

GEOMETRIES OF MATRICES. II. STUDY OF INVOLUTIONS IN THE GEOMETRY OF SYMMETRIC MATRICES

BY
LOO-KENG HUA

1. Introduction. The paper contains a detailed study of the involutions in the geometry of symmetric matrices over the complex field. It is one of the aims of the paper to establish the following theorem:

A topological automorphism of the group formed by the symplectic transformations is either an inner automorphism or an anti-symplectic transformation.

More precisely, we identify two symplectic matrices \mathfrak{T} and $-\mathfrak{T}$ as a symplectic transformation \mathfrak{T}_0 . A continuous automorphism of the group formed by \mathfrak{T}_0 is either of the form $\mathfrak{P}_0 \mathfrak{T}_0 \mathfrak{P}_0^{-1}$ or $\mathfrak{P}_0 \mathfrak{T}_0^* \mathfrak{P}_0^{-1}$, where \mathfrak{P}_0 denotes a symplectic transformation and \mathfrak{T}_0^* is the conjugate complex of \mathfrak{T}_0 .

The following result, which can also be derived from Mohr's results⁽¹⁾ on the representations of the symplectic group, can be obtained as an immediate consequence of our present theorem: Every topological automorphism of the group formed by all symplectic matrices (that is, we do not identify \mathfrak{T} and $-\mathfrak{T}$) is either an inner automorphism or the conjugate complex of an inner automorphism. Actually, by means of the method used in the paper, an independent proof of this result can be obtained which is much simpler than that of the first theorem, since the distinction between involutions of the first and the second kind now is apparent.

In the course of our discussion, we find the explicit normal forms of involutions and anti-involutions. The manifold of the fixed points of all sorts of involutions has also been determined completely.

As an introduction, several types of geometries keeping an involution or an anti-involution as absolute have been enumerated. Those obtained from anti-involutions are generalizations of non-Euclidean geometries and those obtained from involutions give us several new types of geometries, whose real analogy (which will be given elsewhere later) is a generalization of Möbius geometry of circles.

Furthermore, the author shows that every symplectic transformation is a product of *two* involutions and *four* anti-involutions, and that for $n=2^\sigma\tau$, τ odd, in the space of symmetric matrices of order n , we have at most $\sigma+3$ pairs of points of which any two pairs separate each other harmonically.

Presented to the Society, December 29, 1946; received by the editors February 27, 1946,

⁽¹⁾ Göttingen Dissertation, 1933. The author is indebted to the referee for this reference, but unfortunately it is not available in China.

Algebraically speaking, the last result is equivalent to the following one: let $\mathfrak{T}_1, \dots, \mathfrak{T}_s$ be symplectic matrices of order $2n$ satisfying

$$\mathfrak{T}_i^2 = -\mathfrak{J}, \quad \mathfrak{T}_i \mathfrak{T}_j = -\mathfrak{T}_j \mathfrak{T}_i$$

where \mathfrak{J} denotes the $2n$ -rowed identity. Then $s \leq \sigma + 3$ and this maximum is attained. As a by-product the author establishes also that if S_1, \dots, S_s are n -rowed symmetric matrices satisfying $S_i^2 = -I$, $S_i S_j = -S_j S_i$, then $s \leq \sigma + 1$. In case of skew symmetric matrices, we have $s \leq \sigma$. These maximums are all attained.

As in I⁽²⁾, capital latin letters denote $n \times n$ matrices unless the contrary is stated. On the other hand, we use $M^{(l,m)}$ to denote an $l \times m$ matrix and $M^{(m)} = M^{(m,m)}$. I and 0 denote the identity and zero matrices respectively. We use also

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

which are $2n$ -rowed matrices. p and q denote two integers satisfying $p+q=n$.

2. Classification of involutions. First of all we identify the transformations which have the same effect in the space of symmetric matrices.

THEOREM 1. *In the space of symmetric matrices (in homogeneous coordinates), two substitutions*

$$(1) \quad Q(W_1, W_2) = (Z_1, Z_2)\mathfrak{T},$$

and

$$(2) \quad Q_0(W_1, W_2) = (Z_1, Z_2)\mathfrak{F}_0$$

induce the same mapping of the space, if and only if

$$(3) \quad \mathfrak{T} = \pm \mathfrak{F}_0.$$

In particular, (1) carries every point of the space into itself, if and only if

$$\mathfrak{T} = \pm \mathfrak{J}.$$

Proof. It is sufficient to establish the second part of the theorem. Putting $Z_1=0$, we have, by the supposition, $W_1=0$. Hence $C=0$, if we put

$$(4) \quad \mathfrak{T} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Similarly, putting $Z_2=0$, we find $B=0$. Now the transformation becomes

$$W = AZA'$$

(*) The first paper of the series will be referred to as I (Trans. Amer. Math. Soc. vol. 57 (1945) pp. 441–481).

in the nonhomogeneous coordinate system. By the assumption,

$$(5) \quad Z = AZA'$$

holds for all Z , consequently $A = \pm I$.

From Theorem 1, we deduce at once the following theorem.

THEOREM 2. *A symplectic transformation*

$$Q(W_1, W_2) = (Z_1, Z_2)\mathfrak{T}, \quad \mathfrak{T} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is an involution if and only if

$$(6) \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \pm \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix},$$

that is, $\mathfrak{T}\mathfrak{T}$ is either skew symmetric or symmetric according as $\mathfrak{T}^2 = \mathfrak{J}$ or $-\mathfrak{J}$.

By an involution, we understand a symplectic transformation whose square induces the identity mapping. Similarly, we define an anti-involution as an anti-symplectic mapping whose square induces the identity mapping.

THEOREM 3. *An anti-symplectic transformation*

$$(7) \quad Q(W_1, W_2) = (\bar{Z}_1, \bar{Z}_2)\mathfrak{T}, \quad \mathfrak{T} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is an anti-involution, if and only if

$$(8) \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix}^* = \pm \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix},$$

that is, $\mathfrak{T}\mathfrak{T}^$ is either a skew Hermitian or an Hermitian matrix according as $\mathfrak{T}\mathfrak{T}^* = \mathfrak{J}$ or $-\mathfrak{J}$.*

Proof. From (7) and

$$(9) \quad Q^*(Z_1, Z_2) = (\bar{P}_1, \bar{P}_2)\mathfrak{T},$$

we have

$$\bar{Q}^*Q(W_1, W_2) = (P_1, P_2)\mathfrak{T}^*\mathfrak{T}.$$

This represents the identical mapping, if and only if $\mathfrak{T}^*\mathfrak{T} = \pm \mathfrak{J}$. Further, since \mathfrak{T} is symplectic, that is $\mathfrak{T}\mathfrak{T}' = \mathfrak{J}$, we have

$$\mathfrak{T}^*\mathfrak{J} = \mathfrak{T}^*(\mathfrak{T}\mathfrak{T}') = \pm \mathfrak{J}\mathfrak{T}' = \mp (\mathfrak{T}^*\mathfrak{T})^*.$$

The theorem is now evident.

DEFINITION 1. The involutions satisfying $\mathfrak{T}^2 = \mathfrak{J}$ are called *involutions of*

the first kind and those satisfying $\mathfrak{T}^2 = -\mathfrak{J}$ are called *involutions of the second kind*.

DEFINITION 2. The anti-involutions satisfying $\mathfrak{T}\mathfrak{T}^* = \mathfrak{J}$ are called *anti-involutions of the first kind* and those satisfying $\mathfrak{T}\mathfrak{T}^* = -\mathfrak{J}$ are called *anti-involutions of the second kind*.

3. Normal form of involutions. Suppose that \mathfrak{T} is an involution of the first kind. By Theorem 2, $\mathfrak{T}\mathfrak{F}$ is skew symmetric. Now we consider the pair of skew symmetric matrices $(\mathfrak{T}\mathfrak{F}, \mathfrak{F})$. The elementary divisors of the matrix $\mathfrak{T}\mathfrak{F} - \lambda\mathfrak{F} = (\mathfrak{T} - \lambda\mathfrak{J})\mathfrak{F}$ are those of $\mathfrak{T} - \lambda\mathfrak{J}$. Since $\mathfrak{T}^2 = \mathfrak{J}$, the elementary divisors are all simple and the characteristic roots are ± 1 . Since the determinant of \mathfrak{T} is equal to 1, the multiplicity of the root -1 is even. The pair of skew symmetric matrices

$$\left(\begin{pmatrix} 0 & H \\ -H & 0 \end{pmatrix}, \mathfrak{F} \right), \quad H = [1, \dots, 1, -1, \dots, -1]$$

has the same elementary divisors as the pair of matrices $(\mathfrak{T}\mathfrak{F}, \mathfrak{F})$. Here H is a diagonal matrix with p terms 1 and q terms -1 . Hence we have a matrix \mathfrak{P} such that

$$\mathfrak{P}(\mathfrak{T}\mathfrak{F}, \mathfrak{F})\mathfrak{P}' = \left(\begin{pmatrix} 0 & H \\ -H & 0 \end{pmatrix}, \mathfrak{F} \right).$$

Thus \mathfrak{P} is symplectic, and

$$\mathfrak{P}\mathfrak{T}\mathfrak{P}^{-1} = -\mathfrak{P}\mathfrak{T}\mathfrak{F}\mathfrak{P}'\mathfrak{F} = -\begin{pmatrix} 0 & H \\ -H & 0 \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix},$$

which gives the transformation

$$(10) \quad W = HZH.$$

Therefore we have the following theorem.

THEOREM 4. *Every involution of the first kind is equivalent to (10) symplectically, where H is a diagonal matrix with p positive 1's and q negative 1's and $p \leqq q$. Further, no two of these involutions are equivalent.*

The last sentence can be justified by considering the multiplicity of the characteristic root 1 of the symplectic matrix.

DEFINITION 3. This involution is said to be of *signature* (p, q) .

Now we consider an involution \mathfrak{T} of the second kind. Then we have a pair of matrices $(\mathfrak{T}\mathfrak{F}, \mathfrak{F})$; the first matrix is symmetric and the second skew symmetric. The characteristic roots of \mathfrak{T} are $\pm i$ and the elementary divisors are all simple. Let⁽³⁾ $d(\mathfrak{T} - \lambda\mathfrak{J}) = f(\lambda)$. Since $\mathfrak{T}\mathfrak{F} = \mathfrak{F}\mathfrak{T}'^{-1}$, we have

(3) $d(X)$ denotes the determinant of the matrix X .

$$\begin{aligned} f(\lambda) &= d(\mathfrak{T} - \lambda \mathfrak{J})d(\mathfrak{J}) = d(\mathfrak{J}\mathfrak{T}'^{-1} - \lambda \mathfrak{J}) \\ &= \lambda^{2n}d\left(\mathfrak{T}' - \frac{1}{\lambda} \mathfrak{J}\right) = \lambda^{2n}f\left(\frac{1}{\lambda}\right). \end{aligned}$$

Hence the multiplicities of the characteristic roots i and $-i$ are equal.

