\nu^\pi = \varrho$, since π is an isomorphism. It follows from (3) that $P(\nu)$ is the center Q of ϱ. This shows the validity of (L.2); and completes the proof of (4).

Thus we have shown the existence of an L-group Θ of linear transformations of (F, A) such that $\Phi \otimes \{-1\} = \Theta \otimes \{-1\}$; and this completes the proof of Proposition 2.

REMARK 3: Suppose that Φ is an L-group of linear transformations. Then there exists a natural one to one correspondence between the totality of subgroups of index 2 of Θ and the totality of groups Φ of linear transformations which satisfy $\Theta \otimes \{-1\} = \Phi \otimes \{-1\}$. The totality of subgroups of index 2 of an S^*-group and in particular conditions for their non-existence will be discussed in § 8.

8. The group of squares and the Pythagorean case.

We begin by proving the following facts which may or may not be new.

LEMMA 1: *Suppose that G is an S^*-group.*
(a) *If a and b are conjugate involutions in G, then there exists an involution j in G such that $jaj = b$.*
(b) *Products of squares in G are squares in G.*

PROOF: Suppose that a and b are conjugate involutions in G. Then there exists an element g in G such that $b = g^{-1}ag$. There is nothing to prove if $a = b$ [let $j = a$]. Thus we assume that $a \neq b$. If g^* were a, then a and g would commute so that $a = b$ which is impossible. Hence $g^* \neq a$; and it follows from (G.1) and (G.3) that the involution $t = (g^*a)^* = J[J(g^*a)] = J(g^*) \cap J(a) = J(g) \cap J(a)$. Consequently $tg = j$ is an involution and $ta = at$. Hence

$$b = g^{-1}ag = (tj)^{-1}a(tj) = jtatj = jaj;$$

and this proves (a).

Consider next two elements g and h in G. We want to show that g^2h^2 is a square; and so we may assume without loss in generality that neither g^2 nor h^2 is 1. Applying (G.2) and (G.3) again we find

$$J(g) \cap J(h) = \begin{cases} J[J(g^*h^*)] & \text{if } g^* \neq h^* \\ J(s) & \text{if } g^* = h^* = s; \end{cases}$$

and hence there exists always at least one involution z in $J(g) \cap J(h)$. Then $g' = gz$ and $h' = zh$ are involutions. Then $u = g'zg'$ is an involution too. Since $h'zh' = (g'h')^{-1}u(g'h')$ we infer from (a) the existence of an involution j in G such that $h'zh' = juj$. Now $g^2h^2 = g'zg'z\, zh'zh' = g'zg'\, h'zh' = u\, juj = (uj)^2$; and this proves (b).

PROPOSITION 1: *If G' is the commutator subgroup of the S^*-group G, then G' is firstly exactly the totality of all squares of elements in G and G' is secondly exactly the totality of all commutators in G.*

PROOF: Denote by G^2 the totality of all elements of the form g^2 for g in G. Then it follows from Lemma 1, (b) that G^2 is a characteristic subgroup of G. Denote by W the set of all commutators $[x, y]$ for x, y in G. If g is an element in G, then there exist involutions a, b in G such that $g = ab$ [by (G.0)]. Hence $g^2 = abab = [a, b]$ so that $G^2 \leqq W \leqq G'$. On the other hand it is well known that G/G^2 is abelian, since all its elements, not 1, are involutions. Hence $G' \leqq G^2$ so that $G^2 = W = G'$, as we claimed.

PROPOSITION 2: *Suppose that G is an S^*-group. Then the line from* 1 *to the involution j [in the derived geometrical structure $D(G)$] carries a point which is on its canonical polar if, and only if, j belongs to G^2.*

PROOF: If the involution j is in G^2, then there exists an element g in G such that $j = g^2$. Clearly the point g is on the plane g. Suppose that the line from 1 to g is on the plane h. Then h is an involution, since 1 is on h; and gh is an involution so that

$$gh = hg^{-1},\ (jh)^2 = g^2hg^2h = hg^{-2}g^2h = 1,\ j \neq h.$$

Hence j is on every plane through the line from 1 to g so that 1, g, j are collinear, showing the sufficiency of our condition.

