GEOMETRIES OF MATRICES. I. GENERALIZATIONS OF VON STAUDT'S THEOREM

BY

LOO-KENG HUA

It was first shown in the author's recent investigations on the theory of automorphic functions of a matrix-variable that there are three types of geometry playing important roles. Besides their applications, the author obtained a great many results which seem to be interesting in themselves.

The main object of the paper is to generalize a theorem due to von Staudt, which is known as the fundamental theorem of the geometry in the complex domain. The statement of the theorem is:

Every topological transformation of the complex plane into itself, which leaves the relation of harmonic separation invariant, is either a collineation or an anticollineation.

Since the fields and groups may be varied, several generalizations of von Staudt's theorem will be given. The proofs of the theorems have interesting corollaries.

The paper contains also some fundamental results which will be useful in succeeding papers.

The interest of the paper seems to be not only geometric but also algebraic, for example we shall establish the following purely algebraic theorem:

Let \mathfrak{M} be the module formed by n-rowed symmetric matrices over the complex field. Let Γ be a continuous (additive) automorphism of \mathfrak{M} leaving the rank unaltered and $\Gamma(iX) = i\Gamma(X)$. Then Γ is an inner automorphism of \mathfrak{M} , that is, we have a nonsingular matrix T such that

$$\Gamma(X) = TXT'.$$

The author makes the paper self-contained in the sense that no knowledge of the author's contributions to the theory of automorphic functions is assumed.

I. GEOMETRY OF SYMMETRIC MATRICES

Let Φ be any field. In I, II, and III, capital Latin letters denote $n \times n$ matrices unless the contrary is stated. But on the contrary, we use $M^{(n,m)}$ to denote an $n \times m$ matrix, and $M^{(n)} = M^{(n,n)}$. I and 0 denote the identity and zero matrices respectively.

Throughout I, we use

Presented to the Society, April 28, 1945; received by the editors November 20, 1944.

which are 2n-rowed matrices.

1. Definitions. We make the following definitions.

A pair of matrices (Z_1, Z_2) is said to be symmetric if

$$(Z_1, Z_2)\mathfrak{F}(Z_1, Z_2)' = 0$$

that is, if $Z_1Z_2' = Z_2Z_1'$. The pair is said to be nonsingular if (Z_1, Z_2) is of rank n.

A $2n \times 2n$ matrix \mathfrak{T} is said to be symplectic if

$$\mathfrak{T}\mathfrak{F}\mathfrak{T}'=\mathfrak{F}.$$

Explicitly, let

$$\mathfrak{T} = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

then we have

$$AB' = BA',$$
 $CD' = DC',$ $AD' - BC' = I$

Further, it may be easily verified that

$$\mathfrak{T}^{-1} = \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix}$$

is also symplectic.

We define

$$(W_1, W_2) = Q(Z_1, Z_2)\mathfrak{T}$$

to be a symplectic transformation, where Q is nonsingular and \mathfrak{T} is symplectic. Since

$$(W_1, W_2)\mathfrak{F}(W_1, W_2)' = Q(Z_1, Z_2)\mathfrak{T}\mathfrak{F}\mathfrak{T}'(Z_1, Z_2)'Q',$$

a symplectic transformation carries symmetric (nonsingular) pairs into symmetric (nonsingular) pairs.

We identify two nonsingular symmetric pairs of matrices (Z_1, Z_2) and (W_1, W_2) by means of the relation

$$(Z_1, Z_2) = Q(W_1, W_2).$$

It is called a point of the space. The space so defined is unaltered under symplectic transformations, which may be considered as the motions of the space.

If Z_1 and W_1 are both nonsingular and if $(W_1, W_2) = Q(Z_1, Z_2) \mathfrak{T}$ let

$$W = -W_1^{-1}W_2, \qquad Z = -Z_1^{-1}Z_2,$$

then W and Z are both symmetric and

$$Z = (AW + B)(CW + D)^{-1}.$$

Thus a symmetric pair of matrices may be considered as homogeneous coordinates of a symmetric matrix. The terminology "geometry of symmetric matrices" is thus justified.

2. Equivalence of points.

THEOREM 1. Any two nonsingular symmetric pairs of matrices are equivalent. Or what is the same thing: every nonsingular symmetric pair is equivalent to (I, 0).

Proof. Let (Z_1, Z_2) be a nonsingular symmetric pair. (1) If Z_1 is nonsingular, we have

$$(Z_1, Z_2) = Z_1(I, Z_1^{-1}Z_2) = Z_1(I, 0) \begin{pmatrix} I & S \\ 0 & I \end{pmatrix},$$

where $S = Z_1^{-1}Z_2$ is symmetric, and then

is symplectic.

(2) Suppose Z_1 to be singular. We have nonsingular matrices P and Q such that

 $\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}$

$$W_1 = PZ_1Q = \begin{pmatrix} I^{(r)} & 0^{(r,n-r)} \\ 0^{(n-r,r)} & 0^{(n-r)} \end{pmatrix},$$

and

$$(W_1, W_2) = P(Z_1, Z_2) \begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix},$$

and

$$W_2 = PZ_2Q'^{-1} = \binom{s^{(r)} \quad m^{(r,n-r)}}{q^{(n-r,r)} \quad t^{(n-r)}}.$$

Since

is symplectic, (W_1, W_2) is nonsingular and symmetric. Consequently s is symmetric and q is a zero matrix.

 $\begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix}$

Let

$$(U_1, U_2) = (W_1, W_2) \begin{pmatrix} I & -S \\ 0 & I \end{pmatrix},$$

where

$$S = \begin{pmatrix} s^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}.$$

Then

$$W_1, W_2) = F(Z_1, Z_2)$$

$$U_1 = W_1, \qquad U_2 = -W_1S + W_2 = \begin{pmatrix} 0 & m \\ 0 & t \end{pmatrix}.$$

Since (U_1, U_2) is nonsingular, $t^{(n-r)}$ is nonsingular. Let

$$(V_1, V_2) = (U_1, U_2) \begin{pmatrix} I & 0 \\ I & I \end{pmatrix};$$

then

444

$$V_1 = U_1 + U_2 = \begin{pmatrix} I^{(r)} & m \\ 0 & t \end{pmatrix},$$

which is nonsingular. By (1), we have the theorem.

3. Equivalence of point-pairs.

DEFINITION. Let (Z_1, Z_2) and (W_1, W_2) be two nonsingular symmetric pairs of matrices. We define the rank of

$$(Z_1, Z_2)\mathfrak{F}(W_1, W_2)' = Z_1W_2' - Z_2W_1'$$

to be the *arithmetic distance* between the two points represented. Evidently, the notion is independent of the choice of representation. Further, it is invariant under symplectic transformations. In fact, let

$$(Z_1^*, Z_2^*) = Q(Z_1, Z_2)\mathfrak{T}, \qquad (W_1^*, W_2^*) = R(W_1, W_2)\mathfrak{T},$$

then

$$(Z_1^*, Z_2^*)\mathfrak{F}(W_1^*, W_2^*)' = Q(Z_1, Z_2)\mathfrak{TFT}'(W_1, W_2)'R' = Q(Z_1, Z_2)\mathfrak{F}(W_1, W_2)'R'.$$

In nonhomogeneous coordinates, the arithmetic distance between two symmetric matrices W, Z is equal to the rank of W-Z.

THEOREM 2. Two point-pairs are equivalent if and only if they have the same arithmetic distance. What is the same thing: every point-pair with arithmetic distance r is equivalent to

where

$$I_r = \begin{pmatrix} I^{(r)} & 0\\ 0 & 0 \end{pmatrix}.$$

 $(I, 0), (I, I_{*})$

Proof. By Theorem 1, we may assume that the point-pairs are of the form

$$(I, 0), (Z_1, Z_2).$$

The arithmetic distance being r, it follows that Z_2 is of rank r. We have two nonsingular matrices P and Q such that

$$QZ_2P = \begin{pmatrix} I^{(r)} & 0\\ 0 & 0 \end{pmatrix} = I_r.$$

Then

$$Q(Z_1, Z_2) \begin{pmatrix} P'^{-1} & 0 \\ 0 & P \end{pmatrix} = (T, I_r)$$

and

$$Q(I, 0) \begin{pmatrix} P'^{-1} & 0 \\ 0 & P \end{pmatrix} = QP'^{-1}(I, 0).$$

Since (T, I_r) is a nonsingular symmetric pair, we have, consequently,

$$T = \begin{pmatrix} s^{(r)} & t \\ 0 & p^{(n-r)} \end{pmatrix},$$

where s is symmetric and p is nonsingular. Then

$$\binom{I^{(r)} - tp^{-1}}{0}(T, I_r) = \binom{s^{(r)} \ 0}{0} I^{(n-r)}, I_r.$$

Further,

$$\begin{pmatrix} \begin{pmatrix} s^{(r)} & 0\\ 0 & I^{(n-r)} \end{pmatrix}, I_r \end{pmatrix} \begin{pmatrix} I & 0\\ \begin{pmatrix} I-s & 0\\ 0 & 0 \end{pmatrix} I \end{pmatrix} = (I, I_r)$$

and

$$(I, 0) \begin{pmatrix} I & 0 \\ (I - s & 0 \\ 0 & 0 \end{pmatrix} I = (I, 0).$$

Since

$$\begin{pmatrix} I & 0 \\ \begin{pmatrix} I - s & 0 \\ 0 & 0 \end{pmatrix} I \end{pmatrix}$$

is symplectic, we have the result.

l

DEFINITION. The points (X_1, X_2) with singular X_1 are called *points at infinity* (or symmetric matrices at infinity). Finite points are those with non-singular X_1 .

LEMMA. Any finite number of points may be carried simultaneously into finite points by a symplectic transformation, if Φ is the field of complex numbers.

Proof. (1) Given any symmetric pair of matrices (T_1, T_2) , we have a symplectic matrix

$$\binom{P_1 \ P_2}{T_1 \ T_2}.$$

In fact, by Theorem 2, we have a symplectic \mathfrak{T} such that

$$(T_1, T_2) = Q(-I, 0)\mathfrak{T}.$$

1945]

Let

 $(P_1, P_2) = Q'^{-1}(0, I)\mathfrak{T}.$

Then

$$\begin{pmatrix} P_1 & P_2 \\ T_1 & T_2 \end{pmatrix} = \begin{pmatrix} Q'^{-1} & 0 \\ 0 & Q \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \mathfrak{T}$$

which is evidently symplectic.

(2) For a fixed point (X_1, X_2) , the manifold

$$\det ((X_1, X_2)\mathfrak{F}(Z_1, Z_2)') = 0$$

is of dimension n(n+1)-2. Let

$$(A_1, A_2), \cdots, (L_1, L_2)$$

be p given points. Then we have p manifolds

det
$$((A_1, A_2)\mathfrak{F}(Z_1, Z_2)') = 0, \cdots, det ((L_1, L_2)\mathfrak{F}(Z_1, Z_2)') = 0.$$

In the space, there is a point (T_1, T_2) which is not on any one of the manifolds. The transformation

$$(Y_1, Y_2) = Q(X_1, X_2) \begin{pmatrix} P_1 & P_2 \\ T_1 & T_2 \end{pmatrix}^{-1} = Q(X_1, X_2) \begin{pmatrix} T_2' & -P_2' \\ -T_1' & P_1' \end{pmatrix}$$

carries evidently the p points into finite points simultaneously.

