ON A NORMAL FORM OF THE ORTHOGONAL TRANSFORMATION I

Hans Zassenhaus

(received November 20, 1957)

At the Edmonton Meeting of the Canadian Mathematical Congress E. Wigner asked me whether one knew something about the distribution of the characteristic roots of the linear transformations that leave invariant the quadratic form $t^2+x^2-y^2-z^2$, just as one knows that a Lorentz transformation has two complex conjugate characteristic roots and two real characteristic roots that are either inverse to one another or the numbers 1 and -1.

In this paper an answer to E. Wigner's question will be obtained.

We are concerned with the pairs of matrices (X,A) with coefficients in a field of reference F such that the condition

$$X^T A X = A \tag{0.1}$$

is satisfied, where $X^T = (\xi_{ki})$ is the transpose of the matrix $X = (\xi_{ik})$. It follows that both matrices are quadratic of the same degree d.

Our problem is to classify the matrices X according to their characteristic polynomials for the real field as the field of reference and for a fixed symmetric matrix A. To solve this problem we construct normal forms for each class of conjugate elements of the group GO(A,F) formed by the solutions X of (0.1) for a fixed regular and symmetric or anti-symmetric matrix A and

Can. Math. Bull., vol. 1, no. 1, Jan. 1958

https://doi.org/10.4153/CMB-1958-006-4 Published online by Cambridge University Press

for any perfect field of reference F with characteristic distinct from 2. The class representatives will be surveyed in such a way that the characteristic polynomials are set in evidence.

In §1 the concepts of representation space, equivalence and decomposition of matrix pairs are developed. In §§2,3 the indecomposable classes of equivalent matrix pairs are classified. In §4 the normal forms and invariants of arbitrary matrix pairs are expounded. In §5 the results are applied to the real field and to Galois fields as fields of reference.

§1. Representation space, equivalence and decomposition of matrix pairs.

The linear space M over F is called a representation space of the matrix pair

$$(X,A) = ((\xi_{ik}),(\alpha_{ik})) \qquad (i,k = 1,2,\ldots,d)$$

if there is an F-basis $a_1,a_2,\ldots,a_d$, a linear transformation σ of M and a bilinear form f on M such that

$$(1.1) \qquad \sigma\left(\sum_{k=1}^{d} \eta_k a_k\right) = \sum_{i=1}^{d}\sum_{k=1}^{d} \alpha_{ik}\eta_k a_i$$

$$(1.2) \qquad f\left(\sum_{i=1}^{d} \xi_i a_i, \sum_{k=1}^{d} \eta_k a_k\right) = \sum_{i=1}^{d}\sum_{k=1}^{d} \xi_i \eta_k \alpha_{ik}$$

$$(1.3) \qquad f(\sigma a,\sigma b) = f(a,b)$$

for $\xi_i \eta_k$ in F and for a,b in M.

It is clear that for a given matrix pair (X,A) a representation space M can be constructed by defining a linear transformation σ and a bilinear form f on a linear space M with F-basis $a_1,a_2,\ldots,a_d$ by means of (1.1) and (1.2) inasmuch as (1.3) is equivalent to (0.1).

If another F-basis

$$(1.4) \qquad b_k = \sum_{i=1}^{d} \tau_{ik} a_i \qquad (k = 1,2,\ldots,d)$$

of M is chosen so that the matrix

$$(1.5) \qquad T = (\tau_{ik})$$

is regular, then another matrix pair

$$(Y,B) = ((\eta_{ik}),(\beta_{ik}))$$

is defined by means of

$$(1.6) \qquad \sigma b_k = \sum_{i=1}^{d} \eta_{ik} b_i \qquad (k = 1,2,\ldots,d)$$

$$(1.7) \qquad f(b_i,b_k) = \beta_{ik} \qquad (i,k = 1,2,\ldots,d)$$

where the matrix Y is similar to X:

$$(1.8) \qquad Y = T^{-1}X\,T,$$

the matrix B is equivalent to A:

$$(1.9) \qquad B = T^T A\,T,$$

and <u>the matrix pair</u> (Y,B) <u>is equivalent to the matrix pair</u> (X,A) according to

$$(1.10) \qquad (X,A) \sim (T^{-1}X\,T, T^T A\,T).$$

Our problem is to survey the classes of matrix pairs that are equivalent in the sense of the normal relation defined by (1.10). Let us begin with a few definitions.