Assume conversely that the line from 1 to j carries a point p which is on its own canonical polar. The last statement is equivalent to the assertion that p^2 is an involution. There exist involutions a, b such that $p = ab$ [by (G.0)]. Since 1, j and p are collinear, we have $p^* = j$. But it follows from (G.2) and (G.3) that $j = p^* = J[J(p)] = J(a) \cap J(b)$. Next we note that $ap^2 = aabab = bab = baba\ a = p^{-2}a = p^2a$ since p^2 is an involution; and likewise we see that $bp^2 = p^2b$. Thus the involution p^2 belongs to $J(a) \cap J(b)$ too; and this shows $p^2 = j$. This completes the proof.

We have shown a little more than we intended to prove, namely the following fact which will be useful later on.

COROLLARY 1: *Suppose that G is an S^*-group, j an involution in G. Then the point p in $D(G)$ is both on its canonical polar and on the line from* 1 *to j if, and only if, $j = p^2$.*

We are now ready to characterize the special class of S^*-group which is the object of this section.

PROPOSITION 3: *The following properties of the S^*-group G are equivalent.*

(i) $G = G' = G^2$ [*so that every element in G is a commutator and a square*].

(ii) *Every involution in G is a square* [*or* $J \leqq G^2$].

(iii) *Any two commuting involutions in G are conjugate in G.*

(iv) *Any two involutions are conjugate in G.*

PROOF: We shall make use both of the geometrical properties of the derived geometrical structure $D(G)$ [which is a three dimensional projective space by § 7, Theorem 1] and of the characteristic group theoretical properties (G.1) to (G.4). We note that the equivalence of the various properties condensed in (i) is a consequence of Proposition 1.

It is clear that (i) implies (ii). Assume now the validity of (ii) and consider two different, but commuting involutions a and b in G. Then $ab = j$ is an involution in G; and we deduce from (ii) the existence of an element g in G such that $j = g^2$. It follows from Corollary 1 that g is a point on the line from 1 to j [in $D(G)$]. Since $ja = b$ and $jb = a$ are different involutions, the line from 1 to j is on the two planes a and b. Hence g is on these two planes so that ga and gb are involutions. Hence

$$g^{-1}bg = g\,g^{-2}\,bg = g(ab)bg = gag = gaga\,a = a.$$

Thus (iii) is a consequence of (ii).

Assume now the validity of (iii) and consider any two different involutions a and b. Then it follows from (G.3) that the involution $j = (ab)^* = J(a) \cap J(b)$. Since j commutes with a and with b, there exist [by (iii)] elements g and h in G such that $g^{-1}ag = j$ and $h^{-1}jh = b$. Hence $(gh)^{-1}a(gh) = b$ so that (iv) is a consequence of (iii).

Assume finally the validity of (iv); and consider an element $g \neq 1$ in G. It follows from (G.0) that there exist involutions a, b in G such that $g = ab$. We deduce from (iv) and Lemma 1, (a) the existence of an involution j such that $b = jaj$. Then $g = ab = a(jaj) = (aj)^2$ so that (i) is a consequence of (iv).

Corollary 2: *The S^*-group G satisfies $G = G^2$ if, and only if, every line through the point* 1 *[in $D(G)$] carries a point which is on its canonical polar.*

This is an immediate consequence of Corollary 1 and Proposition 3.

Lemma 2: *If Λ is an elliptic group of auto-projectivities of the plane Π, if Q is a point in Π and σ a transformation in Λ, then there exists a reflection in Λ which interchanges the points Q and $Q\sigma$.*

Proof: There exists by (E.2) one and only one reflection ϱ with center Q in Λ. Since Λ is an S^*-group [by § 4, Theorem], we infer from Lemma 1, (a) the existence of an involution ν in Λ such that $\sigma^{-1}\varrho\sigma = \nu\varrho\nu$. It is a consequence of § 4, Lemma 2 that ν too is a reflection. Using the definition of center of a reflection we find that

$$Q\nu = C(\varrho)\nu = C(\nu\varrho\nu) = C(\sigma^{-1}\varrho\sigma) = C(\varrho)\sigma = Q\sigma;$$

and the reflection ν in Λ consequently interchanges Q and $Q\sigma$.

Proposition 4: *The following properties of the elliptic group Λ of auto-projectivities of the plane Π are equivalent.*

(i) $\Lambda = \Lambda^2$.