4. Equivalence of triples of points.

DEFINITION 1. A subspace is said to be *normal* if it is equivalent to the subspace formed by symmetric matrices (in nonhomogeneous coordinates) of the form

$$\binom{Z_0^{(r)} \ 0}{0 \ 0^{(n-r)}}.$$

The least possible r is defined to be the rank of the subspace.

DEFINITION 2. A triple of points is said to be of degeneracy d=n-r if it belongs to a normal subspace of rank r.

Evidently degeneracy is invariant under symplectic transformations.

THEOREM 3. In the complex field, two triples of points are equivalent if and only if they have the same degeneracy and the arithmetic distances between any two corresponding pairs of points are equal.

Proof. Evidently, if two triples are equivalent, they have the same degeneracy and the arithmetic distances between any two corresponding pairs of points are equal.

We prove the converse in six steps.

(1) Every triple with arithmetic distances n, n, r is equivalent to

446

GEOMETRIES OF MATRICES. I

0, I,
$$\begin{pmatrix} -I^{(r)} & 0\\ 0 & 0 \end{pmatrix}$$
 (in nonhomogeneous coordinates).

(Notice that now the degeneracy is 0.) We use r(A, B) to denote the arithmetic distance between A and B. Let A, B, C be the three points of the triple. Then

$$r(A, B) = r(A, C) = n.$$

By Theorem 2, we may write in homogeneous coordinates

$$A = (I, 0), \quad B = (0, I), \quad C = (Z_1, Z_2).$$

Since r(A, C) = n and Z_2 is nonsingular, we may write C as

where S is a symmetric matrix of rank r. We have a nonsingular matrix Γ such that

$$\Gamma S \Gamma' = I_r = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix},$$

then

$$\Gamma\begin{pmatrix}(I, 0)\\(0, I)\\(S, I)\end{pmatrix}\begin{pmatrix}\Gamma' & 0\\0 & \Gamma^{-1}\end{pmatrix} = \begin{pmatrix}\Gamma\Gamma'(I, 0)\\(0; I)\\(I_r, I)\end{pmatrix}.$$

Thus the triple is equivalent to

 $(I, 0), (0, I), (I_r, I).$

Since (in the nonhomogeneous coordinate-system)

0, $I_{r} - I_{r}$

is a triple with distances n, n, r, we have the theorem.

(2) Every triple of points with arithmetic distances n, s, t is equivalent to

$$0, I, \begin{pmatrix} -I^{(p)} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & I^{(q)} \end{pmatrix},$$

where p+q=s, n-q=t. (Obviously, $s+t \ge n$.)

In fact, we may assume that

$$A = (I, 0), \quad B = (I, I), \quad C = (Z_1, Z_2).$$

We may determine two nonsingular matrices U, V such that

$$UZ_2V = \begin{pmatrix} I^{(r)} & 0\\ 0 & 0 \end{pmatrix},$$

1945]

where r is the rank of Z_2 . If we set

$$G = \begin{pmatrix} V'^{-1} & 0 \\ V - V'^{-1} & V \end{pmatrix}$$

the relations

$$U(I, 0)G = UV'^{-1}(I, 0),$$

$$U(I, I)G = UV(I, I),$$

$$U(Z_1, Z_2)G = \left(P, \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}\right)$$

imply that we may assume that

$$Z_1 = P, \qquad Z_2 = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}$$

Owing to the symmetry, we have

$$P = \begin{pmatrix} S^{(r)} & W \\ 0 & T \end{pmatrix},$$

where S is symmetric and T is nonsingular. Further, since

$$\binom{I - WT^{-1}}{0 T^{-1}} \binom{\binom{S^{(r)} W}{0 T}}{\binom{I^{(r)} 0}{0 0}} = \binom{\binom{S^{(r)} 0}{0 I}}{\binom{I^{(r)} 0}{0 0}}, \binom{I^{(r)} 0}{\binom{0}{0 0}},$$

we may assume that

$$Z_1 = \begin{pmatrix} S^{(r)} & 0 \\ 0 & I \end{pmatrix}, \qquad Z_2 = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

In the normal subspace of rank r, the points $(I^{(r)}, 0^{(r)})$, $(I^{(r)}, I^{(r)})$, $(S^{(r)}, I^{(r)})$ are, by (1), equivalent to

$$(I^{(r)}, 0^{(r)}), (I^{(r)}, I^{(r)}), (I^{(r)}, \begin{pmatrix} -I^{(p)} & 0 \\ 0 & 0^{(r-p)} \end{pmatrix}).$$

Thus, we have, in nonhomogeneous coordinates,

$$\binom{I^{(r)} \ 0}{0 \ 0^{(n-r)}}, \qquad \binom{0^{(r)} \ 0}{0 \ I^{(n-r)}}, \qquad \binom{-I^{(p)} \ 0 \ 0}{0 \ 0^{(r-p)} \ 0}, \qquad \binom{-I^{(p)} \ 0 \ 0}{0 \ 0^{(r-p)} \ 0}.$$

The transformation

$$\binom{I^{(r)} \ 0}{0 \ iI^{(n-r)}} \left(Z - \binom{0^{(r)} \ 0}{0 \ I^{(n-r)}} \right) \binom{I^{(r)} \ 0}{0 \ iI^{(n-r)}} = W$$

carries the three points to the required form.

[May

(3) Now we are going to prove that any three points are equivalent to

$$4 = 0, \qquad B = b_1 + \cdots + b_{\lambda}, \qquad C = c_1 + \cdots + c_{\lambda}(1),$$

where b_r and c_r are unit matrices of degree r_r multiplied with a factor 1, 0, or -1. (1) and (2) are special cases of this. We shall consider another special case with

$$A = 0, \qquad B = \begin{pmatrix} 0 & M \\ M' & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & N \\ N' & 0 \end{pmatrix},$$

where

$$M = \begin{pmatrix} 0 \cdots 0 \\ I^{(m)} \end{pmatrix}, \qquad N = \begin{pmatrix} I^{(m)} \\ 0 \cdots 0 \end{pmatrix}, \qquad n = 2m + 1.$$

They form a triple with distances 2m, 2m, 2m.

Now we are going to establish that there exists a symmetric matrix S such that the transformation

$$W = Z(SZ + I)^{-1}$$

will carry the three points to

$$A = 0, \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & B_1^{(n-1)} \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 0 \\ 0 & C_1^{(n-1)} \end{pmatrix},$$

where B_1 is nonsingular. In fact S is given by

and so on. The general form may be obtained easily. Applying the results obtained in (2) to

$$0^{(n-1)}, B_1^{(n-1)}, C_1^{(n-1)},$$

we have the conclusion.

(4) Let B, C be a nonsingular pair of symmetric matrices (in the ordinary sense), that is, we have λ and μ such that

$$\det (\lambda B + \mu C) \neq 0.$$

Suppose C is nonsingular; the conclusion announced in (3) is true by (2). Otherwise $(\lambda \neq 0)$ we have Γ such that

(1) + and \sum' denote direct sums.

1945]

L. K. HUA

$$\Gamma'(\lambda B + \mu C)\Gamma = I,$$

$$\Gamma'C\Gamma = \begin{pmatrix} C_1^{(r)} & 0\\ 0 & 0 \end{pmatrix}, \qquad C_1^{(r)} \text{ nonsingular.}$$

Then

$$\lambda \Gamma' B \Gamma = \begin{pmatrix} I^{(r)} - \mu C_1^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}$$

Applying the results of (2) to

$$0, \quad \frac{1}{\lambda} (I^{(r)} - \mu C_1^{(r)}), \quad C_1^{(r)},$$

and

 $0, \quad \frac{1}{\lambda} I^{(n-r)}, \quad 0,$

we have the result announced in (3).

l

we have a nonsingular matrix Γ such that

$$\Gamma B \Gamma' = b_1 + \cdots + b_{\lambda}$$

and

$$\Gamma C \Gamma' = c_1 \dotplus \cdots \dotplus c_{\lambda},$$

 (b_{r}, c_{r})

where

is either the pair discussed in (4) or the pair discussed in (3), hence the results in (3).

(6) By a rearrangement and some evident modifications, for a triple of points with degeneracy t, we have

$$A = 0^{(p)} + 0^{(q)} + 0^{(r)} + 0^{(s)} + 0^{(s)},$$

$$B = I^{(p)} + 0^{(q)} + I^{(r)} + I^{(s)} + 0^{(t)},$$

$$C = -I^{(p)} + I^{(q)} + 0^{(r)} + I^{(s)} + 0^{(t)},$$

which is the only possible form. The arithmetic distances between two points are given by 10 M . . .

$$a = r(B, C) = p + q + r,$$

$$b = r(C, A) = p + q + s,$$

$$c = r(A, B) = p + r + s.$$

Thus, for given t, a, b, c, if the equations are soluble, the solution is unique. We have therefore the theorem.

The conditions for solubility are

(1)
$$n-t \ge a, b, c,$$
$$a+b+c \ge 2(n-t).$$

In terms of a "triangle" we have the following theorem.

THEOREM 4. A triangle of degeneracy t with sides a, b, c exists if and only if (1) holds. If it exists, it is unique apart from equivalence.

Incidentally, we have

 $a+b \geq 2(n-t)-c \geq c;$

equality holds if and only if c = a + b = n - t.

The "triangle-relation"

 $a+b \ge c$, $b+c \ge a$, $c+a \ge b$

does not guarantee the existence of triangles with a given degeneracy, for example, n=2, t=0, a=b=c=1. But we have the following theorem.

THEOREM 5. Given the lengths of three sides a, b, c ($\leq n$), where the sum of every two is greater than the third one, there are λ non-equivalent triangles, where

$$\lambda = \begin{cases} [(a+b+c)/2] - \max(a, b, c) + 1, & \text{for } n \ge [(a+b+c)/2]^{(2)}, \\ n - \max(a, b, c) + 1, & \text{for } n < [(a+b+c)/2]. \end{cases}$$

Proof. From $a+b \ge c$, $b+c \ge a$, $c+a \ge b$, we have

 $a + b + c \ge 2 \max(a, b, c).$

There always exists a t such that

$$a+b+c \geq 2(n-t) \geq 2 \max (a, b, c).$$

Then

$$\max(0, n - [(a + b + c)/2]) \leq t \leq n - \max(a, b, c).$$

Thus, the number of t's is equal to

$$n - \max(a, b, c) - \max(0, n - [(a + b + c)/2]) + 1$$

= min (n, [(a + b + c)/2]) - max (a, b, c) + 1.