A linear subspace m of M is called invariant under σ if $\sigma m \leq m$. The invariant subspaces of M form a modular lattice when intersection and sum of two invariant subspaces are taken as lattice operations. For example, the subset $P(\sigma)M$ formed by all elements $P(\sigma)u$ with u in M is an invariant subspace for any polynomial

$$(1.11) \qquad P(x) = \alpha_0 + \alpha_1 x + \ldots\ldots + \alpha_n x^n$$

with coefficients in F. The same applies to the

https://doi.org/10.4153/CMB-1958-006-4 Published online by Cambridge University Press

subspace M_p of all elements of M that are annihilated by the linear transformation

$$(1.12) \qquad P(\sigma) = \alpha_0 \underline{1} + \alpha_1 \sigma + \ldots + \alpha_n \sigma^n.$$

The two subsets K_1, K_2 of M are called <u>orthogonal</u> (to each other) if $f(K_1,K_2) = f(K_2,K_1) = 0$ where generally $f(K_1,K_2)$ denotes the set of all values $f(x_1,x_2)$ with x_i contained in K_i $(i = 1,2)$. For any subset K of M the set K' of all elements x of M satisfying $f(x,K) = f(K,x) = 0$ forms a linear subspace of M such that K' is the maximal subset of M that is orthogonal to K.

From $K_1 \leq K_2$ it follows that $K_1' \geq K_2'$. The kernel M_σ of σ belongs to M' because for any x in M

$$f(x,M) = f(\sigma x, \sigma M) = f(0, \sigma M) = 0$$

and similarly $f(M,x) = 0$. For any subset K of M one has $K' = (FK)' = \{K\}' = (K + M')'$ where $\{K\}$ is the module generated by K.

For any linear subspace K of M the dimension $\dim K = \dim_F K$ of K over F satisfies the relation

$$\dim K = \dim \sigma K + \dim K \cap M_\sigma.$$

There is a linear subspace m of K + M' such that the direct decomposition $K + M' = m \dot{+} M'$ holds. Hence $m \cap M' = 0$. For any element u of m for which σu belongs to M', we have $f(u,M) = f(\sigma u, \sigma M) \leq f(M',M) = 0$; and similarly $f(M,u) = 0$. Hence u belongs to M', and since $M' \cap m = 0$ it follows that $u = 0$. Thus $\sigma m \cap M' = 0$, $\dim m = \dim \sigma m$, $\dim(K + M') = \dim(m \dot{+} M') = \dim m + \dim M'$ $= \dim \sigma m + \dim M' = \dim(\sigma m \dot{+} M')$.

For $K = M$ one finds that $\dim M = \dim(\sigma m \dot{+} M')$, so that $M = \sigma m \dot{+} M'$ and $f(\sigma M', M) = f(\sigma M', \sigma m + M')$ $= f(\sigma M', \sigma m) = f(M', m) = 0$.

https://doi.org/10.4153/CMB-1958-006-4 Published online by Cambridge University Press

Similarly $f(M,\sigma M') = 0$; hence M' is invariant under σ.

For any linear subspace we conclude that

$\sigma K+M' = \sigma K+\sigma M'+M' = \sigma(K+M')+M' = \sigma(m\dot{+}M')+M' = \sigma m\dot{+}M'$,

$\dim(\sigma K+M') = \dim \sigma m + \dim M' = \dim m + \dim M' = \dim(K+M')$.

If $\sigma K \leq K$ for any subset K of M, then

$\sigma(\{FK\}) \leq \{FK\}$, $\quad \sigma(\{FK\}+M') \leq \{FK\}+M'$,

$\dim(\sigma\{FK\}+M') = \dim(\{FK\}+M')$, $\quad \sigma\{FK\}+M' = \{FK\}+M'$,

$0 = f(K,K') = f(\sigma K,\sigma K') = f(\sigma\{FK\}+M', \sigma K')$

$= f(\{FK\}+M',\sigma K') = f(\{FK\},\sigma K') = f(K,\sigma K')$;

similarly $f(\sigma K',K) = 0$. Thus the relation $\sigma K \leq K$ implies the invariance of the orthogonal subspace K' of K under σ.