Since

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

has the same elementary divisors as $\mathfrak{T}\mathfrak{J} - \lambda \mathfrak{J}$, we have a symplectic matrix \mathfrak{P} carrying \mathfrak{T} into

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

which corresponds to the transformation

$$(11) \quad W = -Z^{-1}.$$

Hence, we have the following theorem.

THEOREM 5. *Every involution of the second kind is equivalent to (11) symplectically.*

Remarks. 1. For $n=1$, no involution of the first kind exists.

2. The following normal form of an involution of the second kind is sometimes useful:

$$(12) \quad W = -Z.$$

3. In the case $n=2p$, we sometimes use

$$(13) \quad W = \begin{pmatrix} 0 & I^{(p)} \\ I^{(p)} & 0 \end{pmatrix} Z \begin{pmatrix} 0 & I^{(p)} \\ I^{(p)} & 0 \end{pmatrix}$$

as the normal form of an involution of the signature (p, p) .

Evidently, two symplectic transformations with matrices \mathfrak{T}_1 and \mathfrak{T}_2 are commutative if and only if

$$(14) \quad \mathfrak{T}_1 \mathfrak{T}_2 = \pm \mathfrak{T}_2 \mathfrak{T}_1.$$

Consequently, we see that the product of two commutative involutions \mathfrak{T}_1 and \mathfrak{T}_2 of the first kind is an involution either of the first kind or of the second kind according as $\mathfrak{T}_1 \mathfrak{T}_2 = \mathfrak{T}_2 \mathfrak{T}_1$ or $\mathfrak{T}_1 \mathfrak{T}_2 = -\mathfrak{T}_2 \mathfrak{T}_1$. In particular, for n even, $n=2p$, say, (11) may be regarded as a product of two involutions of the first kind:

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

and

$$W = - \begin{pmatrix} 0 & I^{(p)} \\ -I & 0 \end{pmatrix} Z^{-1} \begin{pmatrix} 0 & I^{(p)} \\ I & 0 \end{pmatrix}.$$

For n odd, such a decomposition does not exist.

Further, any involution of the first kind is a product of involutions of the first kind of the signature $(1, n-1)$, which are called *fundamental involutions*.

4. Equivalence of anti-involutions. A little attention should be paid to the equivalence of anti-symplectic transformations. Let $(W_1, W_2) = Q(\bar{Z}_1, \bar{Z}_2)\mathfrak{T}$. From $(U_1, U_2) = Q_1(Z_1, Z_2)\mathfrak{P}$, $(V_1, V_2) = Q_2(W_1, W_2)\mathfrak{P}$, we have

$$(V_1, V_2) = Q_2(W_1, W_2)\mathfrak{P} = Q_2Q(\bar{Z}_1, \bar{Z}_2)\mathfrak{T}\mathfrak{P} = Q_2Q\bar{Q}_1^{-1}(U_1, U_2)\mathfrak{P}^{*-1}\mathfrak{T}\mathfrak{P}.$$

Thus we have the following definition.

DEFINITION. Two anti-symplectic transformations with matrices \mathfrak{T}_1 and \mathfrak{T}_2 are said to be equivalent, if there exists a symplectic matrix \mathfrak{P} such that

$$(15) \quad \mathfrak{P}^{*-1}\mathfrak{T}_1\mathfrak{P} = \mathfrak{T}_2.$$

Notice that if (U_1, U_2) and (Z_1, Z_2) (and (V_1, V_2) and (W_1, W_2)) are related anti-symplectically, then we have $\mathfrak{P}^{*-1}\mathfrak{T}_1^*\mathfrak{P} = \mathfrak{T}_2$ instead of (15).

5. Relation between anti-involutions and hypercircles and the normal form of the anti-involution. Let \mathfrak{H} be an Hermitian matrix. The points (Z_1, Z_2) of the space for which

$$(16) \quad (Z_1, Z_2)\mathfrak{H}(\bar{Z}_1, \bar{Z}_2)'$$

is positive definite form a hypercircle. \mathfrak{H} is called the matrix of the hypercircle. The skew matrix

$$(17) \quad \mathfrak{H}'\mathfrak{H}\mathfrak{H}$$

is called the discriminantal matrix of \mathfrak{H} .

For an anti-involution of the first kind \mathfrak{T} , we have a hypercircle with the matrix

$$(18) \quad i\mathfrak{T}\mathfrak{F},$$

in fact, since \mathfrak{T} is symplectic, $i\mathfrak{T}\mathfrak{F} = i\mathfrak{F}\mathfrak{T}'^{-1} = i\mathfrak{F}\mathfrak{T}^* = (i\mathfrak{T}\mathfrak{F})^*$; and for an anti-involution of the second kind \mathfrak{T} , we have a hypercircle

$$(19) \quad \mathfrak{T}\mathfrak{F}.$$

Their discriminantal matrices are, respectively,

$$(i\mathfrak{T}\mathfrak{F})'\mathfrak{F}(i\mathfrak{T}\mathfrak{F}) = \mathfrak{F}^3 = -\mathfrak{F}$$

and

$$(\mathfrak{T}\mathfrak{F})'\mathfrak{F}(\mathfrak{T}\mathfrak{F}) = -\mathfrak{F}^3 = \mathfrak{F}.$$

THEOREM 6. *To each hypercircle with discriminantal matrix $-\mathfrak{F}$ or \mathfrak{F} , there corresponds an anti-involution of the first and the second kind respectively.*

Proof. (1) Let \mathfrak{H} be an Hermitian matrix satisfying $\mathfrak{H}'\mathfrak{F}\mathfrak{H} = -\mathfrak{F}$. Let

$$\mathfrak{T} = i\mathfrak{H}\mathfrak{F}.$$

Then

$$\mathfrak{T}'\mathfrak{F}\mathfrak{T} = \mathfrak{F}\mathfrak{H}'\mathfrak{F}\mathfrak{H}\mathfrak{F} = -\mathfrak{F}^3 = \mathfrak{F},$$

and

$$\mathfrak{T}^*\mathfrak{T} = -i\mathfrak{H}^*\mathfrak{F}i\mathfrak{H}\mathfrak{F} = -\mathfrak{F}^2 = \mathfrak{J}.$$

Hence \mathfrak{T} is a symplectic matrix and we have an anti-involution of the first kind.

(2) If $\mathfrak{H}'\mathfrak{F}\mathfrak{H} = \mathfrak{F}$, set $\mathfrak{T} = -\mathfrak{H}\mathfrak{F}$. We obtain consequently

$$\mathfrak{T}'\mathfrak{F}\mathfrak{T} = -\mathfrak{F}\mathfrak{H}'\mathfrak{F}\mathfrak{H}\mathfrak{F} = -\mathfrak{F}^3 = \mathfrak{F},$$

$$\mathfrak{T}^*\mathfrak{T} = \mathfrak{H}\mathfrak{F}\mathfrak{H}\mathfrak{F} = -\mathfrak{J},$$

that is, \mathfrak{T} defines an anti-involution of the second kind.

Further, from $\mathfrak{P}^*\mathfrak{T}\mathfrak{P}^{-1} = \mathfrak{T}_1$, we have

$$\mathfrak{P}^*\mathfrak{T}\mathfrak{F}\mathfrak{P}' = \mathfrak{P}^*\mathfrak{T}\mathfrak{P}^{-1}\mathfrak{F} = \mathfrak{T}_1\mathfrak{F}.$$

Therefore, in order to classify anti-involutions, we have to classify their corresponding hypercircles.

Since

$$\mathfrak{H}'\mathfrak{F}\mathfrak{H} - \lambda\mathfrak{F} = \pm\mathfrak{F} - \lambda\mathfrak{F}$$

has characteristic roots either all $+1$ or all -1 and has simple elementary divisors, we have⁽⁴⁾ a symplectic matrix \mathfrak{P} such that

$$\mathfrak{P}^*\mathfrak{H}\mathfrak{P}' = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$$

where H_1 is a diagonal matrix with p terms 1 and q terms -1 .

Since the discriminantal matrix is $\pm\mathfrak{F}$, we have then

$$H_1'H_2 = -I, \quad H_2'H_1 = -I$$

for anti-involutions of the first kind, and

$$H_1'H_2 = I, \quad H_2'H_1 = I$$

for anti-involutions of the second kind.

Thus, for anti-involutions of the first kind, the hypercircle is symplectically conjunctive to⁽⁵⁾

(4) See the author's paper, *On the theory of automorphic functions of a matrix variable*, II, Amer. J. Math. vol. 66 (1944) pp. 531-563.

(5) Two Hermitian matrices H and K are said to be conjunctive, if there exists a matrix A such that $\bar{A}HA' = K$.

$$(20) \quad \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$$

and for the second kind, it is symplectically conjunctive to

$$(21) \quad \begin{pmatrix} H_1 & 0 \\ 0 & H_1 \end{pmatrix}.$$

Therefore, we have the following theorem.

THEOREM 7. *An anti-involution of the first kind is equivalent to*

$$(22) \quad W = \bar{Z}^{-1}$$

and an anti-involution of the second kind is equivalent to

$$(23) \quad W = -H\bar{Z}^{-1}H,$$

where H denotes a diagonal matrix with p terms 1 and q terms -1 , $p \leq q$.

We may also prove that they are all non-equivalent, since their hyper-circles are non-equivalent.

An anti-involution, equivalent to (23), is called an *anti-involution of signature (p, q)* .

Remark. (22) is equivalent to

$$(24) \quad W = -\bar{Z}.$$

In the case $p=q$, (23) is equivalent to

$$(25) \quad W = \begin{pmatrix} 0 & I^{(p)} \\ -I & 0 \end{pmatrix} \bar{Z} \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}.$$

6. Decomposition of involutions into anti-involutions. Now we are going to express involution as product of anti-involutions.

THEOREM 8. *Every involution is a product of two commutative anti-involutions of the first kind.*

Before proving Theorem 8, we give the following rules concerning the multiplication of anti-symplectic transformations.

(1) The product of two anti-symplectic transformations with matrices \mathfrak{T}_1 and \mathfrak{T}_2 is a symplectic transformation with matrix $\mathfrak{T}_1^*\mathfrak{T}_2$.

(2) They are commutative if and only if $\mathfrak{T}_1^*\mathfrak{T}_2 = \pm \mathfrak{T}_2^*\mathfrak{T}_1$.