COROLLARY 1. If one of the sides is of length n, the triangle is unique.

COROLLARY 2. If the sum of two sides is equal to the third, then the triangle is unique.

(2) [x] denotes the integral part of x.

5. Equivalence of quadruples of points.

DEFINITION. Let Z_1 , Z_2 , Z_3 , Z_4 be four points in the nonhomogeneous coordinate-system. The matrix

$$(Z_1 - Z_3)(Z_1 - Z_4)^{-1}(Z_2 - Z_4)(Z_2 - Z_3)^{-1}$$

is defined to be the cross-ratio-matrix of the four points, and it is denoted by

 $(Z_1, Z_2; Z_3, Z_4).$

It is defined only when $Z_1 - Z_4$ and $Z_2 - Z_3$ are nonsingular.

In the homogeneous coordinate-system, we let P_1 , P_2 , P_3 , P_4 be four points with coordinates

$$(X_1, Y_1), (X_2, Y_2), (X_3, Y_3), (X_4, Y_4).$$

In terms of

$$\langle P_i, P_j \rangle = (X_j, Y_j) \mathfrak{F}(X_i, Y_i)',$$

the cross-ratio-matrix is defined by

$$(P_1, P_2; P_3, P_4) = \langle P_1, P_3 \rangle \langle P_1, P_4 \rangle^{-1} \langle P_2, P_4 \rangle \langle P_2, P_3 \rangle^{-1},$$

provided that it is not meaningless.

Let P_i^* be the point with coordinates

$$(X_i^*, Y_i^*) = Q_i(X_i, Y_i)\mathfrak{T},$$

where \mathbf{T} is symplectic; then

$$\langle P_i^*, P_j^* \rangle = (X_j^*, Y_j^*) \mathfrak{F}(X_i^*, Y_i^*)'$$

= $Q_j(X_j, Y_j) \mathfrak{F}(X_i, Y_i)' Q_i' = Q_j \langle P_i, P_j \rangle Q_i'.$

Therefore

$$(P_1^*, P_2^*; P_3^*, P_4^*) = \langle P_1^*, P_3^* \rangle \langle P_1^*, P_4^* \rangle^{-1} \langle P_2^*, P_4^* \rangle \langle P_2^*, P_3^* \rangle^{-1}$$

= $Q_3 \langle P_1, P_3 \rangle Q_1' Q_1'^{-1} \langle P_1, P_4 \rangle Q_4 Q_4^{-1} \langle P_2, P_4 \rangle Q_2' Q_2'^{-1} \langle P_2, P_3 \rangle^{-1} Q_3^{-1}$
= $Q_3 (P_1, P_2; P_3, P_4) Q_3^{-1}$,

and we now state the following theorem.

THEOREM 6. In an algebraically closed field, two quadruples of points, no two of the points having arithmetic distance less than n, are equivalent if and only if their cross-ratio-matrices are equivalent.

In order to prove Theorem 6, we need to establish the following theorem.

THEOREM 7. In the algebraically closed field, any quadruple of points, no two of which have arithmetic distance less than n, is equivalent to

$$0, \qquad \infty, \qquad \sum_{1 \leq i \leq r}' a_i, \qquad \sum_{1 \leq i \leq r}' b_i,$$

where

$$a_{i} = \begin{pmatrix} 0 \cdots 0 & 1 \\ 0 \cdots 1 & 0 \\ \cdots & \ddots & \vdots \\ 1 \cdots & 0 & 0 \end{pmatrix}, \qquad b_{i} = \begin{pmatrix} 0 & 0 \cdots 0 & \lambda_{i} \\ 0 & 0 \cdots & \lambda_{i} & 1 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{i} & 1 \cdots & 0 & 0 \end{pmatrix}, \qquad \lambda_{i} \neq 0 \quad or \quad 1.$$

Proof. In homogeneous coordinates, we may write the four points as

 $(0, I), (I, 0), (Z_1, Z_2), (W_1, W_2).$

Since no two of the arithmetic distances are less than n, Z_1, Z_2, W_1, W_2 are all nonsingular. We may write them in the nonhomogeneous coordinates as

$$0, \quad \infty, \quad S_1, \quad S_2.$$

We have a nonsingular matrix T such that

$$TS_1T' = \sum' a_i, \qquad TS_2T' = \sum' b_i.$$

The theorem follows.

The proof of Theorem 6 is now evident.

REMARK. The equivalence of quadruples in any field seems to be more difficult. The condition in Theorem 6 is insufficient for the real case. (A signature system is required.)

DEFINITION. We define a quadruple of points satisfying

$$(P_1, P_2; P_3, P_4) = -I$$

to be a harmonic range.

Evidently a harmonic range is invariant under a symplectic transformation.

6. Von Staudt's theorem in the complex number field. Now we let Φ be the field formed by complex numbers.

We use \overline{Z} to denote the conjugate complex matrix of Z. The transformation

$$(W_1, W_2) = Q(\overline{Z}_1, \overline{Z}_2)\mathfrak{T}$$

carrying a symmetric pair (W_1, W_2) into a symmetric pair (Z_1, Z_2) is called *anti-symplectic* if Q is nonsingular and \mathfrak{T} symplectic.

THEOREM 8. A transformation satisfying the following conditions:

(1) one-to-one and continuous,

(2) carrying symmetric matrices into symmetric matrices,

- (3) keeping arithmetic distance invariant,
- (4) keeping the harmonic relation invariant,

is either a symplectic or an anti-symplectic transformation.

Proof. Let Γ be the transformation considered. Taking three points A, B,

1945]

C (symmetric matrices), no two of which have arithmetic distance less than n, let A_1 , B_1 , C_1 be their images. By (3), the arithmetic distance between any two of A_1 , B_1 , C_1 is n. Let \mathfrak{T}_1 and \mathfrak{T}_2 be two symplectic transformations carry-

ing respectively A, B, C and A₁, B₁, C₁ into 0, I, ∞ , in accordance with

Theorem 3. Then, without loss of generality, we may assume that

$$0 = \Gamma(0), \qquad I = \Gamma(I), \qquad \infty = \Gamma(\infty).$$

Since

$$Z, Z_1, (Z+Z_1)/2, \infty$$

form a harmonic range, we have

$$\Gamma(Z) + \Gamma(Z_1) = \Gamma(Z + Z_1)$$

Consequently,

$$\Gamma(rZ) = r\Gamma(Z)$$

for all rational r. By continuity, this holds for all real r.

Now we introduce the following notations:

$$E_{ii} = (p_{si}), \qquad p_{si} = \begin{cases} 1 & \text{if } s = t = i, \\ 0 & \text{otherwise} \end{cases}$$

and

$$E_{ij} = (q_{*i}), \qquad q_{*i} = \begin{cases} 1 & \text{if } s = i, t = j \text{ or } s = j, t = i, \\ 0 & \text{otherwise.} \end{cases}$$

Let

$$\Gamma(E_{ii}) = M_{i}.$$

Since M_i is of rank 1 and symmetric, we have

$$M_i = (\lambda_{i1}, \cdots, \lambda_{in})'(\lambda_{i1}, \cdots, \lambda_{in}).$$

Let

$$\Lambda = (\lambda_{ij}).$$

Then

$$I = \Gamma(I) = \sum_{i=1}^{n} \Gamma(E_{ii}) = \sum_{i=1}^{n} M_i$$

= $\sum_{i=1}^{n} (\lambda_{i1}, \dots, \lambda_{in})'(\lambda_{i1}, \dots, \lambda_{in})$
= $\sum_{i=1}^{n} (\lambda_{ij}\lambda_{ik}) = \left(\sum_{i=1}^{n} \lambda_{ij}\lambda_{ik}\right)$
= $\Lambda'\Lambda$.

That is, Λ is an orthogonal matrix

$$(\lambda_{i1}, \cdots, \lambda_{in})\Lambda' = (\delta_{i1}, \cdots, \delta_{in}),$$

where δ_{ij} is Kronecker's delta. Thus

$$\Lambda\Gamma(E_{ii})\Lambda'=E_{ii}$$

Let

$$\Delta(Z) = \Lambda \Gamma(Z) \Lambda',$$

then Δ has the same property as Γ , that is,

$$\Delta(Z + Z_1) = \Delta(Z) + \Delta(Z_1),$$

$$0 = \Delta(0), \quad I = \Delta(I), \quad \infty = \Delta(\infty)$$

and

$$E_{ii} = \Delta(E_{ii}).$$

Let

$$\Delta(E_{ij}) = M = (m_{i}), \qquad i \neq j,$$

M is of rank 2. Since

 $E_{ij} + \lambda E_{ii} + E_{jj}/\lambda$

is of rank 1, owing to the invariance of arithmetic distance, the matrix

(1) $M + \lambda E_{ii} + E_{jj}/\lambda$

is also of rank 1 for all λ . We are going to prove that $M = \pm E_{ij}$. In fact, we may assume that i=1, j=2. The two-rowed minor of (1)

$$\begin{vmatrix} m_{11} + \lambda & m_{12} \\ m_{12} & m_{22} + 1/\lambda \end{vmatrix} = 0$$

for any λ , that is

$$m_{11}m_{22} - m_{12}^2 + m_{11}/\lambda + m_{22}\lambda + 1 = 0,$$

that is

$$m_{11} = m_{22} = 0, \qquad m_{12} = \pm 1.$$

Further

$$\begin{vmatrix} m_{11} + \lambda & m_{1t} \\ m_{1t} & m_{tt} \end{vmatrix} = 0 \qquad t \geq 3,$$

for all λ , then $m_{tt} = 0$, $m_{1t} = 0$ for all $t \ge 3$. Finally

$$\left|\begin{array}{cc}0&m_{st}\\m_{st}&0\end{array}\right|=0\quad\text{if}\quad(s,\,t)\neq(1,\,2),$$

then $m_{st} = 0$ for $(s, t) \neq (1, 2)$. Hence, we have

Thus

 $\Delta(E_{ij}) = \pm E_{ij}.$ Let

$$D = [\epsilon_1, \cdots, \epsilon_n], \qquad \epsilon_r = \pm 1.$$

Then

 $D\Delta(E_{ij})D' = \pm \epsilon_i\epsilon_j E_{ij}.$

 $M = \pm E_{12}.$

Thus we may choose ϵ properly so that

$$D\Delta(E_{1i})D' = E_{1i}.$$

Let $D\Delta D' = \Pi$. Then Π has all properties of Δ and further

$$\Pi(E_{1i}) = E_{1i}.$$

Now we consider E_{ij} . Without loss of generality we take (i, j) = (2, 3). Then, if $\Pi(E_{23}) = -E_{23}$, we have

$$\Pi(E_{11}+E_{33}+E_{12}+E_{13}+E_{23})=E_{11}+E_{33}+E_{12}+E_{13}-E_{23},$$

since

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & \epsilon \\ 1 & \epsilon & 1 \end{vmatrix} = - (\epsilon - 1)^2,$$

which is equal to zero for $\epsilon = 1$ and not zero for $\epsilon = -1$. Consequently the ranks of $E_{11}+E_{33}+E_{12}+E_{13}+E_{23}$ and $E_{11}+E_{33}+E_{12}+E_{13}-E_{23}$ are not equal. This is impossible.