A decomposition

$$(1.13) \qquad M = M_1 \dot{+} M_2 \dot{+} \dots \dot{+} M_r = \dot{\sum}_{i=1}^{r} M_i$$

of M into the direct sum of non vanishing invariant subspaces $M_1,\dots,M_r$ is called an <u>orthogonal decomposition</u> if any two distinct subspaces M_i, M_k are orthogonal. If we choose an F-basis $a_{j1}, a_{j2},\dots,a_{jd_j}$ of M_j then a matrix Y_j is defined by

$$(1.14) \qquad \sigma a_{jk} = \sum_{i=1}^{d_j} \eta^{(j)}_{ik} a_{ji} \qquad (k = 1,2,\dots,d_j)$$

and

$$(1.15) \qquad Y_j = (\eta^{(j)}_{ik}) \qquad (j = 1,2,\dots,r)$$

such that X is similar to the matrix

$$(1.16) \qquad Y = \begin{bmatrix} Y_1 & & & \\ & Y_2 & & \\ & & \ddots & \\ & & & Y_r \end{bmatrix} = Y_1 \dot{+} Y_2 \dot{+} \dots \dot{+} Y_r = \dot{\sum}_{i=1}^{r} Y_i$$

Also, there are bilinear forms f_j induced on the invariant subspaces M_j with matrix B_j defined by

$$(1.17) \qquad B_j = (\beta^{(j)}_{ik})$$

and

$$(1.18) \qquad f_j(a_{ji}, a_{jk}) = \beta^{(j)}_{ik}$$

such that

$$(1.19) \quad (X,A) \sim (Y,B) = (\dot{\sum}_{j=1}^{r} Y_j, \dot{\sum}_{j=1}^{r} B_j) = \dot{\sum}_{j=1}^{r} (Y_j, B_j).$$

Conversely, any equivalence (1.19) corresponds to an orthogonal decomposition (1.13) of M. If there is no such decomposition with more than one component, then we call the matrix pair <u>indecomposable</u>.

Any matrix pair is equivalent to the direct sum of indecomposable matrix pairs. Conversely, it is clear that for any r-tuple of matrix pairs (Y_j, B_j) $(j = 1,2,\ldots,r)$ there is the matrix pair

$$(\dot{\sum}_{j=1}^{r} Y_j, \dot{\sum}_{j=1}^{r} B_j)$$

that is the direct sum of the given r matrix pairs in their given order.

2. <u>Indecomposable matrix pairs I</u>.

In this section the indecomposable matrix pairs are studied.

LEMMA 1: If the invariant subspaces M_P, M_Q are not orthogonal then there is an extension of the field of reference in which there is a root of the polynomial $Q(x)$ equal to the inverse of a root of the polynomial $P(x)$.

<u>Proof</u>: Since P,Q occur symmetrically both in the assumption and in the assertion it may be assumed that $f(M_P, M_Q) \neq 0$. Among the invariant subspaces of M_P that are not orthogonal to M_Q there is a minimal subspace m. We call the two polynomials R,S with coefficients in F congruent if $f((R(\sigma) - S(\sigma))m, M_Q) \doteq 0$. This is a

normal congruence relation defined on the polynomial ring $F[x]$ over F satisfying the substitutional laws of addition and multiplication. The constant polynomial 1 is not congruent to 0 because $f(m,M_Q) \neq 0$. Moreover, since m is contained in M_P and therefore $P(\sigma)m = 0$, it follows that the congruence of R and S modulo $P(x)$ implies congruence in the sense defined above. Finally, if both $R(x)$ and $S(x)$ are not congruent to σ, then each of the invariant subspaces $R(\sigma)m$, $S(\sigma)m$ of m is not orthogonal to M_Q; by the minimal property of m it follows that $R(\sigma)m = S(\sigma)m = m$, $(RS(\sigma))m = (R(\sigma)S(\sigma))m = R(\sigma)(S(\sigma)m) = R(\sigma)m = m$, RS is not congruent to 0. Hence the congruence classes of the polynomial ring $F[x]$ form a finite extension E of F in which $P(x)$ represents the zero class. Since