Proof of Theorem 8. (1) Let

$$\mathfrak{T}_1 = \begin{pmatrix} 0 & iI \\ iI & 0 \end{pmatrix}, \quad \mathfrak{T}_2 = \begin{pmatrix} 0 & H_i \\ H_i & 0 \end{pmatrix}.$$

Then

$$\mathfrak{T}_2^* \mathfrak{T}_1 = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \mathfrak{T}_1^* \mathfrak{T}_2,$$

which corresponds to the involution $W=HZH$ of the first kind. Further $\mathfrak{T}_1^* \mathfrak{T}_1 = \mathfrak{T}_2^* \mathfrak{T}_2 = \mathfrak{J}$, hence \mathfrak{T}_1 and \mathfrak{T}_2 represent two anti-involutions of the first kind.

(2) Let

$$\mathfrak{T}_1 = \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix}, \quad \mathfrak{T}_2 = \begin{pmatrix} 0 & Ii \\ Ii & 0 \end{pmatrix}.$$

Then $\mathfrak{T}_1^* \mathfrak{T}_1 = \mathfrak{T}_2^* \mathfrak{T}_2 = \mathfrak{J}$. Further

$$\mathfrak{T}_2^* \mathfrak{T}_1 = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix} = -\mathfrak{T}_1^* \mathfrak{T}_2$$

which corresponds to the involution $Z_1 = -Z^{-1}$ of the second kind.

THEOREM 9. *Every anti-involution of the second kind is a product of three mutually commutative anti-involutions of the first kind.*

Proof. The anti-involution of the second kind

$$Z_1 = -H\bar{Z}^{-1}H$$

is a product of $Z_1 = -Z_2^{-1}$ and $Z_2 = H\bar{Z}H$, and the former one is a product of two anti-involutions of the first kind:

$$Z_1 = -\bar{Z}_3, \quad Z_3 = \bar{Z}_2^{-1}.$$

The three anti-involutions so obtained are evidently mutually commutative.

Remark. Theorems 8 and 9 (and later Theorem 10) suggest that anti-involutions of the first kind can be used as generators in the group of symplectic and anti-symplectic transformations. Does the anti-involution of the second kind play the same role? The answer seems to be negative. In fact, an involution of the second kind cannot be decomposed into a product of two anti-involutions of the second kind. Let \mathfrak{T} be an involution of the second kind. Suppose the contrary, that is, suppose that we have two anti-involutions \mathfrak{T}_1 and \mathfrak{T}_2 of the second kind such that $\mathfrak{T} = \mathfrak{T}_1^* \mathfrak{T}_2$. Then, we have

$$-\mathfrak{J} = \mathfrak{T}^2 = (\mathfrak{T}_1^* \mathfrak{T}_2)(\mathfrak{T}_1^* \mathfrak{T}_2),$$

that is,

$$(26) \quad \mathfrak{T}_2 \mathfrak{T}_1^* = -\mathfrak{T}_1 \mathfrak{T}_2^*.$$

Now, we are going to show that, in particular, for $\mathfrak{T}_1 = \mathfrak{J}$ we have no \mathfrak{T}_2 satisfying this condition. (Notice that no generality is lost.) From

$$\mathfrak{T}_2 \mathfrak{J} = -\mathfrak{J} \mathfrak{T}_2^*,$$

and (by Theorem 3) $\mathfrak{T}_2\mathfrak{J} = (\mathfrak{T}_2\mathfrak{J})^{*'} = -\mathfrak{J}\mathfrak{T}_2^*$, we deduce that \mathfrak{T}_2 is symmetric. Further, the equation

$$\mathfrak{T}_2\mathfrak{T}_2^{*'} = \mathfrak{T}_2\mathfrak{T}_2^* = -\mathfrak{J}$$

is impossible, since the matrix on the left is a positive definite Hermitian matrix, while the matrix on the right is negative definite.

7. Decomposition of symplectic transformations into involutions. First of all we give the normal form of a symplectic matrix \mathfrak{T} . We have a symplectic matrix \mathfrak{P} such that $\mathfrak{P}^{-1}\mathfrak{T}\mathfrak{P}$ is a direct sum of symplectic transformations of the forms

$$(27) \quad W^{(\sigma)} = J_{\pm 1}^{(\sigma)} Z^{(\sigma)} J_{\pm 1}^{(\sigma)*} + S^{(\sigma)}$$

and

$$(28) \quad W^{(\tau)} = J_{\alpha}^{(\tau)} Z^{(\tau)} J_{\alpha}^{(\tau)*}, \quad \alpha \neq \pm 1, \tau \text{ odd},$$

where

$$J_{\alpha}^{(\tau)} = \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 1 & \alpha & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \alpha \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

By a direct sum of two symplectic transformations with matrices

$$\begin{pmatrix} A^{(\sigma)} & B_1 \\ C_1 & D_1 \end{pmatrix}, \quad \begin{pmatrix} A_2^{(\tau)} & B_2 \\ C_2 & D_2 \end{pmatrix}$$

we mean a symplectic transformation with the $2(\sigma+\tau)$ -rowed matrix

$$\begin{pmatrix} (A_1 \ 0) (B_1 \ 0) \\ (0 \ A_2) (0 \ B_2) \\ (C_1 \ 0) (D_1 \ 0) \\ (0 \ C_2) (0 \ D_2) \end{pmatrix}.$$

This result, according to valuable information from Professor H. Weyl, is due to Williamson; however, it was also proved by the author independently. Since Williamson's paper is not available in China, the author is obliged to give the preceding result without a necessary quotation.

THEOREM 10. *Every symplectic transformation is a product of two involutions of the second kind; consequently, every symplectic transformation is a product of four anti-involutions of the first kind.*

Proof. (1) Let

$$J = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}, \quad \mathfrak{P} = \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}.$$

Evidently, \mathfrak{P} is an involution of the second kind. Let

$$\mathfrak{T} = \begin{pmatrix} J_\alpha & 0 \\ 0 & J_\alpha'^{-1} \end{pmatrix}.$$

Then

$$(\mathfrak{T}\mathfrak{P})^2 = \begin{pmatrix} 0 & J_\alpha J \\ -J_\alpha'^{-1} J & 0 \end{pmatrix}^2 = -I,$$

since $J_\alpha J = JJ_\alpha'$. Thus \mathfrak{T} is a product of two involutions of the second kind.

(2) Next we consider the case

$$(29) \quad \mathfrak{T} = \begin{pmatrix} J_1 & SJ_1'^{-1} \\ 0 & J_1'^{-1} \end{pmatrix}.$$

Let

$$(30) \quad M^{(n)} = M = (m_{ij}), \quad m_{ij} = \begin{cases} (-1)^{i-1} \binom{i-1}{j-1} & \text{for } i \geq j, \\ 0 & \text{for } i < j, \end{cases}$$

and $M^2 = (t_{ij})$. Then, by (30),

$$t_{ij} = \sum_{h=1}^m m_{ih} m_{hj} = (-1)^{i-1} \sum_{i \leq k \leq j} (-1)^{k-1} \binom{i-1}{k-1} \binom{k-1}{j-1} = \begin{cases} 0 & \text{for } i \neq j, \\ 1 & \text{for } i = j. \end{cases}$$

Therefore, we have

$$(31) \quad M^2 = I.$$

Consequently, the matrix

$$\mathfrak{P} = \begin{pmatrix} iM & 0 \\ 0 & -iM' \end{pmatrix}$$

denotes an involution of the second kind. We may verify directly that

$$J_1 M^{(n)} = \begin{pmatrix} 1 & 0 \\ 0 & -M^{(n-1)} \end{pmatrix}.$$

Thus

$$\mathfrak{T}\mathfrak{P} = i \begin{pmatrix} J_1 M & -S J_1'^{-1} M' \\ 0 & -J_1'^{-1} M' \end{pmatrix}$$

is also an involution of the second kind, since $S = J_1 M S M' J_1'$.

(3) Similarly we treat the case

$$\begin{pmatrix} J_{-1} & S J_{-1}'^{-1} \\ 0 & J_{-1}'^{-1} \end{pmatrix}.$$

On account of the result quoted at the beginning of the section, we have the theorem.

8. Geometries induced by anti-involutions. The results of sections 8, 9, 10, 11 and 12 can be used to introduce several types of geometry; the detailed study will be given elsewhere.

We take an anti-involution \mathfrak{J} of the first kind as an absolute. The group G formed by all symplectic transformations \mathfrak{T} commutative with \mathfrak{J} is called the group of motion. Correspondingly, we have a hypercircle with the matrix $i\mathfrak{J}\mathfrak{F}$. The group of transformations \mathfrak{T} with $\mathfrak{T}\mathfrak{J} = \mathfrak{J}\mathfrak{T}^*$ form a subgroup G_1 whose index in G is equal to 2.

In fact, from

$$\mathfrak{T}_1 \mathfrak{J} = \mathfrak{J} \mathfrak{T}_1^*$$

and

$$\mathfrak{T}_2 \mathfrak{J} = \mathfrak{J} \mathfrak{T}_2^*$$

we deduce $\mathfrak{T}_1 \mathfrak{T}_2 \mathfrak{J} = \mathfrak{T}_1 \mathfrak{J} \mathfrak{T}_2^* = \mathfrak{J} \mathfrak{T}_1 \mathfrak{T}_2^*$.

As the transformation

$$(32) \quad (W_1, W_2) = Q(Z_1, Z_2) \mathfrak{T}$$

of G_1 carries

$$(33) \quad (Z_1, Z_2) i\mathfrak{J}\mathfrak{F}(Z_1, Z_2)^*$$

into

$$Q(W_1, W_2) i\mathfrak{T} \mathfrak{J} \mathfrak{F} \mathfrak{T}^* (W_1, W_2)^* \bar{Q}' = Q(W_1, W_2) i\mathfrak{J}\mathfrak{F}(W_1, W_2)^* \bar{Q}'$$

for \mathfrak{T} belonging to G_1 , the rank and signature of the Hermitian matrix (33) classify the points of the space into transitive sets. This statement will be proved in the remark of the next section.

Now we take the set of points for which (33) is positive definite. This set is called a *hyperbolic space*. The corresponding geometry is called a *hyperbolic geometry of symmetric matrices*. By Theorem 7, we find that, apart from equivalence, there is one and only one type of hyperbolic geometry. The group G_1 is called the group of motion of the space.

Let P_1 and P_2 be two points of the hyperbolic space. Every motion evidently carries the cross-ratio matrix

$$(34) \quad \begin{aligned} \{P_1, P_2\} &= (P_1, \mathfrak{J}(P_1), P_2, \mathfrak{J}(P_2)) \\ &= (P_1 - P_2)(P_1 - \mathfrak{J}(P_2))^{-1}((\mathfrak{J}(P_1) - P_2)(\mathfrak{J}(P_1) - \mathfrak{J}(P_2))^{-1})^{-1} \end{aligned}$$

into a similar matrix. (34) is called the *distance-matrix* between two points. We have the following theorems.