(ii) *The group Λ is transitive on the points [lines] in Π.*

(iii) *There exists a reflection in Λ which interchanges the points Q and R in Π whenever there exists a reflection in Λ with center Q and axis through R.*

(iv) *If the group Φ of semi-linear transformations induces Λ isomorphically, then Φ is an L-group of linear transformations.*

(v) *If Λ is induced by the group Φ of all the motions of the elliptic plane (F, A, f), then*

(a) *$1 + t^2$ for t in F is a square, not 0, of an element in F [so that F is a formally real, Pythagorean field] and*

(b) *$f(x, x)$ is a square of an element, not 0, in F for every $x \neq 0$ [so that f is positive definite].*

NOTE: In order to obtain (*b*) it is necessary to make the normalization hypothesis § 2, (F.g) assuring the existence of an element e in A such that $f(e, e) = 1$. Without such a hypothesis one could only assert that $f(x, x)\, f(y, y)^{-1}$, for x and y not 0 in A, is a square in F.

PROOF: We note first that Λ is an S^*-group so that we may make use of all the results of this section. Assume first the validity of (i). If Q and R are different points in Π, then there exist by (E.2) uniquely determined reflections α and β in Λ with centers Q and R respectively. It is a consequence of Proposition 3 and hypothesis (i) that α and β are conjugate in Λ. Hence there exists a transformation σ in Λ such that $\sigma^{-1}\alpha\sigma = \beta$. It follows from the properties of the center of a reflection that

$$Q\sigma = C(\alpha)\sigma = C(\sigma^{-1}\alpha\sigma) = C(\beta) = R.$$

Hence (ii) is a consequence of (i); and it is a fairly immediate consequence of Lemma 2 that (ii) implies (iii).

Assume now the validity of (iii) and consider two different, but commuting involutions α and β in Λ. It is a consequence of § 4, Lemma 1 and 2 that α and β are reflections and that $C(\alpha)$ is on $a(\beta)$. We infer now from condition (iii) the existence of a reflection ϱ in Λ interchanging $C(\alpha)$ and $C(\beta)$. Hence $C(\varrho\beta\varrho) = C(\beta)\varrho = C(\alpha)$ so that the reflections α and $\varrho\beta\varrho$ have the same center. It follows from (E.2) that $\alpha = \varrho\beta\varrho$; and thus we have shown that Λ meets requirement (iv) of Proposition 3. But then $\Lambda = \Lambda^2$ by Proposition 3. Hence (i) is a consequence of (iii); and we have shown the equivalence of conditions (i) to (iii).

Assume now the validity of (i); and assume that Φ is a group of semi-linear transformations of (F, A) which induces Λ isomorphically — note that the linear manifold (F, A) represents the projective plane Π. We deduce from § 7, Proposition 2 the

existence of an L-group Ξ of linear transformations of (F, A) such that $\Phi \otimes \{-1\} = \Xi \otimes \{-1\}$. It follows from condition (i) that Φ does not possess subgroups of index 2; and this implies that every element in the group Φ of linear transformations has determinant $+1$. Hence $\Phi = \Xi$; and we have shown that (iv) is a consequence of (i).

Assume next that (i) is false. Then it follows [using Proposition 1] that Λ possesses a subgroup of index 2. We note that Λ is isomorphically induced by the group Φ of all the motions of the elliptic plane (F, A, f) [§ 7, Proposition 2 and § 7, Corollary 2]. Since Φ and Λ are isomorphic, Φ possesses a subgroup T of index 2. Denote by Θ the group of linear transformations consisting of all the τ in T and all the $-\nu$ for ν in Φ, but not in T. The two groups Φ and Θ both induce Λ isomorphically. Since every element in Φ has determinant $+1$, not every element in Θ has determinant $+1$. Hence Θ is not an L-group of linear transformations [§ 2, Corollary 5]. Thus (iv) is false if (i) is false so that (iv) implies (i).

Suppose next that Φ is the group of all the motions of the elliptic plane (F, A, f) and that Φ induces Λ. Assume the validity of the equivalent conditions (i) to (iv). Consider any $a \neq 0$ in A. There exists by (ii) a transformation ν in Φ which maps the point Fa upon the point Fe [where e is such that $f(e, e) = 1$]. Then there exists a number $t \neq 0$ in F such that $a\nu = te$. Since ν preserves f, we have

$$f(a, a) = f(a\nu, a\nu) = f(te, te) = t^2;$$

and this proves the validity of (v.b). One proves readily the existence of an element d in A such that $f(d, d) = 1$, $f(e, d) = f(d, e) = 0$. If x is any number in F, then

$$1 + x^2 = f(e, e) + f(xd, xd) = f(e + xd, e + xd);$$

and (v.a) is seen to be a consequence of (v.b).