$$0 \neq f(m,M_Q) = f(\sigma m, \sigma M_Q) \leq f(\sigma m, M_Q)$$

it follows that x is not congruent to 0 and hence there is a polynomial $U(x)$ in $F[x]$ for which $xU(x)$ is congruent to 1. For any two elements u of m and v of M_Q we have $f(u,\sigma v) = f(\sigma U(\sigma)u, \sigma v) = f(U(\sigma)u, v)$,

$$f(u, \sigma^{1} v) = f((U(\sigma)^{1} u, v)$$

and

$$f(u, R(\sigma)v) = f(R(U(\sigma))u, v), \tag{2.1}$$

where $R(x)$ is any polynomial with coefficients in F. In particular, for the polynomial $Q(x)$ we find that

$$0 = f(u, Q(\sigma)v) = f(Q(U(\sigma))u, v).$$

Hence the polynomial $Q(R(x))$ is congruent to 0. Furthermore the congruence class represented by $R(x)$ is a root of Q and inverse to the congruence class represented by x (which is a root of P). Lemma 1 suggests that there be formed for every polynomial (1.11) with non vanishing lowest coefficient α_m the polynomial

(2.2) $P^*(x) = x^{n-m} + \alpha_m^{-1}\alpha_{m+1}x^{n-m-1} + \ldots + \alpha_m^{-1}\alpha_n$

with highest coefficient 1 and roots inverse to the non vanishing roots of $P(x)$. Lemma 1 states that M_P, M_Q are orthogonal if Q^* is prime to P.

If two polynomials R,S are mutually prime, then we have $M_{RS} = M_R + M_S$, $M_R \cap M_S = 0$; hence there is the decomposition of M_{RS} into the direct sum of M_R and M_S. This remark is applied to the factorization of the characteristic polynomial $\chi_X(x) = \det(xI_d - X)$ of the matrix X into the product of two mutually prime factors R,S with highest coefficients 1. In this case the direct decomposition $M_{RS} = M_R \dot{+} M_S$ corresponds to a matrix decomposition $T^{-1}XT = Y_1 \dot{+} Y_2$ where $\chi_{Y_1} = R$, $\chi_{Y_2} = S$, and T is a suitable regular matrix.

Hence from Lemma 1 it follows that for an indecomposable matrix pair (X,A) one of the following 3 cases holds:

(2.3) I: $A \neq 0, \chi_X = P^\mu$ where $P = P^*$ is a symmetric irreducible polynomial,

II: $A \neq 0, \chi_X = (PP^*)^\mu$ where P is an asymmetric irreducible polynomial with highest coefficient 1,

III: $A = 0, \chi_X = P^\mu$ where P is any irreducible polynomial.

In the case III no restriction is imposed on X by the condition (0.1) so that in this case the indecomposability of the matrix pair (X,A) simply means that the matrix X is not similar to a diagonal matrix of matrices, or in other terms, the representation space is not the direct sum of two proper invariant subspaces. Such spaces are called <u>indecomposable representation spaces</u>. It is well known from ordinary elementary divisor theory of matrices that a linear space of finite dimension is indecomposable under the linear transformation σ if and only if the minimal polynomial m_σ of σ is equal to the characteristic polynomial χ_σ of σ, a power of an irreducible polynomial. In this case we call the linear transformation σ and the corresponding matrices <u>indecomposable</u>.

The condition $A = 0$ is equivalent to the vanishing of the bilinear form f, in which case one speaks of an <u>isotropic linear space</u> M. Similarly a linear subspace of a representation space is called isotropic if the given bilinear form vanishes identically on the subspace.

The result (2.3) constitutes a first answer to our problem inasmuch as it states that the characteristic polynomial of any matrix X solving (0.1) for a regular matrix A necessarily contains any irreducible polynomial P with highest coefficient 1 with the same multiplicity as the polynomial P*.

In the next section a normal form for the indecomposable matrix pairs will be established and used to find sufficient conditions for the characteristic polynomial of X.

<u>McGill University</u>