THEOREM 11. *The hyperbolic space is transitive.*

THEOREM 12. *The distance matrix has simple elementary divisors and positive characteristic roots. Two point-pairs are equivalent if and only if their distance matrices have the same characteristic roots (multiplicities are counted).*

THEOREM 13. *The space is symmetric.*

By a symmetric space, we mean that to each point of the space there exists an involution with the point as its isolated fixed point and that every transformation of the space having the point as fixed point is commutative with the involution.

The proof of these three theorems will be given in the next section.

9. Visualization of the hyperbolic geometry. For the sake of concreteness, we take (cf. (24))

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

The hypercircle is now formed by those points $Z = X + iY$ where X and Y are real and Y is positive definite. The group G_1 is formed by the symplectic transformations

$$(35) \quad W = (AZ + B)(CZ + D)^{-1},$$

where

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

is real. This is Siegel's generalization of the Poincaré half-plane.

Sometimes we take, by Theorem 7,

$$\mathfrak{J} = i \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

The space is formed by those points for which $I - ZZ^*$ is positive definite. The group of motions consists of the transformations

$$(36) \quad W = (AZ + B)(\bar{B}Z + \bar{A})^{-1}.$$

This is a generalization of the unit circle in the complex plane.

Theorem 11 is evident, since any point $P = Q + iR$ with positive definite R may be carried into iR by the transformation $W = Z - Q$ of (35) and since there exists a real matrix C such that $CRC' = I$, then $W = C^{-1}ZC'^{-1}$ carries iR into iI .

To prove Theorem 12, we use the second representation. We may take one of the points to be zero. Then $\{Z, 0\} = (Z, \bar{Z}^{-1}, 0, \infty) = Z\bar{Z}$, which is positive definite. We have a unitary matrix U such that

$$UZ\bar{Z}U' = [\lambda_1^2, \dots, \lambda_n^2], \quad \lambda_r \geq 0,$$

and

$$UZU' = [\lambda_1, \dots, \lambda_n].$$

This gives Theorem 12.

The space is transitive. In order to prove Theorem 13, we have to show that there exists one and only one involution which has 0 as its isolated fixed point and that the subgroup leaving 0 invariant is commutative with it.

The transformation leaving 0 invariant carries also ∞ into itself. Then it takes the form

$$(37) \quad W = AZA'.$$

(37) denotes an involution if and only if $A^2 = \pm I$. The equation $Z = AZA'$ has no other solution but zero if and only if the characteristic roots of the second power matrix of A are different from 1. Further the roots of A are ± 1 and $\pm i$; the only possibility is that $A = \pm iI$ by Theorem 44.4 of MacDuffee⁽⁶⁾. Now we have the unique involution

$$(38) \quad W = -Z.$$

It is evidently commutative with all transformations (37).

Remark. In order to prove the promised statement of the preceding section, it is sufficient to prove that the points

$$X + Yi, \quad X, Y \text{ real},$$

are classified into transitive sets according to the ranks and signatures of Y . This is evident, since $Z_1 = Z - X$ carries the point into Yi and $Z_1 = AZA'$ carries Yi into a diagonal matrix of the form $i[1, \dots, 1, -1, \dots, -1, 0, \dots, 0]$.

10. **Elliptic geometries.** Now we take \mathfrak{J} to be an anti-involution of the second kind as an absolute. More definitely, we take

$$\mathfrak{J} = \begin{pmatrix} 0 & -H \\ H & 0 \end{pmatrix}$$

where

$$H = [1, \dots, 1, -1, \dots, 1],$$

where there are p 1's and q -1 's, $q \geq p$. The hypercircle has the matrix

$$\begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}.$$

(6) *Theory of matrices*, 1933.

The space is formed by the points for which

$$(39) \quad Z_1 H \bar{Z}_1' + Z_2 H \bar{Z}_2' = (Z_1, Z_2) \mathfrak{J} \mathfrak{F}(Z_1, Z_2)^*$$

is of the same signature as H . This geometry will be called the *elliptic geometry of signature* (p, q) . The group of motions is defined by the symplectic transformations

$$(40) \quad (Z_1, Z_2) = Q(W_1, W_2) \mathfrak{T},$$

with

$$(41) \quad \mathfrak{T} \mathfrak{J} = -\mathfrak{J} \mathfrak{T}^*,$$

since (40) carries (39) into

$$Q(W_1, W_2) \mathfrak{T} \mathfrak{J} \mathfrak{T}^*(W_1, W_2)' \bar{Q}' = Q(W_1, W_2) \mathfrak{J} \mathfrak{F}(W_1, W_2)^* \bar{Q}'.$$

In the case $p=q$, the transformations (40) with $\mathfrak{T} \mathfrak{J} = -\mathfrak{J} \mathfrak{T}^*$ instead of (41) also leave the space invariant. Then the group of motions is now constituted by both kinds of transformations.

From (41), we have

$$\mathfrak{T} = \begin{pmatrix} A & B \\ -H \bar{B} H & H \bar{A} H \end{pmatrix}.$$

THEOREM 14. *The space is transitive.*

Proof. For any point (A, B) of the space making $\bar{A} H A' + \bar{B} H B'$ of signature (p, q) we can find a matrix P such that

$$\bar{P}(\bar{A} H A' + \bar{B} H B') P' = H.$$

Then

$$(42) \quad \mathfrak{P} = \begin{pmatrix} PA & PB \\ -H \bar{P} \bar{B} H & H \bar{P} \bar{A} H \end{pmatrix}$$

is symplectic, in fact

$$PA(PB)' = PAB'P' = (PB)(PA)',$$

$$(-H \bar{P} \bar{B} H)(H \bar{P} \bar{A} H)' = (H \bar{P} \bar{A} H)(-H \bar{P} \bar{B} H)',$$

and

$$PA(H \bar{P} \bar{A} H)' - PB(H \bar{P} \bar{B} H)' = P(A \bar{H} A' + B \bar{H} B') \bar{P}' \cdot H = I.$$

The transformation $(Z_1, Z_2) = Q(W_1, W_2) \mathfrak{P}$ is a motion of the space, since

$$\mathfrak{P}^* \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \mathfrak{P}' = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix},$$

and it carries $(I, 0)$ into the point (A, B) .

The group of stability at the origin, that is, the subgroup of transforma-

tions leaving 0 invariant, consists of the transformations of the form

$$W = AZA',$$

where A is a conjunctive automorphism of H , that is, $\bar{A}HA' = H$. We may prove also the following theorem.

THEOREM 15. *The elliptic space of signature (p, q) is symmetric.*

As in §9, we may introduce the distance matrix between two points P_1 and P_2 by $\{P_1, P_2\} = (P_1, \mathfrak{J}(P_1), P_2, \mathfrak{J}(P_2))$. Putting $P_1 = Z$ and $P_2 = 0$, we have

$$(43) \quad \{Z, 0\} = ZH\bar{Z}H.$$

Here the problem arises to classify symmetric matrices Z under the group of conjunctive automorphisms of an Hermitian matrix. It would require too much space to solve this problem: hence at present we content ourselves with the special case $H = I$, which is the direct generalization of elliptic geometry.

THEOREM 16. *The distance matrix has simple elementary divisors and positive characteristic roots in the elliptic space of signature $(n, 0)$. Two point-pairs are equivalent if and only if their distance matrices have the same characteristic roots (multiplicities are counted).*

Notice that in the elliptic space of signature $(n, 0)$ the group of motions is formed by all unitary symplectic matrices.

11. Geometries induced by involutions. Now we take an involution \mathfrak{J} of the second kind as the absolute; without loss of generality we may take

$$(44) \quad W = -Z.$$

From

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix} = \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

we deduce that $B = C = 0$. Thus the transformations of the space are given by

$$(45) \quad Z_1 = AZA',$$

which form a group G_1 . If the involution $Z_1 = -Z^{-1}$ is adjoined to G_1 , a group G is obtained which contains G_1 as a subgroup of index 2. The geometry of the symmetric matrices under the group G_1 is equivalent to the algebraic problem "congruent classification of matrices." Evidently the space is not transitive. The rank of P is the characteristic invariant for a finite point.

For a pair of finite points P_1 and P_2 , we have $(P_1, P_2, 0, \infty) = P_1 P_2^{-1}$. Thus the elementary divisors of $P_1 P_2^{-1}$ characterize the equivalence of a pair of finite points.

Now we take an involution \mathfrak{J} of the first kind with signature (p, q) as

an absolute, for example

$$(46) \quad Z_1 = HZH.$$

Now the matrix \mathfrak{T} of the transformations satisfies

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Consequently we have

$$A = \begin{pmatrix} a_1^{(p)} & 0 \\ 0 & a_2^{(q)} \end{pmatrix}, \quad B = \begin{pmatrix} b_1^{(p)} & 0 \\ 0 & b_2^{(q)} \end{pmatrix}, \quad C = \begin{pmatrix} c_1^{(p)} & 0 \\ 0 & c_2^{(q)} \end{pmatrix}, \quad D = \begin{pmatrix} d_1^{(p)} & 0 \\ 0 & d_2^{(q)} \end{pmatrix}.$$

Then \mathfrak{T} may be considered as a direct product of two symplectic matrices

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

The group so formed is denoted by G_1 .

The equation

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = - \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

cannot hold, except when $p=q$, $n=2p$. Then we have a group G which is generated by G_1 and the additional transformation

$$W = \begin{pmatrix} 0 & I^{(p)} \\ I & 0 \end{pmatrix} Z \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

For simplicity's sake, we take $p=n-1$, $q=1$, that is, the absolute is a fundamental involution.

THEOREM 17. *The arithmetic distance of P and $\mathfrak{Z}(P)$ characterizes the equivalence of points. More definitely, every point is either equivalent to 0 or equivalent to*

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Proof. Let

$$P = \begin{pmatrix} P_1 & V' \\ V & P \end{pmatrix}, \quad P_1 = P_1^{(n-1)}.$$

Then

$$W = Z - \begin{pmatrix} P_1 & 0 \\ 0 & P \end{pmatrix}$$

carries P into

$$(47) \quad \begin{pmatrix} 0 & v' \\ v & 0 \end{pmatrix}.$$

If $v=0$, there is nothing to be proved. Otherwise, we have a matrix M such that $vM=(1, 0, \dots, 0)$, $M=M^{(n-1)}$. Then the transformation

$$W = \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix} Z \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$$

carries (47) into the required form.

The non-equivalence of the two points given in Theorem 17 is evident.

It is easy to extend the theorem for arbitrary ϕ and q .

Remarks. 1. The geometries so obtained are generalizations of the complex analogy of the Möbius geometry of circles. There is a particularly great variety of geometries over the real field.