Thus, we have

 $\Pi(X) = X$

for all real X. (If we do not use continuity, it holds for all rational X.) We may assume Γ to be II.

Further for real Y, the four points Yi, -Yi, Y, -Y, form a harmonic range, while

$$\Gamma(Y) = Y, \qquad \Gamma(-Y) = -Y,$$

thus we have

$$\Gamma(iY)Y^{-1} = -Y\Gamma(iY)^{-1}.$$

In particular,

$$(\Gamma(iI))^2 = -I.$$

Then

$$\Gamma(iI) = iJ$$

where J is an involutory symmetric matrix, that is $J^2 = I$ and J = J'. We have

456

a matrix T (not necessarily orthogonal) such that

Let
$$J = T'T.$$
$$T'^{-1}\Gamma(Z)T^{-1} = \Phi(Z),$$

we have then

$$\Phi(\mathfrak{i} I) = \mathfrak{i} I.$$

- / • - >

$$\nabla(Z) = -i\Phi(iZ)$$

Then

 $\nabla(0) = 0, \quad \nabla(I) = I, \quad \nabla(\infty) = \infty,$

so the ranks of Z and $\nabla(Z)$ are equal. By the method used before, we have

$$\nabla_1 = B' \nabla B$$

such that

 $\nabla_1(X) = X,$

for all real X. Thus, we have finally that

$$\Gamma(X + iY) = \Gamma(X) + \Gamma(iY) = X + iA'YA,$$

where A is independent of X and Y.

Now we have

$$A'YA \cdot Y^{-1} = Y(A'YA)^{-1},$$

that is,

$$(A'YAY^{-1})^2 = I,$$

for all real Y. Here we introduce a lemma.

LEMMA. Let A be a nonsingular matrix. If

$$(A'YAY^{-1})^2 = I$$

for all symmetric Y then $A = \rho I$, where $\rho = \pm 1$ or $\pm i$.

If the lemma is true, then

$$\Gamma(X + iY) = X + iY$$
 or $X - iY$.

The theorem is proved.

Proof of the lemma. (1) We have a nonsingular matrix Γ such that

$$\Gamma^{-1}A\Gamma = B$$

and

$$B=J_1\dotplus\cdots \dotplus J_{\nu},$$

where J_i is a Jordan matrix of degree n_i . Evidently

457

$$(B'(\Gamma'Y\Gamma)B(\Gamma'Y\Gamma)^{-1})^2 = \Gamma'(A'YAY^{-1})^2\Gamma'^{-1} = I.$$

Thus it is sufficient to prove the theorem for B instead of A.

(2) We shall prove $n_i = 1$. In fact, if

$$J_i = \begin{pmatrix} \lambda & 1 \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix},$$

then

which is impossible. Thus $n_i = 1$, that is,

$$B = [\epsilon_1, \cdots, \epsilon_n], \qquad \epsilon_r \neq 0,$$

which is a diagonal matrix.

(3) Putting

$$Y = \begin{pmatrix} 1 & 1 & 0 & 0 \cdots & 0 \\ 1 & 0 & 0 & 0 \cdots & 0 \\ 0 & 0 & 1 & 0 \cdots & 0 \\ 0 & 0 & 0 & 1 \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 \cdots & 1 \end{pmatrix}$$

we have

$$\left(\binom{\epsilon_1 \ 0}{0 \ \epsilon_2}\binom{1 \ 1}{1 \ 0}\binom{\epsilon_1 \ 0}{0 \ \epsilon_2}\binom{0 \ 1}{1 \ -1}\right)^2 = \binom{2 \ 2 \ 2}{\epsilon_1\epsilon_2} \frac{2 \ 2}{2\epsilon_1\epsilon_2}(\epsilon_1 - \epsilon_2) \\ 0 \ \epsilon_1\epsilon_2 \\ 0 \ \epsilon_1\epsilon_1 \\ 0 \ \epsilon_1\epsilon_2 \\ 0 \ \epsilon_1\epsilon_1 \\ 0 \ \epsilon_1\epsilon_2 \\ 0 \ \epsilon_1\epsilon_1 \\ 0 \ \epsilon_1\epsilon_2 \\ 0 \ \epsilon_1\epsilon_1 \\ 0 \ \epsilon_1 \\$$

which implies

$$\epsilon_1 = \epsilon_2.$$

Similarly

$$B = \epsilon I, \qquad \epsilon \neq 0.$$

Then $A = \epsilon I$. For Y = I, we have $\epsilon^4 = 1$, that is $\epsilon = \pm 1$, $\pm i$. The lemma is thus completely proved.

7. **Remarks.** The following results are contained in the proof of Theorem 8:

THEOREM 9. Let Φ be the complex field, and let \mathfrak{M} be a module formed by sym-

metric matrices over Φ . Let Γ be an additive continuous automorphism of \mathfrak{M} leaving the rank invariant, so that Γ satisfies

(i) $\Gamma(X) \in \mathfrak{M}$, if $X \in \mathfrak{M}$;

(ii) $\Gamma(X+Y) = \Gamma(X) + \Gamma(Y)$, if $X \in \mathfrak{M}$ and $Y \in \mathfrak{M}$;

(iii) $\Gamma(iX) = i\Gamma(X); and$

(iv) $\Gamma(X)$ has the same rank as X.

Then $\Gamma(X)$ is an inner automorphism, that is

$$\Gamma(X) = TXT'$$

for certain T.

In the case of the real field the situation is more complicated. In Theorem 9, we require an additional condition that the signature of $\Gamma(X)$ is the same as that of X.

The analogue of Theorem 8 in the real field is more complicated. Since Theorem 7 is not true in case of the real field, degeneracy and lengths of sides do not characterize the equivalence of triples of points, for example, there does not exist a real symplectic transformation Γ satisfying

$$\Gamma(0) = 0, \quad \Gamma(\infty) = \infty, \quad \Gamma\begin{pmatrix}2 & 0\\ 0 & -2\end{pmatrix} = \begin{pmatrix}-2 & 0\\ 0 & -2\end{pmatrix}.$$

In fact the transformation satisfying the first two of these relations is of the form

$$\Gamma(Z) = CZC'$$

where C is nonsingular and real. It keeps the signature invariant. By means of the signature of a triple, we may obtain an analogue of Theorem 9 in the real field.

II. GEOMETRY OF SKEW-SYMMETRIC MATRICES

Throughout II, we use

$$\mathfrak{F}_1 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}, \qquad \mathfrak{T} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}.$$

We let n = 2m.

8. Notions. A pair of matrices (Z_1, Z_2) is said to be skew-symmetric if

$$(Z_1, Z_2)\mathfrak{F}_1(Z_1, Z_2)' = 0,$$

that is,

$$Z_1 Z_2' = - Z_2 Z_{1-}'$$

A $2n \times 2n$ matrix \mathfrak{T} is said to be \mathfrak{F}_1 -orthogonal, if

$$\mathfrak{TF}_1\mathfrak{T}'=\mathfrak{F}_1.$$

We define

$$(W_1, W_2) = Q(Z_1, Z_2)\mathfrak{T}$$

to be an \mathcal{F}_1 -orthogonal transformation if Q is nonsingular.

The transformation carries nonsingular skew-symmetric pairs into nonsingular skew-symmetric pairs.

The nonsingular skew-symmetric pair of matrices may be considered as the homogeneous coordinates of a skew-symmetric matrix.

It is easy to verify that the geometry so obtained (analogous to I) is *transitive*, that is, any two points of the space are equivalent.

We define the rank of

$$(Z_1, Z_2)\mathfrak{F}_1(W_1, W_2)'$$

to be the arithmetic distance between the two points represented by (Z_1, Z_2) and (W_1, W_2) .

We have also:

Two point-pairs are equivalent if and only if they have the same arithmetic distance.

We may also define the cross-ratio-matrix of four points P_1 , P_2 , P_3 , P_4 , $P_i = (X_i, Y_i)$ (i=1, 2, 3, 4) by

$$\langle P_1, P_3 \rangle \langle P_1, P_4 \rangle^{-1} \langle P_2, P_4 \rangle \langle P_2, P_3 \rangle^{-1},$$

where

$$\langle P_i, P_j \rangle = (X_j, Y_j) \mathfrak{F}_1(X_i, Y_i)'.$$

The analogue of Theorem 6 is also true.

If the cross-ratio-matrix is equal to -I, we define P_1 , P_2 , P_3 , P_4 to be a harmonic range.

9. An algebraic theorem. On the ground of similarity, the following statement seems to be true.

Let Γ be a continuous (additive) automorphism of the module formed by all skew-symmetric matrices, such that $\Gamma(iX) = i\Gamma(X)$, and that the rank is left invariant. Then $\Gamma(X)$ is an inner automorphism.

Unfortunately, this statement is false and so the situation becomes more complicated. For n = 2,

	0	a	b	c		0	a	b	d
r.	- a	0	ď	e	=	— a	0	C	e
1	— b	- d	0	f		<i>-</i> − b	- c	0	f
	(– c	- e	-f	0		$\left - d \right $	- e	-f	0)

is an automorphism but not an inner automorphism.

It is an automorphism of the required kind, since the principal minors form equal sets, say

$$(af - be + cd)^2$$
; a^2 , b^2 , c^2 , d^2 , e^2 , f^2 .

[May

It is not an inner automorphism. In fact, we write

$$\Gamma\begin{pmatrix}P&Q\\-Q'&R\end{pmatrix}=\begin{pmatrix}P&Q'\\-Q&R\end{pmatrix},$$

where P and R are two-rowed skew-symmetric matrices. Suppose it is an inner automorphism, that is, that there exists a nonsingular matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

such that

(1)
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} P & Q \\ -Q' & R \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}' = \begin{pmatrix} P & Q' \\ -Q & R \end{pmatrix},$$

for all P, Q, R.

In particular, if P = R = 0, Q = I, we have

(2)
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}' = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

Combining (1) and (2), we have

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} Q & -P \\ R & Q' \end{pmatrix} = \begin{pmatrix} Q' & -P \\ R & Q \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Putting P = R = 0, we have

$$AQ = Q'A$$
, $BQ' = Q'B$, $CQ = QC$, $DQ' = QD$

for any Q. Consequently, we obtain

$$B = \beta I, \quad C = \gamma I, \quad A = D = 0.$$

But

$$\binom{0 \quad \beta I}{\gamma I \quad 0} \binom{P \quad Q}{-Q' \quad R} \binom{0 \quad \gamma I}{\beta I \quad 0} = \binom{\beta^2 R \quad -\beta \gamma Q'}{\beta \gamma Q \quad \gamma^2 P},$$

which, in general, is not equal to

$$\binom{P \ Q'}{-Q \ R}.$$

Thus the automorphism is *not* an inner automorphism.