Assume conversely the validity of (v). If Q and R are different points, then there exist by (v.b) elements q and r such that $Q = Fq$, $R = Fr$ and $1 = f(q, q) = f(r. r)$. Since Φ is an L-group of linear transformations [§ 3, Theorem], there exists an involution ν in Φ which interchanges q and r [by Property (L.3) derived during the proof of § 3, Theorem]; and this involution ν interchanges the points Q and R. Thus Λ has property (ii); and this completes the proof.

Remark 1: Condition (iv) may be restated as follows.

(iv*) *There exists one and essentially only one group of semi-linear transformations which induces Λ isomorphically.*

Thus the validity of a Uniqueness Theorem is characteristic for this class of groups [see § 7, Remark 2].

REMARK 2: The *S*-groups* G satisfying $G = G^2$ may be termed *Pythagorean* because of the characteristic property (v) of Proposition 4. The question arises which S^*-groups may be imbedded into Pythagorean S^*-groups. In this respect one proves without much difficulty the following result.

The group Φ of all the motions of the elliptic plane (F, A, f) may be imbedded into a Pythagorean S^*-group if, and only if, there exists an algebraical order of the field F with the property:

(PD) $0 < f(x, x)$ *for every* $x \neq 0$ *in* A

Naturally this presupposes that f is subjected to the normalization $f(e, e) = 1$ for some e.

It is interesting to note that the above result ceases to be true once we omit the condition (PD), as may be seen from the following *example*. F is the field of all rational numbers, A the group of all triplets (x_0, x_1, x_2) with rational coefficients x_i and

$$f(x, y) = x_0y_0 + 3x_1y_1 - 2x_2y_2.$$

It is not difficult to verify that $f(x, x) \neq 0$ for $x \neq 0$. Thus (F, A, f) is an elliptic plane. But it is clear that f does not satisfy (PD). Thus the group of motions of (F, A, f) cannot be imbedded into a Pythagorean group in spite of the fact that F admits of one and only one algebraical order.

This example is interesting for another reason. The points Fa such that $f(x, x) < 0$ form a hyperbolic plane; and the group of motions of the elliptic plane (F, A, f) is at the same time the group of motions of the hyperbolic plane just defined.

REMARK 3: Suppose that P is a Pythagorean field [in the sense of Proposition 4, (v.a)]. Then one may show that the field F of all formal power series in one indeterminate with coefficients from P is likewise Pythagorean. We form a linear manifold (F, A) of rank 3 over F and consider a positive definite, symmetrical bilinear form $f(x, y)$ [in the sense of Proposition 4, (v.b)]. The group Φ of all the motions of the elliptic plane (F, A, f) is known not to be simple [Dieudonné [1], p. 35]; but it follows from Proposition 4 that Φ is an S^*-group which satisfies $\Phi = \Phi^2$. We see therefore that the equivalent conditions (i) to (iv) of Proposition 3 do not imply simplicity of the S^*-group G, though simplicity of G certainly implies $G = G^2$.

REMARK 4: Reidemeister-Podehl [1, § 11] have shown that the property (v) is a consequence of the possibility of "bisecting right angles" which is essentially the same as our condition (iii).

BIBLIOGRAPHY.

R. Baer,

[1] Polarities in finite projective planes. Bull. Amer. Math. Soc., vol. 52 (1946), pp. 77—93.

G. Birkhoff—J. von Neumann,

[1] The logic of quantum mechanics. Ann. of Math. vol. 37 (1936), pp. 823—843.

J. Dieudonné,

[1] Sur les groupes classiques. Actualités scientifiques et industrielles 1040; Paris 1948.

K. Menger,

[1] The projective space. Duke Math. Journal, vol. 17 (1950), pp. 1—14.

E. Podehl—K. Reidemeister,

[1] Eine Begründung der ebenen elliptischen Geometrie. Hamburger Abhdlg. vol. 10 (1934), pp. 231—255.

A. Schmidt,

[1] Über die Bewegungsgruppe der ebenen elliptischen Geometrie. Journal für die r.u.a. Math., vol. 186 (1949), pp. 230—240.

(Oblatum 29-1-51).