2. We may take several commutative involutions as absolutes; for example, we take $W=-Z$, $W=Z^{-1}$ as absolutes, then the transformations take the form $W=\Gamma Z\Gamma'$, where Γ is an orthogonal matrix. Thus “the orthogonal classification of symmetric matrices” may be considered as the geometry of symmetric matrices with two absolutes.

3. To each involution \mathfrak{J} of the second kind, we have a symplectic symmetric matrix $\mathfrak{J}\mathfrak{F}$, and conversely. Thus, the geometry of symplectic symmetric matrices may be considered as a geometry of involutions of the second kind. In particular, for $n=1$, it gives the ordinary treatment of involutions in the complex plane. It may also be extended to the study of anti-involutions, and so on. But the author will not go into the detailed discussion of this problem.

12. **Laguerre's geometry of matrices.** The transformations

$$(48) \quad W = AZA' + S$$

form a subgroup, which leaves ∞ invariant. The geometry under this group is called *Laguerre's geometry of symmetric matrices*, or *affine geometry of symmetric matrices*.

THEOREM 18. *Finite points are transitive under the group. Two point-pairs are equivalent if and only if their arithmetic distances are the same.*

We may obtain invariants from the “projective” geometry of symmetric matrices by selecting a point to be infinity. For the discussion of the equivalence of the triples of points, we introduce a “simple ratio-matrix,” that is,

$$(X_1, X_2, X_3, \infty) = (X_1 - X_2)(X_3 - X_2)^{-1}.$$

Further, the transformations (48) with unitary A form a subgroup. The geometry under this group may be called the Euclidean geometry of symmetric matrices. The transformations (48) with A of determinant I form also a group. The corresponding geometry may be called the special Laguerre geometry.

13. Fixed points of an involution of the second kind. In §§13, 14 we determine the fixed points of involutions.

THEOREM 19. *An involution of the second kind has two isolated fixed points; they form a nonspecial pair, that is, a pair of points with arithmetic distance n . Conversely, a nonspecial pair of points determines uniquely an involution of the second kind having the points as its isolated fixed points.*

Proof. (1) It is sufficient to prove that $\pm iI$ are two isolated solutions of

$$(49) \quad Z^2 = -I.$$

If Z_0 is a non-scalar solution of (49), then $\Gamma Z_0 \Gamma'$ is also a solution for all orthogonal Γ . Thus Z_0 is not an isolated fixed point of $W = -Z^{-1}$.

If Z_0 is scalar, then $Z_0 = \pm iI$. From $(iI + \Delta)^2 = -I$ we have $\Delta(\Delta + 2iI) = 0$. For sufficiently small Δ , $\Delta + 2iI$ is nonsingular, consequently $\Delta = 0$. This establishes that $\pm iI$ are the two isolated fixed points.

(2) Conversely, let 0 and ∞ be two fixed points. Then the involution takes the form

$$W = AZA', \quad A^2 = -I.$$

Using this in connection with (37), we have $W = -Z$.

THEOREM 20. *Let P_1 and P_2 be two isolated fixed points of an involution of the second kind; all its fixed points X are given by*

$$(50) \quad r(P_1, X) + r(X, P_2) = n$$

and conversely⁽⁷⁾.

Proof. (1) All the solutions of (49) are given by

$$Z = \Gamma \begin{pmatrix} -I^{(p)}i & 0 \\ 0 & I^{(q)}i \end{pmatrix} \Gamma',$$

where Γ is orthogonal, since the elementary divisors of $Z - \lambda I$ are all simple. Further

$$r(Z, Ii) = r\left(\left(\begin{matrix} -I^{(p)}i & 0 \\ 0 & I^{(q)}i \end{matrix}\right), Ii\right) = p$$

and $r(-Ii, Z) = q$.

(7) $r(A, B)$ denotes the rank of $A - B$; it is called the arithmetic distance between A and B .

(2) Now we let

$$r(Z, iI) = p \quad \text{and} \quad r(Z, -iI) = q.$$

There exists a matrix Q such that

$$QZQ' = \sum' J_k^{(c_k)}, \quad QIQ' = \sum' J^{(c_k)}$$

where

$$J = \begin{pmatrix} 0 & 0 \cdots 0 & 1 \\ 0 & 0 \cdots 1 & 0 \\ \cdots & \cdots & \cdots \\ 1 & 0 \cdots 0 & 0 \end{pmatrix}, \quad J_k = \begin{pmatrix} 0 & \cdots & 0 & \lambda_k \\ 0 & \cdots & \lambda_k & 1 \\ \cdots & \cdots & \cdots \\ \lambda_k & \cdots & 0 & 0 \end{pmatrix}.$$

Direct verification shows that $C_k=1$ and that $d(Z-\lambda I)=0$ has i as root of multiplicity p and has $-i$ as root of multiplicity q . Thus we have an orthogonal Q such that

$$Z = Q \begin{pmatrix} I^{(p)}i & 0 \\ 0 & -I^{(q)}i \end{pmatrix} Q'.$$

THEOREM 21. Let P_1 and P_2 be two isolated fixed points of an involution of the second kind. Let X be a point satisfying $r(P_1, X) = r(P_2, X) = n$, and let X_0 be the image of X under the involution. Then P_1, P_2, X, X_0 form a harmonic range.

Proof. We may take $P_1=0$, $P_2=\infty$. Then $X_0=-X$. We have consequently $(P_1, P_2, X, X_0)=(0, \infty, X, -X)=-I$.

14. Fixed elements of an involution of the first kind. In order to determine the fixed elements of an involution of the first kind, we have to introduce the concept of decomposable subspace.

DEFINITION. A manifold in the space is said to form a *decomposable subspace of the type (p, q)* , if we have a symplectic transformation carrying the manifold to a manifold formed by the points of the form

$$(51) \quad \begin{pmatrix} Z_1^{(p)} & 0 \\ 0 & Z_2^{(q)} \end{pmatrix}, \quad p+q=n,$$

where Z_1 and Z_2 are called *components*.

THEOREM 22. Let $p+q=n$. The fixed points of an involution of signature (p, q) form a decomposable subspace of type (p, q) .

Proof. We write

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

and

$$Z = \begin{pmatrix} Z_{11}^{(p)} & Z_{12} \\ Z_{12}' & Z_{22}^{(q)} \end{pmatrix}.$$

Then

$$HZH - Z = \begin{pmatrix} 0 & -2Z_{12} \\ -2Z'_{12} & 0 \end{pmatrix} = 0$$

which implies $Z_{12}=0$. Thus we have the theorem.

Theorems 22 and 2 give us a general definition of decomposable subspace:

Let \mathfrak{K} be a skew symmetric symplectic matrix. The points (Z_1, Z_2) satisfying

$$(52) \quad (Z_1, Z_2)\mathfrak{K}(Z_1, Z_2)' = 0$$

define a decomposable space. It is of the type (p, q) , if $d(\mathfrak{K}-\lambda\mathfrak{F})=0$ has 1 and -1 as roots of multiplicity $2p$ and $2q$ respectively.

The justification is almost evident, since on multiplying $(W_1, W_2) = Q(Z_1, Z_2)\mathfrak{T}$ on the right by $\mathfrak{F}(Z_1, Z_2)'$, we obtain

$$(W_1, W_2)\mathfrak{F}(Z_1, Z_2)' = Q(Z_1, Z_2)\mathfrak{K}(Z_1, Z_2)'.$$

(Notice that (Z_1, Z_2) and (W_1, W_2) denote the same point, if and only if $(Z_1, Z_2)\mathfrak{F}(W_1, W_2)'=0$.)

Further we may prove that the involution is uniquely determined by the decomposable subspace.

In the same way we may define the manifold of the fixed points of an involution of the second kind.

15. Fixed points of an anti-involution. Now we are going to find the fixed elements of anti-involutions.

THEOREM 23. *The fixed points of an anti-involution of the first kind form a connected piece of dimension $n(n+1)/2$ (real parameters).*

In fact, the fixed points of

$$(24) \quad W = \bar{Z}$$

are the real Z . The theorem is now evident.

THEOREM 24. *An anti-involution with signature (p, q) ($p \neq q$) has no fixed point and that with signature (p, p) has fixed points depending on $n(n+1)/2$ real parameters.*

Proof. We have (23). Its fixed points are given by $ZHZ = -H$. This is impossible except for $p=q$.

In the case $p=q$, we take the normal form

$$(25) \quad W = \begin{pmatrix} 0 & I^{(p)} \\ I & 0 \end{pmatrix} \bar{Z} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

Set

$$Z = \begin{pmatrix} Z_1 & Z_2 \\ Z'_2 & Z_3 \end{pmatrix}.$$

The fixed points of (25) are given by

$$Z_1 = \bar{Z}_3, \quad Z_2 = \bar{Z}'_2.$$

The number of parameters of Z_1 and Z_2 are $p(p+1)$, p^2 respectively. Thus the total number of parameters is equal to

$$p(p+1) + p^2 = p(2p+1) = n(n+1)/2.$$

16. Number of parameters of involutions. Now we are going to determine the dimensions of the manifolds formed by involutions and anti-involutions.

THEOREM 25. *The number of parameters (complex) of involutions of the second kind is equal to $n(n+1)$ and that of involutions of the first kind of signature (p, q) is equal to $4pq$.*

Notice that $4pq \leq n^2 < n(n+1)$.

Proof. (1) By Theorem 19, we have the first part of the theorem.

(2) Now we consider involutions of the signature (p, q) . It is known that the group of $2n$ -rowed symplectic matrices depends on $n(2n+1)$ parameters. We are going to find the number of parameters of the subgroup leaving the decomposable subspace

$$\begin{pmatrix} X_1^{(p)} & 0 \\ 0 & X_2^{(q)} \end{pmatrix}$$

invariant. By the result of §11 and Theorem 22, the number of parameters of the subgroup is equal to $p(2p+1) + q(2q+1)$. Therefore the number of parameters of involutions of the signature (p, q) is equal to

$$n(2n+1) - p(2p+1) - q(2q+1) = 2(n^2 - p^2 - q^2) = 4pq,$$

since $n = p+q$.

Now we give also the number of parameters of anti-involutions.

THEOREM 26. *Anti-involutions of the first or the second kind each form an $n(2n+1)$ parametric family (real parameters).*

Proof. We consider the anti-involution \mathfrak{T} of the first kind. Put

$$\mathfrak{T} = (\mathfrak{J} - \mathfrak{S}\mathfrak{F})(\mathfrak{J} + \mathfrak{S}\mathfrak{F})^{-1}.$$

From $\mathfrak{T}^*\mathfrak{T} = \mathfrak{J}$ and $\mathfrak{T}\mathfrak{F}\mathfrak{T}' = \mathfrak{F}$ we deduce easily that

$$\mathfrak{S} + \mathfrak{S}^* = 0, \quad \mathfrak{S} = \mathfrak{S}'.$$

That is, \mathfrak{S} is pure imaginary and symmetric. The theorem follows.