The above argument suggests that in general we might have m-1 basic automorphisms:

- (i) $a_{14} \rightleftharpoons a_{23}$, other elements invariant;
- (ii) $a_{14} \rightleftharpoons a_{23}, a_{16} \rightleftharpoons a_{25}$, other elements invariant;

1945]

(iii) $a_{14} \rightleftharpoons a_{23}$, $a_{16} \rightleftharpoons a_{25}$, $a_{18} \rightleftharpoons a_{27}$, other elements invariant;

 $(m-1) a_{14} \rightleftharpoons a_{23}, \cdots, a_{1,2m} \rightleftharpoons a_{2,2m-1}$, other elements invariant.

Such a reasonable suggestion is a false one, since for $m \ge 3$, " $a_{14} \rightleftharpoons a_{23}$ " does not keep the rank invariant, for example,

$$\Gamma \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & -1 & 0 \end{pmatrix}$$

Here one matrix is singular while the other is nonsingular.

THEOREM 10. Let Φ be the field of complex numbers. Let \mathfrak{M} be the module formed by all skew-symmetric matrices over Φ . Let Γ be a continuous (additive) automorphism of Φ leaving the rank invariant and $\Gamma(iX) = i\Gamma(X)$. Then, for $m \neq 2$, Γ is an inner automorphism. For m = 2 there exists a nonsingular matrix Tsuch that

$$\Gamma(X) = TX, T'$$

where X, is either X or

0	a_{12}	a_{13}	a_{23}	
$-a_{12}$. 0	a_{14}	a24	
$-a_{13}$	$-a_{14}$	0	a ₃₄	
$-a_{23}$	$-a_{24}$	$-a_{34}$	0)	

Proof. (i) Evidently, the automorphisms

$$Y = TX_{\nu}T'$$

satisfy the requirement, where T is nonsingular.

(ii) The additive property may be stated as

(1)
$$\Gamma(X+Y) = \Gamma(X) + \Gamma(Y),$$

for any two X and Y belonging to \mathfrak{M} . Putting X = Y = 0, we have

(2)
$$\Gamma(0) = 0.$$

It is also very easy to deduce that

(3)
$$\Gamma(rX) = r\Gamma(X)$$

for any rational r. By continuity, it holds for any real r. Since $\Gamma(iX) = i\Gamma(X)$, the relation holds for all complex r.

Let

$$A = \Gamma\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right),$$

where A is a nonsingular skew-symmetric matrix. There exists a matrix Q such that

$$QAQ' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \dotplus \cdots \dotplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $\Gamma_1(X) = Q\Gamma(X)Q'$, then Γ_1 is an automorphism satisfying the properties given in the theorem and

(4)
$$\Gamma_1(J) = J,$$

where

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Write Γ instead of Γ_1 . (In the following we shall repeat this procedure by the simple statement "we may let Γ satisfy (4).")

(iii) Let $\lambda_1, \dots, \lambda_m$ be *m* distinct numbers, and let

$$A = \begin{pmatrix} 0 & \lambda_1 \\ -\lambda_1 & 0 \end{pmatrix} \dotplus \cdots \dotplus \begin{pmatrix} 0 & \lambda_m \\ -\lambda_m & 0 \end{pmatrix}.$$

Consider the two pairs of matrices A, J and $\Gamma(A)$, J. Since $\Gamma(A - \lambda J) = \Gamma(A) - \lambda J$, the characteristic roots of $\Gamma(A - \lambda J)$ are also $\lambda_1, \dots, \lambda_m$. (Each is a double root.) We have a nonsingular matrix M such that

(5)
$$M\Gamma(A)M' = A, \quad MJM' = J.$$

Now we are going to prove that M can be chosen independent of the λ 's. Write $M = M_{\lambda_1, \dots, \lambda_m}$. We have

$$\Gamma\left(\begin{pmatrix}0&0\\0&0\end{pmatrix} + \cdots + \begin{pmatrix}0&1\\-1&0\end{pmatrix} + \cdots + \begin{pmatrix}0&0\\0&0\end{pmatrix}\right)$$
$$= M_i\left(\begin{pmatrix}0&0\\0&0\end{pmatrix} + \cdots + \begin{pmatrix}0&1\\-1&0\end{pmatrix} + \cdots + \begin{pmatrix}0&0\\0&0\end{pmatrix}\right)M'_i(3),$$

where $M_i = M_{\lambda_1, \dots, \lambda_m}$ with $\lambda_i = 1$ and $\lambda_j = 0$ for $j \neq i$. In this expression, only the (2i-1)th and 2*i*th columns are significant. Let P be a matrix having (2i-1)th and 2*i*th columns in common with M_i for $i = 1, 2, \dots, n$. Then

$$\Gamma(A) = PAP'.$$

Putting $\lambda_1 = \cdots = \lambda_m = 1$, we find that P is nonsingular.

463

1945]

⁽³⁾ The term different from the zero-matrix is the *i*th term of the sum.

Now we may let

(6)

$$\Gamma(A)=A,$$

where

$$A = \begin{pmatrix} 0 & \lambda_1 \\ -\lambda_1 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & \lambda_m \\ -\lambda_m & 0 \end{pmatrix}.$$

(iv) The theorem is evident for m = 1. Now we take m = 2. Let

$$\Gamma \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix} = \begin{pmatrix} 0 & a' & b' & c' \\ -a' & 0 & d' & e' \\ -b' & -d' & 0 & f' \\ -c' & -e' & -f' & 0 \end{pmatrix}$$

Since

$$\begin{vmatrix} 0 & a - \lambda & b & c \\ -a + \lambda & 0 & d & e \\ -b & -d & 0 & f - \mu \\ -c & -e & -f + \mu & 0 \end{vmatrix} = 0,$$

that is, $(a-\lambda)(f-\mu)-be+dc=0$, if and only if

$$\begin{vmatrix} 0 & a' - \lambda & b' & c' \\ -a' + \lambda & 0 & d' & e' \\ -b' & -d' & 0 & f' - \mu \\ -c' & -e' & -f' + \mu & 0 \end{vmatrix} = 0,$$

we have

(7)
$$a = a', f = f',$$

(8) $be - cd = b'e' - c'd'.$

Now we consider

$$\Gamma \begin{pmatrix} \cdot & 1 & 0 \\ \cdot & 0 & 1 \\ * & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & M \\ * & \cdot \end{pmatrix},$$
$$\Gamma \begin{pmatrix} \cdot & 1 & 0 \\ \cdot & 0 & 0 \\ * & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & M_1 \\ * & \cdot \end{pmatrix},$$

where "." stands for zero-matrix and "*" stands for a matrix which either is

evident or has no essential significance in the consideration. (This convention will be retained for the rest of the paper.) Then M is of rank 2, M_1 and $M - M_1$ are of ranks less than or equal to 1, that is

$$|M_1-\lambda M|=0$$

has two characteristic roots 0 and 1. We can find two matrices P and Q of determinant 1, such that

$$PMQ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad PM_1Q = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Therefore

$$\binom{P \ 0}{0 \ Q'}\binom{M}{*}\binom{P' \ 0}{0 \ Q} = \begin{pmatrix} & 1 \ 0 \ & 1 \end{pmatrix},$$

$$\binom{P \ 0}{0 \ Q'}\binom{\cdot \ M_1}{\ast \ \cdot \ }\binom{P' \ 0}{0 \ Q} = \begin{pmatrix} 1 \ 0 \\ \cdot \ 0 \ 0 \\ \ast \ \cdot \ \end{pmatrix}.$$

Since

$$\begin{pmatrix} P & 0 \\ 0 & Q' \end{pmatrix} \begin{pmatrix} 0 & \lambda & \\ -\lambda & 0 & \\ & 0 & \mu \\ & -\mu & 0 \end{pmatrix} \begin{pmatrix} P' & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} 0 & \lambda & \\ -\lambda & 0 & \\ & 0 & \mu \\ & -\mu & 0 \end{pmatrix},$$

we may let

$$\Gamma\left(\begin{array}{cc} b & 0\\ 0 & e\\ * & \end{array}\right) = \left(\begin{array}{cc} b & 0\\ 0 & e\\ * & \end{array}\right).$$

We deduce easily that

(9)

$$b = b', \quad e =$$

e'.

From (8) we have

$$cd = c'd'.$$

In particular, we have

$$\Gamma\left(\begin{array}{c} 0 \ 1 \\ 1 \ 0 \\ * \end{array}\right) = \left(\begin{array}{c} 0 \ c' \\ d' \ 0 \\ * \end{array}\right), \quad c'd' = 1.$$

Since

$$\begin{pmatrix} (d')^{1/2} & 0 & 0 & 0 \\ 0 & (d')^{-1/2} & 0 & 0 \\ 0 & 0 & (d')^{-1/2} & 0 \\ 0 & 0 & 0 & (d')^{1/2} \end{pmatrix} \begin{pmatrix} 0 & a & b & c' \\ -a & 0 & d' & e \\ -b & -d' & 0 & f \\ -c' & -e & -f & 0 \end{pmatrix} \begin{pmatrix} (d')^{1/2} & 0 & 0 & 0 \\ 0 & (d')^{-1/2} & 0 & 0 \\ 0 & 0 & (d')^{-1/2} & 0 \\ 0 & 0 & 0 & (d')^{1/2} \end{pmatrix}$$
$$= \begin{pmatrix} 0 & a & b & 1 \\ -a & 0 & 1 & e \\ -b & -1 & 0 & f \\ -1 & -e & -f & 0 \end{pmatrix}$$

we may let

$$\Gamma \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Finally, we have

$$\Gamma \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & \lambda \\ 0 & 0 & \mu & 0 \\ 0 & -\mu & 0 & 0 \\ -\lambda & 0 & 0 & 0 \end{pmatrix}.$$

Then

$$\left| \begin{pmatrix} 0 & \lambda \\ \mu & 0 \end{pmatrix} - k \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right| = 0$$

for k = 1 and 0, so we have either

or

$$\Gamma(X) = X_1.$$

 $\Gamma(X) = X$

(v) For the sake of simplicity, we give the proof for m = 3. The method is valid for any m.