In the case of anti-involutions of the second kind, we have correspondingly

$$\mathfrak{S}\mathfrak{F}\mathfrak{S}^* = \mathfrak{F}, \quad \mathfrak{S} = \mathfrak{S}'.$$

Putting $\mathfrak{S} = (\mathfrak{J} - \mathfrak{P})(\mathfrak{J} + \mathfrak{P})^{-1}$ again, we have $\mathfrak{P}\mathfrak{S} + \mathfrak{S}\mathfrak{P}^* = 0$, $\mathfrak{P} = \mathfrak{P}'$, that is,

$$\mathfrak{P} = \begin{pmatrix} S & H \\ H' & -S \end{pmatrix},$$

where S is symmetric and H is Hermitian. The number of parameters is $n(n+1) + n^2 = n(2n+1)$.

17. Dieder manifolds. In this section we study the dimension of dieder manifold.

DEFINITION. Let A and B form a nonspecial pair. The locus of the points X satisfying

$$(50) \quad r(A, X) + r(X, B) = n$$

is called a *dieder manifold* of the point-pair (A, B) .

As a consequence of Theorem 20, the fixed points of an involution of the second kind form a dieder manifold of its two isolated fixed points. It is called the *dieder manifold of the involution*.

THEOREM 27. *Let \mathfrak{S} be an involution commutative with \mathfrak{T} , an involution of the second kind. Then \mathfrak{S} carries the dieder manifold of \mathfrak{T} into itself.*

Proof. \mathfrak{S} carries the isolated fixed points (A, B) of \mathfrak{T} to (C, D) . Then (C, D) are isolated fixed points of $\mathfrak{S}\mathfrak{T}\mathfrak{S}^{-1}$. Since $\mathfrak{S}\mathfrak{T}\mathfrak{S}^{-1} = \pm \mathfrak{T}$, \mathfrak{S} either keeps A and B fixed or permutes A and B . In both cases the dieder manifold is invariant.

DEFINITION. The part of the dieder manifold satisfying

$$(53) \quad r(A, X) = p$$

is called the *component of index p* with respect to A .

THEOREM 28. *The component of index p is of dimension $2pq$.*

Proof. It is now more convenient to use the homogeneous coordinate-system. We may assume that A and B are $(0, I)$ and $(I, 0)$ respectively. The component of index p is constituted by the points

$$(54) \quad (Z_1, Z_2)$$

where Z_1 is of rank p and Z_2 of rank q . Evidently

$$(55) \quad Z_1 = \begin{pmatrix} I^{(p)} & a \\ 0 & 0 \end{pmatrix}, \quad Z_2 = \begin{pmatrix} 0 & 0 \\ b & I^{(q)} \end{pmatrix}$$

are points on the component. The number of parameters is $2pq$. Thus we have to establish the following two facts:

(1) We have no Q , different from the identity, such that

$$(56) \quad Q \left(\begin{pmatrix} I^{(p)} & a \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ b & I^{(q)} \end{pmatrix} \right) = \left(\begin{pmatrix} I^{(p)} & a_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ b_1 & I^{(q)} \end{pmatrix} \right).$$

(2) In general, each point on the component is of the form (55).

To prove (1), we let

$$Q = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}.$$

Comparing the elements on both sides of (56), we have $q_{11} = I^{(p)}$, $q_{12} = 0$, $q_{21} = 0$, $q_{22} = I^{(q)}$. Thus (1) is true.

(2) The transformation leaving $(0, I)$ and $(I, 0)$ invariant of is the form

$$W_1 = QZ_1A, \quad W_2 = QZ_2D, \quad AD' = I.$$

Thus the points on the components are given by

$$W_1 = Q \begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix} A = Q \begin{pmatrix} a_{11}^{(p)} & a_{12} \\ 0 & 0 \end{pmatrix},$$

$$W_2 = Q \begin{pmatrix} 0 & 0 \\ 0 & I^{(q)} \end{pmatrix} A'^{-1} = Q \begin{pmatrix} 0 & 0 \\ \alpha_{21} & \alpha_{22} \end{pmatrix},$$

where

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad A'^{-1} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

We take the general case $d(a_{11}) \neq 0$, $d(a_{22}) \neq 0$. Thus

$$\begin{pmatrix} a_{11}^{-1} & 0 \\ 0 & a_{22}^{-1} \end{pmatrix} \left(\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \right)$$

gives the required form. The conditions of inequality are irrelevant in counting the parameters.

Consequently, two components of indices r and s of a dieder manifold are not equivalent topologically, if $r \neq s$ and $r+s \neq n$. As a consequence of Theorem 27, we have the following theorem.

THEOREM 29. *A dieder manifold is of dimension $2[n/2](n-[n/2])$ where $[x]$ denotes the integral part of x .*

18. Commutative involutions of the second kind. Without loss of generality the problem to be solved can be stated as follows:

Given an involution of the second kind, say (12), find all involutions of the second kind commutative with it.

Let \mathfrak{T} be the matrix of the required involution, then $\mathfrak{T}^2 = -\mathfrak{T}$ and

$$(57) \quad \mathfrak{T} \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix} = \pm \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix} \mathfrak{T}.$$

(1) Taking the upper sign, we have

$$\mathfrak{T} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad B = C = 0.$$

That is, the involution takes the form

$$(58) \quad W = AZA', \quad A^2 = -I.$$

Now we are going to find its isolated fixed points. There exists a nonsingular matrix Γ such that $\Gamma A \Gamma^{-1} = iH$, where $H = [1, \dots, 1, -1, \dots, -1]$, where there are p 1's and q -1's. Let

$$W_0 = \Gamma W \Gamma', \quad Z_0 = \Gamma Z \Gamma';$$

we have

$$(59) \quad W_0 = -HZ_0H$$

and notice that (12) takes the form $W_0 = -Z_0$. We drop the subscript 0.

Using homogeneous coordinates, we have

$$(60) \quad (Z_1, Z_2) = Q(W_1, W_2) \begin{pmatrix} iH & 0 \\ 0 & -iH \end{pmatrix}.$$

The transformation

$$(61) \quad \mathfrak{T} = \begin{pmatrix} I^p & iI_q \\ iI_q & I^p \end{pmatrix}, \quad I^p = \begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix}, \quad I_q = \begin{pmatrix} 0 & 0 \\ 0 & I^{(q)} \end{pmatrix}$$

carries (60) into

$$\begin{aligned} \mathfrak{T} \begin{pmatrix} iH & 0 \\ 0 & -iH \end{pmatrix} \mathfrak{T}^{-1} &= \begin{pmatrix} I^p & iI_q \\ iI_q & I^p \end{pmatrix} \begin{pmatrix} iH & 0 \\ 0 & -iH \end{pmatrix} \begin{pmatrix} I^p & -iI_q \\ -iI_q & I^p \end{pmatrix} \\ &= \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix}. \end{aligned}$$

The last matrix represents (12), and it has 0 and ∞ as its isolated fixed points. Thus the isolated fixed points of (60) are (I^p, iI_q) , (iI_q, I^p) which lie on the dieder manifold of (12).

(2) Taking the lower sign of (57), we have $A = D = 0$. Then

$$\mathfrak{T} = \begin{pmatrix} 0 & B \\ -B'^{-1} & 0 \end{pmatrix}.$$

Since

$$\begin{pmatrix} 0 & B \\ -B'^{-1} & 0 \end{pmatrix}^2 = \begin{pmatrix} -BB'^{-1} & 0 \\ 0 & * \end{pmatrix} = -\mathfrak{J},$$

B is symmetric ($= S$, say). Then we have

$$(62) \quad W = SZ^{-1}S.$$

It has $\pm S$ as its two isolated fixed points. Since $0, \infty, S, -S$ form a harmonic range, we have the following theorem.

THEOREM 30. *If an involution of the second kind is commutative with a fixed involution of the same kind, its isolated fixed points either lie on the dieder manifold of the fixed involution or separate the isolated fixed points of the fixed involution harmonically.*

The proof of Theorem 29 suggests also the following theorem.

THEOREM 31. *The involution of the second kind commutative with a fixed involution of the second kind depends on $n(n+1)/2$ parameters (complex).*

Proof. The case (2) gives us $n(n+1)/2$ parameters, as S is symmetric. The case (1) gives $2[n/2](n-[n/2])(< n(n+1)/2)$ parameters as shown by the following:

LEMMA. *The solution of the matrix equation*

$$(63) \quad A^2 = I$$

depends on $2[n/2](n-[n/2])$ parameters.

In fact, let A have 1 as characteristic root of multiplicity p , and -1 of multiplicity q . The most general solution is given by

$$\Gamma^{-1}[1, \dots, 1, -1, \dots, -1]\Gamma$$

where Γ is nonsingular.

Further, if $\Gamma^{-1}[1, \dots, 1, -1, \dots, -1]\Gamma = [1, \dots, 1, -1, \dots, -1]$ then

$$\Gamma = \begin{pmatrix} \gamma_1^{(p)} & 0 \\ 0 & \gamma_2^{(q)} \end{pmatrix},$$

which depends on p^2+q^2 variables. Thus for a fixed P , A depends on

$$n^2 - p^2 - q^2 = 2pq$$

parameters. This expression has its maximum for $p = [n/2]$.

Since

$$2[n/2](n - [n/2]) \leq 2(n/2)^2 < n(n+1)/2,$$

we have Theorem 30.

19. **Number of parameters of involutions commutative with a given involution.** Now we push Theorem 31 a little further.

THEOREM 32. *The involutions commutative with a fixed involution of the second kind depend on $n(n+1)/2$ parameters.*

Proof. We need only to consider the involutions of the first kind commutative $W = -Z$. Then, we have either

$$(64) \quad Z_1 = AZA', \quad A^2 = I$$

or, for even n ,

$$(65) \quad Z_1 = KZ^{-1}K$$

where K is skew symmetric. (64) depends on $[n/2](n-[n/2])$ parameters by the lemma of the last section. (65) depends on $n(n-1)/2$ parameters. Both do not exceed $n(n+1)/2$.

THEOREM 33. *The involutions commutative with a fixed involution of the first kind of signature (p, q) depend on $p(p+1)+q(q+1)$ parameters.*

Proof. We take $Z_1 = HZH$, $H = [1, \dots, 1, -1, \dots, -1]$ as the fixed involution. Let

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

be an involution commutative with it, then we have

$$(66) \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \pm \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

(1) Taking the upper sign, we have

$$A = \begin{pmatrix} a_1^{(p)} & 0 \\ 0 & a_2 \end{pmatrix}, \quad B = \begin{pmatrix} b_1^{(p)} & 0 \\ 0 & b_2 \end{pmatrix}, \quad C = \begin{pmatrix} c_1^{(p)} & 0 \\ 0 & c_2 \end{pmatrix}, \quad D = \begin{pmatrix} d_1^{(p)} & 0 \\ 0 & d_2 \end{pmatrix},$$

where

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

are involutions of the same kind. By Theorem 25, the number of parameters is

$$p(p+1) + q(q+1).$$

(2) We take the lower sign in (66). This is possible only when $p=q$. Then

$$A = \begin{pmatrix} 0^{(p)} & a_1 \\ a_2 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & b_1 \\ b_2 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & c_1 \\ c_2 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & d_1 \\ d_2 & 0 \end{pmatrix}.$$

Let

$$T_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

We have $T_1 T_2 = I^{(p)}$ and T_1 is symplectic. Thus the number of parameters of T_1 is equal to $p(2p+1)$ and T_2 is determined uniquely. Since

$$p(2p+1) < 2p(p+1)$$

we have the theorem.

Notice that

$$(67) \quad \begin{aligned} p(p+1) + q(q+1) &= p^2 + q^2 + p + q \\ &\geq (p+q)^2/2 + p + q > n(n+1)/2. \end{aligned}$$

20. Further study of commutative involutions. First of all, let us classify commutative involutions.

DEFINITION. Two commutative involutions of the second kind, \mathfrak{T}_1 and \mathfrak{T}_2 , which have isolated fixed points forming a harmonic range, are said to be commutative nondegenerately. Otherwise, we say they are commutative degenerately. For the degenerate case, the arithmetic distance between an isolated fixed point of \mathfrak{T}_1 and the other of \mathfrak{T}_2 is either p or q . We assume that $0 < p \leq n/2$. Then p is called the *arithmetic distance* of \mathfrak{T}_1 and \mathfrak{T}_2 .

Analytically, \mathfrak{T}_1 and \mathfrak{T}_2 are commutative nondegenerately if and only if

$$(68) \quad \mathfrak{T}_1 \mathfrak{T}_2 = -\mathfrak{T}_2 \mathfrak{T}_1$$

(see (2) of §18). In the present section we are going to establish the following theorem.

THEOREM 34. Let $n = 2^\sigma \tau$, where τ is odd. There are $\sigma+3$ involutions of the second kind any two of which are commutative nondegenerately, and $\sigma+3$ is the maximal number.

In other words, there are $\sigma+3$ nonspecial pairs of points such that any two pairs form a harmonic range.

We prove the present theorem together with the following:

THEOREM 35. Let $n = 2^\sigma \tau$, where τ is odd. Let $P(n)$, $\Sigma(n)$ and $K(n)$ denote the greatest integer s for which there exist s n -rowed symplectic, symmetric and skew-symmetric matrices T_1, \dots, T_s such that

$$(69) \quad T_i^2 = -I, \quad T_i T_j = -T_j T_i, \quad i \neq j,$$

respectively. Then

$$(70) \quad P(n) = \sigma + 2 \quad (\sigma \geq 1),$$

$$(71) \quad \Sigma(n) = \sigma + 1 \quad (\sigma \geq 0),$$

and

$$(72) \quad K(n) = \sigma \quad (\sigma \geq 1).$$

Notice that (70) implies Theorem 35 and that $P(n)$ and $K(n)$ are defined only for even n .

We establish (70), (71) and (72) as consequences of the equalities

$$(73) \quad P(2n) = 2 + \Sigma(n),$$

$$(74) \quad \Sigma(2n) = 2 + K(n)$$

and

$$(75) \quad K(2n) = 1 + K(n)$$

and the three initial equalities

$$(76) \quad K(2\tau) = 1,$$

$$(77) \quad \Sigma(\tau) = 1$$

and

$$(78) \quad \Sigma(2\tau) = 2$$

for odd τ .

We are going to prove (73) first. We start with the involution (12). By (2) of §18, the involutions commutative with (12) are of the form (62), where S is a symmetric matrix. There is a matrix Γ such that $\Gamma'\Gamma = S^{-1}$. We put $\Gamma'WT$ and $\Gamma'Z\Gamma$ instead of W and Z , then (12) takes its original form and (62) becomes

$$(79) \quad W = Z^{-1}.$$

Hence any pair of nondegenerately commutative involutions may be carried simultaneously to (12) and (79).

Now we consider an involution of the second kind commutative with both (12) and (79). Since it commutes with (12), it is of the form (62); since it commutes with (79), we have $S^2 = -I$. Let

$$W = S_i Z^{-1} S_i, \quad 1 \leq i \leq P(2n) - 2,$$

be involutions commutative nondegenerately. Then we have $S_i^2 = -I$, $S_i S_j^{-1} = -S_j S_i^{-1}$, that is,

$$(80) \quad S_i S_j = -S_j S_i, \quad S_i^2 = -I.$$

Therefore, we have

$$P(2n) - 2 \leq \Sigma(n).$$

On the other hand, if we have $\Sigma(n)$ symmetric matrices satisfying (80), we

may find $2+\Sigma(n)$ symplectic matrices with the required property. (In the following we shall not repeat this statement at similar occasions.) Therefore we have (73).

From (80), it follows that S_1 has simple elementary divisors and $\pm i$ are its characteristic roots. We have an orthogonal matrix Γ' such that

$$\Gamma S_1 \Gamma' = \begin{pmatrix} I^{(a)}i & 0 \\ 0 & -I^{(b)}i \end{pmatrix}.$$

We may put

$$(81) \quad S_1 = \begin{pmatrix} I^{(a)}i & 0 \\ 0 & -I^{(b)}i \end{pmatrix}.$$

If there exists an S_2 such that

$$S_1 S_2 = -S_2 S_1, \quad S_1 = -S_2 S_1 S_2^{-1},$$

then S_1 and $-S_1$ have the same characteristic equation. This is only possible for $a=b$. Therefore, we have (77). Now we take $n=2a$.

From $S_1 S_l + S_l S_1 = 0$, $S_l^2 = -I$ we deduce that

$$(82) \quad S_l = \begin{pmatrix} 0 & iA_l^{(a)} \\ iA_l^{-1} & 0 \end{pmatrix}, \quad \geq 2,$$

where

$$(83) \quad A_l A_l' = I.$$

Putting

$$\begin{pmatrix} A_2' & 0 \\ 0 & I^{(a)} \end{pmatrix} S_k \begin{pmatrix} A_2 & 0 \\ 0 & I^{(a)} \end{pmatrix}$$

instead of S_k , we find that (81) remains unaltered and S_2 takes the form

$$(84) \quad S_2 = \begin{pmatrix} 0 & iI \\ iI & 0 \end{pmatrix}.$$

If (82) is commutative with (84) nondegenerately, for $l \geq 3$, then the A_l ($l \geq 3$) are skew symmetric and satisfy $A_l^2 = -I^{(a)}$, $A_l A_k = -A_k A_l$. In case a is odd, there is no such A , we have therefore (78). Otherwise, we have (74).

Now we start again with $(2n)$ -rowed skew symmetric matrices

$$\mathfrak{R}_1, \dots, \mathfrak{R}_s$$

satisfying

$$(85) \quad \mathfrak{R}_i \mathfrak{R}_j = -\mathfrak{R}_j \mathfrak{R}_i, \quad \mathfrak{R}_i^2 = -\mathfrak{J}.$$

We may take

$$\mathfrak{R}_1 = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} = \mathfrak{F}.$$

From $\mathfrak{R}_i \mathfrak{R}_j = -\mathfrak{R}_j \mathfrak{R}_i$, we find

$$\mathfrak{R}_k = \begin{pmatrix} K_{1k} & K_{2k} \\ K_{2k} & -K_{1k} \end{pmatrix},$$

where K_{1k} and K_{2k} are skew symmetric matrices.

We introduce the transformation

$$(86) \quad \mathfrak{R}_k^\dagger = \frac{i}{2} \begin{pmatrix} I & iI \\ I & -iI \end{pmatrix} \mathfrak{R}_k \begin{pmatrix} I & I \\ iI & -iI \end{pmatrix}.$$

Then $\mathfrak{R}_1^\dagger = \mathfrak{F}$ and

$$\mathfrak{R}_k^\dagger = \begin{pmatrix} L_k & 0 \\ 0 & M_k \end{pmatrix},$$

where

$$(87) \quad L_k = -K_{2k} + iK_{1k},$$

$$(88) \quad M_k = K_{2k} + iK_{1k}.$$

\mathfrak{R}_k^\dagger ($k \geq 2$) can exist only when n is even. Thus we have (76). From (85), we deduce that

$$(89) \quad L_i M_i = I$$

and

$$(90) \quad L_i M_j + L_j M_i = 0, \quad i \geq 2, j \geq 2.$$

Consequently, we have L_2, \dots, L_s such that

$$(91) \quad L_i L_j^{-1} + L_j L_i^{-1} = 0.$$

We have Γ such that $\Gamma L_2 \Gamma' = F$, where

$$F = \begin{pmatrix} 0 & I^{(a)} \\ -I & 0 \end{pmatrix}, \quad a = 2n.$$

We may take $L_2 = F$. Let

$$N_i = F^{-1} L_i, \quad 3 \leq i \leq s.$$

Then, from (91),

$$(92) \quad N_i^2 = L_i^{-1} L_i L_i^{-1} L_i = -I,$$

$$(93) \quad FN_i + N_i F = L_i + F^{-1} L_i F = 0$$

and

$$(94) \quad N_i N_j + N_j N_i = L_2^{-1} L_j L_2^{-1} L_i + L_2^{-1} L_i L_2^{-1} L_j = - (L_j^{-1} L_i + L_i^{-1} L_j) = 0.$$

Further

$$N'_i = L'_i F'^{-1} = L_i F^{-1} = - F^{-1} L_i = - N_i.$$

Thus we have $s-1$ n -rowed skew symmetric matrices F, N_3, \dots, N_s satisfying (92), (93) and (94). Thus, we have (75).

Remark. If we restrict the T 's to be orthogonal in the theorem, the maximum s is equal to $K(n)=\sigma$. In fact, from

$$T^2 = -I, \quad TT' = I,$$

we deduce immediately $T = -T'$.

21. Parameters of involutions commutative with a pair of involutions.

Now we establish the characteristic distinction of all sorts of commutative involutions of the second kind.

THEOREM 36. *Given two nondegenerately commutative involutions of the second kind, the involutions of the second kind commutative with both depend on $[n/2](n-[n/2])$ parameters (complex).*

Proof. (1) Now we take, without loss of generality, the two fixed involutions as (12) and (11).