Let $M = (a_{ij}), M_1 = (a'_{ij})$ and

$$\Gamma(M) = M_1.$$

Since, by (iii),

$$\Gamma \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ & 0 \lambda & \cdot \\ & -\lambda 0 & \cdot \\ \cdot & & 0 \mu \\ \cdot & & -\mu 0 \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ & J \lambda & \cdot \\ & -\lambda 0 & \cdot \\ \cdot & & 0 \mu \\ \cdot & & -\mu 0 \end{pmatrix},$$

466

[May

the determinants of

.

$$M = \begin{pmatrix} \cdot & \cdot & \cdot \\ & 0 \lambda & \cdot \\ & -\lambda 0 & \cdot \\ & & 0 \mu \\ \cdot & & -\mu 0 \end{pmatrix} \text{ and } M_1 = \begin{pmatrix} \cdot & \cdot & \cdot \\ & 0 \lambda & \cdot \\ & -\lambda 0 & \cdot \\ & & 0 \mu \\ \cdot & & -\mu 0 \end{pmatrix}$$

are identically equal. Comparing the coefficients of $\lambda^2 \mu^2$, we find $a_{12} = a_{12}'$. Similarly, we deduce

$$a_{34} = a'_{34}, \qquad a_{56} = a'_{56}.$$

Now we let

$$\Gamma \begin{pmatrix} 1 & 0 & . \\ 0 & 1 & . \\ * & . & . \\ . & . & . \end{pmatrix} = M_1.$$

Since for $\lambda \mu = 1$

$$\left| \begin{array}{c} \cdot & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \ast & \cdot \end{array} \right| - \left| \begin{array}{c} 0 & \lambda & \cdot \\ -\lambda & 0 & \cdot \\ \cdot & 0 & \mu \\ \cdot & -\mu & 0 \end{array} \right| = 0,$$

it follows that

is of rank not greater than 2 for all λ , μ satisfying $\lambda \mu = 1$. Thus we have

$$\begin{vmatrix} 0 \lambda & a'_{13} & a'_{14} \\ -\lambda 0 & a'_{23} & a'_{24} \\ & 0 & \mu \\ * & -\mu & 0 \end{vmatrix} = \begin{vmatrix} 0 \lambda & a'_{13} & a'_{15} \\ -\lambda 0 & a'_{23} & a'_{25} \\ & 0 & a'_{35} \end{vmatrix} = \begin{vmatrix} 0 \lambda & a'_{13} & a'_{16} \\ -\lambda 0 & a'_{23} & a'_{26} \\ & 0 & a'_{36} \end{vmatrix},$$
$$= \begin{vmatrix} 0 \lambda & a'_{14} & a'_{15} \\ -\lambda 0 & a'_{24} & a'_{25} \\ & 0 & a'_{45} \end{vmatrix} = \begin{vmatrix} 0 \lambda & a'_{14} & a'_{16} \\ -\lambda 0 & a'_{24} & a'_{26} \\ & 0 & a'_{46} \end{vmatrix} = \begin{vmatrix} 0 \lambda & a'_{14} & a'_{16} \\ -\lambda 0 & a'_{25} & a'_{26} \\ & 0 & a'_{45} \end{vmatrix}, = \begin{vmatrix} 0 \lambda & a'_{46} & a'_{46} \\ & -\lambda & 0 & a'_{46} \\ & & -a'_{46} & 0 \end{vmatrix} = \begin{vmatrix} 0 \lambda & a'_{15} & a'_{16} \\ -\lambda 0 & a'_{25} & a'_{26} \\ & & & \cdot \end{vmatrix} = 0.$$

.

The first equation gives

$$\left|\begin{array}{cc}a'_{13} & a'_{14}\\a'_{23} & a'_{24}\end{array}\right| = 1,$$

so we may take

$$\begin{pmatrix} a'_{13} & a'_{14} \\ a'_{23} & a'_{24} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(In fact, we can choose a suitable Q such that

$$\begin{pmatrix} I & 0 & 0 \\ 0 & Q & 0 \\ 0 & 0 & I \end{pmatrix} M \begin{pmatrix} I & 0 & 0 \\ 0 & Q' & 0 \\ 0 & 0 & I \end{pmatrix}$$

has the required form.)

Then, from the system of equations, we have

$$a'_{35} = a'_{36} = a'_{45} = a'_{46} = a'_{15} = a'_{16} = a'_{25} = a'_{26} = 0.$$

Thus, we may let

$$\Gamma \left(\begin{array}{ccc} & 1 & 0 & \\ & 0 & 1 & \\ & & \ddots & \\ & & \ddots & \\ & & & \ddots \end{array} \right) = \left(\begin{array}{ccc} & 1 & 0 & \\ & 0 & 1 & \\ & & \ddots & \\ & & & \ddots \end{array} \right).$$

Let

$$\Gamma \begin{pmatrix} \cdot & 1 & 0 & \cdot \\ \cdot & 0 & 0 & \cdot \\ * & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & P & * \\ * & \cdot & * \\ * & * & \cdot \end{pmatrix} = M_1.$$

Since M_1 is of rank 2, we have |P| = 0. Since

(10)
$$\begin{pmatrix} & 1 & 0 & \\ & 0 & 1 & \\ & & \ddots & \\ & & \ddots & \\ & & \ddots & & \end{pmatrix} - M_1$$

is of rank 2, we have |P-I| = 0. There is also a matrix Q such that

$$QPQ^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus we may assume that

[May

468

$$\Gamma\left(\begin{array}{cccc} & 1 & 0 & \\ & & 0 & 0 & \\ & & & \ddots & \\ & & & \ddots & \\ & & & & \ddots \end{array}\right) = \left(\begin{array}{cccc} & 1 & 0 & a_{15}' & a_{16}' \\ & & 0 & 0 & a_{25}' & a_{26}' \\ & & & a_{35}' & a_{36}' \\ & & & & a_{35}' & a_{36}' \\ & & & & a_{45}' & a_{46}' \\ & & & & & \ddots \end{array}\right).$$

By consideration of the ranks of the previous matrix and the matrix given in (10) we find

$$a'_{15} = a'_{16} = a'_{25} = a'_{26} = a'_{35} = a'_{36} = a'_{45} = a'_{46} = 0.$$

Consider again a general skew-symmetric matrix M and its image $M_1 = \Gamma(M)$. By the same method used for m = 2, we have either

	{ 0	a_{12}	<i>a</i> ₁₃	<i>a</i> ₁₄	a'_{15}	a_{16}
		· 0	a 23	a_{24}	a'_{25}	a_{26}^{\prime}
			0	a ₈₄	a'_{35}	a'86
$M_1 =$				0	a'45	a'_{46}
		*			0	a_{56}^{\prime}
	l					0

$$M_{1} = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{23} & a_{15}' & a_{16}' \\ 0 & a_{14} & a_{24} & a_{25}' & a_{26}' \\ & 0 & a_{34} & a_{35}' & a_{36}' \\ & & 0 & a_{45}' & a_{46}' \\ * & & 0 & a_{56}' \\ & & & 0 \end{pmatrix}$$

Repeating the process for

$$\binom{a_{15}}{a_{25}} \stackrel{a_{16}}{a_{26}},$$

we obtain either

 $a_{25} \rightleftharpoons a_{25}, \quad a_{16} \rightleftharpoons a_{16},$

 $a_{25} \rightleftharpoons a_{16}, \quad a_{16} \rightleftharpoons a_{25}.$

or

For the equivalence of $a_{14} \rightleftharpoons a_{23}$ and $a_{16} \rightleftharpoons a_{25}$, we have three cases: (α) $\Gamma(M) = M_1$, M_1 is obtained by replacing a_{35} , a_{36} , a_{45} , a_{46} by a_{35}' , a_{36}' , a_{45}' , a_{46}' in M;

$$(\beta) \qquad \Gamma(M) = M_2 = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{23} & a_{15} & a_{16} \\ 0 & a_{14} & a_{24} & a_{25} & a_{26} \\ & 0 & a_{34} & a_{35}' & a_{36}' \\ & & 0 & a_{45}' & a_{46}' \\ & & & 0 & a_{56}' \\ & & & & 0 \end{pmatrix}$$

$$(\gamma) \qquad \Gamma(M) = M_3 = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{23} & a_{15} & a_{25} \\ 0 & a_{14} & a_{24} & a_{16} & a_{26} \\ & 0 & a_{34}' & a_{35}' & a_{36}' \\ & & 0 & a_{45}' & a_{46}' \\ & & & 0 & a_{56}' \\ & & & & 0 & a_{56}' \\ & & & & & 0 \end{pmatrix}$$

(α) We leave a_{35} , a_{36} , a_{45} , a_{46} arbitrary. Putting $a_{16} = a_{24} = a_{34} = 1$, $a_{25} = x$, and the others equal to 0, we have det $(M) = (x - a_{35})^2$, det $(M_1) = (x - a'_{35})^2$. We have det(M) = 0 if and only if det $(M_1) = 0$, that is $a_{35} = a'_{35}$. Next putting $a_{16} = a_{23} = a_{34} = 1$, $a_{25} = x$, and the others equal to 0, we obtain $a_{45} = a'_{45}$. Putting $a_{15} = a_{24} = a_{14} = 1$, $a_{26} = x$, and the others equal to 0 and putting $a_{15} = a_{23} = a_{34}$ = 1, $a_{26} = x$ and the others equal to 0, we have respectively

$$a_{36} = a_{36}', \quad a_{46} = a_{46}'.$$

Thus we have

 $\Gamma(M) \doteq M.$

(β) and (γ) Putting $a_{24} = a_{34} = 1$, $a_{15} = a_{25} = x$ and others equal to 0, we have $a_{35} = a'_{35}$. Further, if we put

$$a_{12} = a_{13} = 0$$
, $a_{14} = x$, $a_{15} = 1$, $a_{16} = 0$, $a_{23} = y$, $a_{24} = a_{25} = 0$, $a_{26} = 1$,
 $a_{34} = 0$, $a_{35} = -1$, $a_{36} = a_{45} = a_{46} = 0$, $a_{56} = 1$,

then

$$d(M) = (x(y-1))^2, \quad d(M_1) = (y(x-1))^2.$$

By putting x = -1, y = +1, we see that this is impossible.

The general proof may be arranged in the following steps:

(a) Dividing the matrix into m^2 2-rowed matrices.

(b) Choosing the first row of the small matrices as in the case m = 3 and applying the analogous method as above to the image.

(c) Determining the other small matrices by the method given for m=3 (from (10) et seq.).

(d) Considering the 6-rowed minors we find that the exceptional case appearing for m = 2 cannot exist for $m \ge 3$.

10. Another generalization of von Staudt's theorem. The transformation

$$(W_1, W_2) = Q(\overline{Z}_1, \overline{Z}_2)\mathfrak{T}$$

is called *anti-orthogonal* if Q is nonsingular and \mathfrak{T} is \mathfrak{F}_1 -orthogonal.

LEMMA. Let A be a nonsingular matrix. Suppose that

$$(A'YAY^{-1})^2 = I$$

holds for all skew-symmetric Y. For m = 1, A is a matrix of determinant ± 1 . For m > 1, then

$$A = \rho I$$
, or $A = \rho T [1, \dots, 1, -1] T^{-1}$,

where $\rho = \pm 1$, $\pm i$, and conversely.

Proof. (i) The result is evident for m = 1.

For m > 1, $A = \rho I$ evidently satisfies the equation. Now we prove that $A = \rho T [1, \dots, 1, -1] T^{-1}$ satisfies the equation.