The involutions, nondegenerately commutative with both given involutions, are given by

$$(62) \quad W = SZ^{-1}S, \quad S^2 = -I.$$

We have an orthogonal matrix Γ such that

$$\Gamma S T' = H i, \quad H = [1, \dots, 1, -1, \dots, -1].$$

The totality of orthogonal matrices Γ depends on $n(n-1)/2$ parameters. Further from $\Gamma H T' = H$, we deduce

$$\Gamma = \begin{pmatrix} t^{(p)} & 0 \\ 0 & t^{(q)} \end{pmatrix},$$

which depends on $p(p-1)/2 + q(q-1)/2$ parameters. Thus S depends on

$$(n(n-1) - p(p-1) - q(q-1))/2 = pq \leq [n/2](n-[n/2])$$

parameters.

(2) Consider the involutions commutative degenerately with one of the fixed involutions, say $W = -Z$. Then they are of the form (58). If they commute with $W = -Z^{-1}$, either degenerately or not, then

$$W = AZ^{-1}A' = (AZA')^{-1} = A'^{-1}ZA^{-1},$$

and we deduce $A'A = \pm I$. Then

$$A' = -A'A^2 = \mp A,$$

that is, A is either symmetric or skew-symmetric. If it is symmetric, the number of symmetric involutions A has been counted in (1).

Now we assume that A is skew-symmetric and orthogonal. Consequently n is even, equal to $2p$, say. Since $A^2 = -I$, A has $\pm i$ as its characteristic roots and its elementary divisors are simple. Since

$$d(A - \lambda I) = d(A - \lambda I)' = d(-A - \lambda I),$$

the multiplicities of i and $-i$ are equal.

The pair of matrices

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

has the prescribed elementary divisors. Thus we have an orthogonal matrix Γ such that

$$\Gamma A \Gamma' = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The totality of orthogonal matrices depends on $n(n-1)/2$ parameters and symplectic orthogonal matrices of order $2p$ depend on p^2 parameters. Thus the number of parameters is

$$n(n-1)/2 - n^2/4 < ((n-1)/2)(n - ((n-1)/2)) \leq [n/2](n - [n/2]),$$

and the theorem follows.

THEOREM 37. *The involutions of the second kind commutative with two commutative involutions of the second kind of arithmetic distance p depend on $p(p+1)/2 + q(q+1)/2$ parameters.*

Proof. We may write both fixed involutions as (12) and

$$(59) \quad W = -HZH$$

where $H = [1, \dots, 1, -1, \dots, -1]$.

(1) The involutions commutative degenerately with (12) are given by (58). If they commute with (59), we have $AH = \pm HA$. Consequently, we have

$$A = \begin{pmatrix} a_1^{(p)} & 0 \\ 0 & a_2^{(q)} \end{pmatrix}, \quad \text{or} \quad A = \begin{pmatrix} 0 & b_1^{(p)} \\ b_2^{(q)} & 0 \end{pmatrix},$$

the second case can appear only when $p = n/2$.

(11) The number of parameters of

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}, \quad a_1^2 = -I^{(p)}, \quad a_2^2 = -I^{(q)}$$

is equal to $2[p/2](p - [p/2]) + 2[q/2](q - [q/2])$, by the lemma of §18.

(12) From $A^2 = -1$, we deduce

$$\begin{pmatrix} 0 & b_1 \\ b_2 & 0 \end{pmatrix}, \quad b_1 b_2 = -I^{(p)}.$$

Thus the number of parameters is equal to p^2 , which is less than $p(p+1)$.

(2) The involutions commuting with (12) nondegenerately are of the form

$$W = SZ^{-1}S.$$

If they commute with (59), we have $HS = \pm SH$. Consequently, we obtain

$$S = \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix}, \quad \text{or} \quad S = \begin{pmatrix} 0 & t \\ t' & 0 \end{pmatrix}.$$

The number of parameters in the first case is

$$p(p+1)/2 + q(q+1)/2,$$

and in the second case, $n = 2p$, is $p^2 < p(p+1)$.

Finally, we have the theorem, since

$$2[p/2](p - [p/2]) + 2[q/2](q - [q/2]) < p(p+1)/2 + q(q+1)/2.$$

22. Automorphisms of the group of symplectic transformations. Finally, we are going to prove the following theorem.

THEOREM 38. *A topological automorphism of the group of symplectic transformations is either an inner automorphism or an anti-symplectic transformation.*

More explicitly: Let \mathfrak{G} be the group of symplectic transformations. It may be visualized as the totality of symplectic matrices \mathfrak{T} , but we have to identify \mathfrak{T} and $-\mathfrak{T}$. \mathcal{A} is called an automorphism over \mathfrak{G} , written as

$$(95) \quad \mathcal{A}(\mathfrak{T}) = \mathfrak{T}\dagger,$$

if it builds up a one-to-one and bi-continuous relation between \mathfrak{T} and $\mathfrak{T}\dagger$, and if

$$(96) \quad \mathcal{A}(\mathfrak{T}_1\mathfrak{T}_2) = \mathfrak{T}_1\dagger\mathfrak{T}_2\dagger.$$

The conclusion of the theorem is that we have either a symplectic matrix \mathfrak{P} such that

$$(97) \quad \mathcal{A}(\mathfrak{T}) = \mathfrak{P}\mathfrak{T}\mathfrak{P}^{-1}$$

or a symplectic matrix \mathfrak{P} such that

$$(98) \quad \mathcal{A}(\mathfrak{T}) = (\mathfrak{P}\dagger\mathfrak{T})\dagger\mathfrak{P}^{-1} = \mathfrak{P}\mathfrak{T}\dagger\mathfrak{P}^{-1},$$

for all \mathfrak{T} .

Proof. Evidently the automorphism \mathcal{A} carries an involution into an in-

volution and a pair of commutative involutions into a pair of commutative involutions. The involutions commutative with an involution of the first kind of signature (p, q) form a manifold of dimension $p(p+1)+q(q+1)$, by Theorem 33, and those commutative with an involution of the second kind form a manifold of dimension $n(n+1)/2$ by Theorem 32. Since the numbers

$$n(n+1)/2, \quad p(p+1)+q(q+1), \quad 1 \leq q \leq n/2,$$

are never equal, and since a topological transformation leaves the dimension invariant, \mathcal{A} leaves the kind and signature of involutions invariant.

Further, the manifold formed by the involutions of the second kind permuting with a pair of commutative involutions of arithmetic distance p is of dimension

$$p(p+1)/2 + q(q+1)/2$$

by Theorem 37. They are all different for $0 < p \leq n/2$. Moreover the manifold formed by the involutions of the second kind permuting with a pair of non-degenerate commutative involutions is of dimension $[n/2](n-[n/2])$, by Theorem 36. Therefore the “degeneracy” of a pair of commutative involutions is also invariant under \mathcal{A} .

Each involution of the second kind is determined uniquely by its two isolated fixed points. Thus, we use (A, B) to denote an involution of the second kind possessing A and B as its two isolated fixed points.

We now prove that two involutions with a common isolated fixed point, and the other two fixed points forming a nonspecial pair, are carried by \mathcal{A} into involutions with the same property. In fact, let

$$(99) \quad (A, B), \quad (A, C)$$

be the two involutions under consideration, and suppose that \mathcal{A} carries them into

$$(100) \quad (P, Q), \quad (R, S).$$

The transformations commutative degenerately with both involutions (99) form a group isomorphic to the orthogonal group. In fact we may take $A = 0$, $B = \infty$ and $C = I$; the conclusion follows immediately.

Suppose that at least one of the arithmetic distances $r(P, R)$, $r(P, S)$, $r(Q, R)$ and $r(Q, S)$ is different from 0 and n . Then the subgroup formed by the transformations commutative degenerately with (P, Q) and (R, S) is reducible. In fact, we may let, in homogeneous coordinates,

$$P = (I, 0), \quad Q = (0, I), \quad R = \left[\begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix} \right].$$

Direct verification asserts that the group is formed by the elements of the form:

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}, \quad A = \begin{pmatrix} A_{11} & 0 & 0 \\ A_{21} & A_{22} & 0 \\ A_{31} & A_{32} & A_{33} \end{pmatrix}, \quad A_{22}A'_{22} = I.$$

Since the orthogonal group cannot be isomorphic to a reducible group, we have the conclusion that either our assertion is true or that

$$r(P, R) = r(P, S) = r(Q, R) = r(Q, S) = n.$$

The latter case cannot happen. In fact, there is no pair of matrices (X, Y) to separate both (A, B) and (A, C) harmonically, and this may be justified easily by putting $A=0$, $B=\infty$ and $C=I$. On the other hand, there exists a nonspecial pair (X, Y) to separate (P, Q) and (R, S) both harmonically. In fact, we may take $P=0$, $Q=\infty$, $R=I$; then the pair $(S_1, -S_1)$ separates both pairs harmonically when $S_1^2=S$. Thus we have established our assertion.

Let $\Sigma(A)$ be the set of involutions having a common fixed point A . Then, by \mathbf{A} , it is mapped into another set with the same property. In fact, if (A, B) , (A, C) , $(r(B, C)=n)$ are mapped into $(A\dagger, B\dagger)$, $(A\dagger, C\dagger)$; a third pair (A, D) must be mapped into either $(A\dagger, D\dagger)$ or $(B\dagger, C\dagger)$. The latter case cannot happen, since \mathbf{A} cannot map a fourth one. We may remove the assumption $r(B, C)=n$ by means of a consideration of continuity.

Suppose $\Sigma(A)$ is carried into $\Sigma(A\dagger)$ by \mathbf{A} . Therefore \mathbf{A} induces a mapping of the space of symmetric matrices: $(A \rightarrow A\dagger)$.

Let $r(A, B)=p$. The points C satisfying

$$r(A, C) = n, \quad r(B, C) = q$$

form a manifold of dimension $nq-q(q+1)/2$. Let D be the image of B under the involution (A, C) . Then (A, C) , (B, D) are two commutative involutions with the arithmetic distance q . Suppose \mathbf{A} carries $\Sigma(A)$ and $\Sigma(B)$ into $\Sigma(A\dagger)$ and $\Sigma(B\dagger)$. Then we find that $r(A\dagger, B\dagger)=p$ or q . Since $np-p(p+1)/2 \neq nq-q(q+1)/2$ for $p \neq q$, we have $r(A\dagger, B\dagger)=p$.

Therefore the automorphism \mathcal{A} induces a mapping on the space of symmetric matrices possessing the following properties:

- (1) It is topological.
- (2) It keeps harmonic separation invariant.
- (3) It keeps arithmetic distance invariant.

The theorem follows from the generalization of von Staudt's theorem for symmetric matrices.