We write

$$T'YT = \begin{pmatrix} Y_1^{(n-1)}v \\ -v' 0 \end{pmatrix}, \qquad (T'YT)^{-1} = \begin{pmatrix} Y_1^* & v^* \\ -v^{*'} & 0 \end{pmatrix}.$$

Then

$$\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} Y_1 & v \\ -v' & 0 \end{pmatrix} \begin{pmatrix} Y_1^* & v^* \\ -v^{*'} & 0 \end{pmatrix} = \begin{pmatrix} Y_1 Y_1^* - v v^{*'} & Y_1 v^* \\ -v' Y_1^* & -v' v^* \end{pmatrix}.$$

Further

$$T'A'YAY^{-1}T'^{-1} = \rho^{2}[1, \cdots, 1, -1] \begin{pmatrix} Y_{1} & v \\ -v' & 0 \end{pmatrix} [1, \cdots, 1, -1] \begin{pmatrix} Y_{1}^{*} & v^{*} \\ -v'^{*} & 0 \end{pmatrix}$$
$$= \rho^{2} \begin{pmatrix} Y_{1}Y_{1}^{*} + vv^{*} & Y_{1}v^{*} \\ v'Y_{1}^{*} & v'v^{*} \end{pmatrix} = \rho^{2} \begin{pmatrix} I + 2vv^{*} & 0 \\ 0 & -1 \end{pmatrix}.$$

Since $v^*'v = -1$, we have

$$(I^{(n-1)} + 2vv^{*'})^2 = I + 4vv^{*'} + 4vv^{*'}vv^{*'} = I^{(n-1)};$$

hence the result.

(ii) As in the proof of the lemma of §6, we may assume that

$$A = J_1 \dotplus J_2 \dotplus \cdots$$

where J_r is again of degree n_r . The number of odd n_r 's is always even.

(iii) We consider the case

L. K. HUA

$$A=J^{(n)},$$

where n is even. Write

$$J = \begin{pmatrix} p & q \\ 0 & p \end{pmatrix}, \qquad p = p^{(n/2)}, \qquad q = q^{(n/2)},$$

where

$$p = \begin{pmatrix} \lambda & 1 & 0 \cdots & 0 \\ 0 & \lambda & 1 \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 \cdots & \lambda \end{pmatrix}, \qquad q = \begin{pmatrix} 0 & 0 \cdots & 0 \\ 0 & 0 \cdots & 0 \\ \vdots & \vdots & \vdots \\ 1 & 0 \cdots & 0 \end{pmatrix}.$$

Take

$$Y = \begin{pmatrix} 0 & I^{(n/2)} \\ - & I^{(n/2)} & 0 \end{pmatrix};$$

then

$$I = (A'YAY^{-1})^{2} = \left(\begin{pmatrix} p' & 0 \\ q' & p' \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} p & q \\ 0 & p \end{pmatrix} \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix} \right)^{2}$$
$$= \begin{pmatrix} (p'p)^{2} & * \\ * & * \end{pmatrix}$$

implies $(p'p)^2 = I^{(n/2)}$, which is impossible for n > 2 (that is m > 1). (iv) Let

 $A = J_1 + J_2, \qquad n_1 + n_2 = n$

where n_1 and n_2 are both odd. Let $n_1 = n_2$. Write

$$A = \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & I^{(n/2)} \\ - & I & 0 \end{pmatrix}.$$

Then, we have

$$(A'YAY^{-1})^2 = \begin{pmatrix} (p'q)^2 & * \\ * & * \end{pmatrix} = I,$$

which is possible only for $n_1 = n_2 = 1$. Further let $n_1 > n_2$. We write

$$A = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & I^{(n/2)} \\ -I & 0 \end{pmatrix}.$$

Then

$$(A'YAY^{-1})^2 = \begin{pmatrix} (p'r)^2 & * \\ * & * \end{pmatrix} = I,$$

which is impossible for $n_1 > 3$. For $n_1 = 3$ and $n_2 = 1$, we have consequently

$$A = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}, \qquad \mu = -\lambda, \qquad \lambda^4 = 1.$$

Taking

$$Y = \left(\begin{array}{cc} & 2 & 1 \\ & 1 & 1 \\ * & & \end{array}\right),$$

we find this also to be impossible.

Thus each of the numbers

 n_1, n_2, \cdots

must be either 1 or 2.

(v) It is easily seen that no two of the n_r 's can be 2. In fact

$$A = \begin{pmatrix} \lambda_1 & 1 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 1 \\ 0 & 0 & 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} p \\ \cdot \\ q \end{pmatrix}$$

say. Taking

$$Y = \begin{pmatrix} 0 & I \\ - & I & 0 \end{pmatrix},$$

we find this to be impossible.

(vi) Further, if one of the n,'s is 2, then n is equal to 2. In fact, suppose that

$$A = \begin{pmatrix} \lambda_1 & 1 & \\ 0 & \lambda_1 & \\ & \lambda_2 & 0 \\ & & 0 & \lambda_3 \end{pmatrix}.$$

Taking

$$Y = \begin{pmatrix} 0 & I \\ - & I & 0 \end{pmatrix},$$

we have

$$\lambda_2 = -\lambda_3, \qquad \lambda_1^2 \lambda_2^2 = 1.$$

Taking further

$$Y = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ -1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

we have $\lambda_2 = \lambda_3$. Both results cannot hold simultaneously. (vii) Suppose $n \ge 4$. Let

$$A = [\lambda_1, \lambda_2, \lambda_3, \lambda_4].$$

Taking

$$Y = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ -1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

we have

$$(1) (A'YAY^{-1})^{2} = \begin{pmatrix} \lambda_{1}^{2} \lambda_{4}^{2} & \lambda_{1}(\lambda_{1}\lambda_{4} + \lambda_{2}\lambda_{3})(\lambda_{3} - \lambda_{4}) & \cdot & \cdot \\ \cdot & \lambda_{2}^{2} \lambda_{3}^{2} & \cdot & \cdot \\ \cdot & \lambda_{2}^{2} \lambda_{3}^{2} & \lambda_{3}(\lambda_{1}\lambda_{4} + \lambda_{2}\lambda_{3})(\lambda_{1} - \lambda_{2}) \\ \cdot & \cdot & \lambda_{1}^{2} \lambda_{4}^{2} \end{pmatrix} = I$$

which implies

$$\lambda_1^2 \lambda_4^2 = \lambda_2^2 \lambda_3^2 = 1.$$

Since λ_1 , λ_2 , λ_3 , λ_4 can be permuted, we have

$$\lambda_i^2 \lambda_j^2 = 1 \qquad \text{for all } i, j \ (i \neq j).$$

Thus

$$\lambda_1^4 = 1, \qquad \lambda_1^2 = \lambda_2^2 = \lambda_3^2 = \lambda_4^2 = \pm 1.$$

In general $A = [\lambda_1, \dots, \lambda_n]$ where $\lambda_1^2 = \dots = \lambda_n^2 = \pm 1$. By choosing a suitable ρ in the lemma, we may consider the case with

$$\lambda_1^2 = \lambda_2^2 = \cdots = \lambda_n^2 = 1.$$

If among the λ 's there occur two positive and two negative numbers, we take $\lambda_1 = \lambda_4 = 1$, $\lambda_2 = \lambda_3 = -1$. Then (1) is impossible. Thus we have the lemma.

THEOREM 11. A transformation satisfying the following conditions:

- (1) one-to-one and continuous,
- (2) carrying skew-symmetric matrices into skew-symmetric matrices,

[May

(3) keeping arithmetic distance invariant, and

(4) keeping the harmonic relation invariant,

is for $n \neq 4$ either \mathfrak{F}_1 -orthogonal or anti-orthogonal. In the case n = 4, the transformation is either \mathfrak{F}_1 -orthogonal or anti-orthogonal, or is equivalent to

$$\Gamma(Z) = Z_1, \quad where \quad Z = \begin{pmatrix} p & q \\ -q' & r \end{pmatrix}, \qquad Z_1 = \begin{pmatrix} p & q' \\ -q & r \end{pmatrix},$$

or equivalent to

$$\Gamma(Z) = \overline{Z}_1.$$

Proof. (i) A triple of points, no two of which have arithmetic distance less less than n, is equivalent to

$$0, \qquad \begin{pmatrix} 0 & I^{(m)} \\ - & I^{(m)} & 0 \end{pmatrix}, \quad \infty.$$

We may let the transformation satisfy

 $\Gamma(0) = 0, \quad \Gamma(\mathfrak{F}) = \mathfrak{F}, \quad \Gamma(\infty) = \infty.$

(ii) As in the symmetric case, we have

$$\Gamma(Z) + \Gamma(Z_1) = \Gamma(Z + Z_1).$$

Again, for $n \neq 4$, we have, analogous to the symmetric case,

$$\Gamma(X+iY)=X+iA'YA.$$

Since Y, -Y are separated harmonically by iY and -iY for real Y, we have

$$\Gamma(Yi)Y^{-1} = -Y(\Gamma(Yi))^{-1},$$

that is,

$$(A'YAY^{-1})^2 = I$$

for all real Y. Now we suppose $m \ge 3(4)$; then we have

$$\Gamma(X+iY)=X\pm iY$$

or

$$\Gamma(X + iY) = X \pm iT'^{-1}[1, \cdots, 1, -1]T'YT[1, \cdots, 1, -1]T^{-1}.$$

The first case is what we require. Changing variables in the second case we may let

$$\Gamma(X + iY) = X \pm i[1, \cdots, 1, -1]Y[1, \cdots, 1, -1].$$

Since

⁽⁴⁾ For m = 1, the result is almost evident.

L. K. HUA

$$\begin{vmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & i & i \\ * & \cdot & \cdot \end{vmatrix} = 0 \text{ and } \begin{vmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & i - i \\ * & \cdot & \cdot \end{vmatrix} \neq 0$$

the rank is not invariant. The last case does not satisfy our requirement.

In case m = 2, a great deal of special consideration is needed. Apart from the lemma, we require the solutions of

$$(A'Y_1AY^{-1})^2 = I,$$

where

$$Y = \begin{pmatrix} P & Q \\ -Q' & R \end{pmatrix}, \qquad Y_1 = \begin{pmatrix} P & Q' \\ -Q & R \end{pmatrix}.$$

The proof of the lemma establishes that either

$$A = \rho I$$

or

$$A = \rho T[1, 1, 1, -1]T^{-1}.$$

(The Q used here is always symmetric.)

As in the preceding proof we have four cases,

$$\Gamma(X + iY) = X \pm iA'YA, \text{ or } X_1 \pm iA'Y_1A',$$

or $X_1 \pm iA'YA, \text{ or } X \pm iA'Y_1A.$

By the previous argument, for $m \ge 3$, we have, for the first two cases,

$$\Gamma(Z) = Z, \overline{Z}, Z_1, \overline{Z}_1,$$

where Z = X + iY, and Z_1 is obtained from Z by the process yielding Y_1 from Y.

Next, if $\Gamma(X+iY) = X_1 \pm iA'YA$, we have either

$$\Gamma(X + iY) = X_1 \pm iY$$
 or $X_1 \pm i[1, 1, 1, -1]Y[1, 1, 1, -1].$

Putting

$$Z = \begin{pmatrix} 0 & 0 & i & i \\ 0 & 0 & 1 & 1 \\ -i & -1 & 0 & 0 \\ -i & -1 & 0 & 0 \end{pmatrix},$$

$$\Gamma(Z) = \begin{pmatrix} 0 & 0 & i & i+1 \\ 0 & 0 & 0 & 1 \\ -i & 0 & 0 & 0 \\ -i & -1 & -1 & 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 0 & i & -i+1 \\ 0 & 0 & 0 & 1 \\ -i & 0 & 0 & 0 \\ i & -i & -1 & 0 & 0 \end{pmatrix},$$

[May

we see that both these automorphisms could render a singular matrix nonsingular. Thus both these cases are ruled out.

Finally, the possibility of

$$\Gamma(X + iY) = X \pm iAY_1A'$$

may be treated in a similar way.

III. GEOMETRY OF HERMITIAN MATRICES

The geometry of symmetric matrices in the real domain is closely analogous to the present geometry.

11. Notions. We define an Hermitian pair (Z_1, Z_2) of matrices by

$$(\overline{Z}_1,\overline{Z}_2)\mathfrak{F}(Z_1,Z_2)'=0.$$

A conjunctively symplectic matrix \mathfrak{T} is defined by(⁵)

$$\mathfrak{T}^*\mathfrak{F}\mathfrak{T}'=\mathfrak{F}.$$

We define a conjunctively symplectic transformation by

$$(W_1, W_2) = Q(Z_1, Z_2)\mathfrak{T}.$$

We identify two nonsingular Hermitian pairs of matrices (Z_1, Z_2) and (W_1, W_2) by means of the relation

$$(Z_1, Z_2) = Q(W_1, W_2).$$

It is called a point of the space. Evidently, the space so defined is transitive. The rank of

 $(\overline{W}_1, \overline{W}_2)\mathfrak{F}(Z_1, Z_2)'$

is defined to be the arithmetic distance of the points (W_1, W_2) and (Z_1, Z_2) . Two pairs of points are equivalent if and only if they have the same arithmetic distance.

Let P_1 , P_2 , P_3 be three points no two of which have arithmetic distance less than *n*. Then they are equivalent to the three points

0, ∞ , $K(=[1, \cdots, 1, -1, \cdots, -1])$.

The signature of K is defined to be the signature of the range P_1 , P_2 , P_3 . (The order of points is significant.)

Evidently the signature is invariant under the group. We also may say that two triples of points are in the same sense if they have the same signature. We may prove that if two ranges are in the same sense, there is a conjunctively symplectic transformation carrying one into the other.

As to the equivalence of quadruples of points, a great deal of difficulty arises from the fact that the existing treatments of the theory of Hermitian

⁽⁵⁾ I* denotes the conjugate complex matrix of I.

forms are incomplete. We shall give elsewhere a complete classification and then its application to the present problem will be immediate.

12. A further generalization of von Staudt's theorem.

THEOREM 12. Let Γ be an additive continuous automorphism of the module formed by all Hermitian matrices keeping rank and signature invariant. Then Γ is either an inner automorphism or an anti-automorphism $(Z \rightarrow \overline{PZ}P')$.

Proof. (Cf. the results of §6.) (i) We have $\Gamma(0) = 0$. Let

 $\Gamma(I) = H_0.$

Since H_0 is positive definite, we may let

 $\Gamma(I) = I.$

As in the proof of Theorem 8 (in the real field), we may let

$$\Gamma(X) = X$$

for all real symmetric X.

Let Y be any real skew-symmetric matrix, and let

$$\Gamma(iY) = H.$$

Since

 $\det\left(X+iY\right)=0$

if and only if

 $\det\left(X+H\right)=0,$

by Hilbert's theorem on polynomial ideals, we have an integer ρ such that

 $(\det (X + iY))^{\rho} \equiv 0 \pmod{\det (X + H)}$

and

 $(\det (X + H))^{\rho} \equiv 0 \pmod{\det (X + iY)},$

in the polynomial ring formed from the real field by adjunction of the elements of X. Let $X = X' = (x_{ij})$. We write

$$det (X + iY) = f_1 x_{11} + g_1,$$

$$det (X + H) = f_2 x_{11} + g_2,$$

where f_1, f_2, g_1, g_2 are elements in the ring \Re (generated by the elements of X omitting x_{11}). Since

$$(f_2(f_1x_{11} + g_1) - f_1(f_2x_{11} + g_2))^{\rho} \equiv 0 \pmod{\det(X + H)},$$

and since $f_2g_1 - f_1g_2$ is independent of x_{11} , we have

$$f_2g_1 - f_1g_2 = 0.$$

Since the determinant of a Hermitian matrix is an irreducible polynomial in its elements, f_1 and f_2 are irreducible and f_1 and g_1 have no common divisor. Consequently we have

$$f_1 = f_2, \qquad g_1 = g_2.$$

In this procedure, we have to compare one of the coefficients.

Thus

$$\det (X + iY) = \det (X + H).$$

Consequently each principal minor of iY equals the corresponding principal minor of H. We complete the proof with the aid of the following lemma.

LEMMA. If two Hermitian matrices H and K have the same principal minors of orders 1, 2, 3, then (for exp $(x) = e^x$)

$$H = [\exp(i\theta_1), \cdots, \exp(i\theta_n)]K^*[\exp(-i\theta_1), \cdots, \exp(-i\theta_n)]_{i}$$

where K^* is obtained from K by replacing k_r , by either k_r , or \bar{k}_r .

From the lemma, we may let

$$h_{rs} = \pm i y_{rs}.$$

Since one of

(2	i	-i		{ 2	i	-i
- i	0	1	and	- i	0	1
i	1	o)		lī	1	0)

is singular and the other is not, we have

$$H = \pm iY.$$

The proof of the lemma is straightforward. Considering the 1-rowed principal minors of $H = (h_{rs})$, $K = (k_{rs})$, we have

$$h_{rr} = k_{rr}$$

Since

$$\begin{vmatrix} h_{rr} & h_{rs} \\ \bar{h}_{rs} & h_{ss} \end{vmatrix} = \begin{vmatrix} h_{rr} & k_{rs} \\ \bar{k}_{rs} & h_{ss} \end{vmatrix},$$

We may choose
$$\theta_1, \cdots, \theta_n$$
 such that the matrix

$$\left[\exp\left(i\theta_{1}\right),\cdots,\exp\left(i\theta_{n}\right)\right]H\left[\exp\left(-i\theta_{1}\right),\cdots,\exp\left(-i\theta_{n}\right)\right]$$

 $|h_{rs}|^2 = |k_{rs}|^2$.

has real $h_{12}, h_{13}, \cdots, h_{1n}$. We may let

 $h_{1i} = k_{1i}$

be real and positive. Consider

$$\begin{vmatrix} h_{11} & h_{1i} & h_{ij} \\ \bar{h}_{1i} & h_{ii} & h_{ij} \\ \bar{h}_{1j} & \bar{h}_{ij} & h_{jj} \end{vmatrix} = \begin{vmatrix} h_{11} & h_{1i} & h_{1j} \\ \bar{h}_{11} & h_{ii} & h_{ij} \\ \bar{h}_{1j} & \bar{k}_{ij} & h_{jj} \end{vmatrix}.$$

We have

$$h_{ij}+\bar{h}_{ij}=k_{ij}+\bar{k}_{ij};$$

then letting $h_{ij} = \alpha + \beta i$, $k_{ij} = \gamma + \delta i$, we have

$$\alpha^2 + \beta^2 = \gamma^2 + \delta^2, \qquad \alpha = \gamma.$$

Thus $\beta = \pm \delta$ and we have

$$h_{ij} = k_{ij}$$
 or \bar{k}_{ij} . Q.E.D.

THEOREM 13. A transformation satisfying the following conditions:

(1) one-to-one and continuous,

(2) carrying Hermitian matrices into Hermitian matrices,

(3) keeping arithmetic distance invariant,

(4) keeping sense of triples of points invariant,

(5) keeping the harmonic relation invariant,

is either a conjunctively symplectic or a conjunctively anti-symplectic transformation.

The proof is omitted because of the similarity to the real analogue of Theorem 8 (cf. ?).

IV. GEOMETRY OF RECTANGULAR MATRICES

13. Subgeometries of the geometry of unitary matrics. The geometry studied in III may also be interpreted as the geometry of unitary matrices. Since the matrix

$$\mathfrak{F}=i\begin{pmatrix}0&I\\-I&0\end{pmatrix}$$

is of signature 0, we may use

$$\mathfrak{F} = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$$

instead of it. Then the pair of matrices (Z_1, Z_2) , satisfying

$$(\overline{Z}_1, \overline{Z}_2) \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix} (Z_1, Z_2)' = 0,$$

that is

$$\overline{Z}_1 Z_1' - \overline{Z}_2 Z_2' = 0, \qquad I - (\overline{Z}_1^{-1} \overline{Z}_2) (Z_1^{-1} Z_2)' = 0,$$

is the homogeneous representation of a unitary matrix. We can generalize the idea a little further. Let

$$\mathfrak{F}_2 = \begin{pmatrix} I^{(n)} & 0 \\ 0 & -I^{(m)} \end{pmatrix}, \qquad n \geq m.$$

The matrix $\Gamma^{(m+n)}$ satisfying

 $\Gamma \mathfrak{F}_2 \Gamma' = \mathfrak{F}_2$

is called conjunctive with signature (n, m). The pair $(Z_1^{(n)}, Z_2^{(n,m)})$ of matrices satisfying

$$(\overline{Z}_1, \overline{Z}_2)\mathfrak{F}_2(Z_1, Z_2)' = 0$$

is called an (n, m)-unitary pair.

Instead of going into the details of this geometry we shall be content to make the following remark.

Let

$$W_1^{(n,m)} = Z_1^{-1} Z_2.$$

Then we have

$$\overline{W}_1 W_1' = I.$$

 W_1 is formed by *m* columns of a unitary matrix. Thus the geometry may be considered as a subgeometry of the geometry of unitary matrices by identifying the elements with the same *m* columns as an element of the subgeometry. This may be described in short as "the process of projection."

14. Remarks.

(i) The condition "one-to-one" is redundant, since the invariance of arithmetic distance implies it.

(ii) The continuity for the real case is also very probably redundant. (Cf. Sierpinski's contribution to the solution of the functional equation f(x+y) = f(x)+f(y).)

(iii) The geometry of pairs of matrices $(Z_1^{(n)}, Z_2^{(n,m)})$ with the group given in IV has interesting applications to the study of automorphic functions. It is *not* an analogue of projective geometry but of non-Euclidean geometry.

(iv) Analogous to IV, we may establish a geometry of real rectangular matrices.

Finally the author should like to express his warmest thanks to the referee for his help with the manuscript.

NATIONAL TSING HUA UNIVERSITY, KUNMING, YUNNAN, CHINA.

1945]