JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 76B, Nos. 3 and 4, July–December 1972

Normal Matrices With Entries from an Arbitrary Field of Characteristic $\neq 2$

Martin H. Pearl and Alan I. Penn*

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(July 11, 1972)

Let F be an arbitrary field of characteristic $\neq 2$ and let conjugation in F be defined by an arbitrary involutory automorphism (possibly the identity mapping). A matrix with entries from F is normal if it commutes with its conjugate transpose. Several conditions which are equivalent to normality when F is the complex field are properly nested when F is an arbitrary field. Of these conditions, normality is the weakest and unitary diagonalizability is the strongest.

When the underlying field is closed the unitarily diagonalizable matrices are those which possess a spectral representation with Hermitian idempotents. These matrices may be characterized in terms of their EP properties.

A matrix is indecomposable if it has a single elementary divisor of the form $(x-s)^i$. For $i>1$, normal indecomposable matrices do not exist when F is the complex field. However there exist fields for which normal indecomposable matrices of all finite orders exist. A matrix is a normal indecomposable matrix if and only if it can be expressed as $r(B)$ where $r(x)$ is a polynomial such that $r'(0)\neq 0$ and B is a matrix having the single elementary divisor x^i and satisfying the equation $B^*=sB$ for some scalar s.

When the involutory automorphism of F is the identity mapping indecomposable normal matrices of even order exist if and only if the vector space F^n is hyperbolic, and in this case the matrices are symmetric. Moreover, indecomposable normal matrices of odd order exist if and only if F^n is the orthogonal sum of a hyperbolic space and a one dimensional space, and in this case both symmetric and nonsymmetric indecomposable normal matrices exist.

Key words: Field; matrices; normality; hyperbolic space.

1. Introduction

Since Toeplitz [13][1] introduced normal matrices in 1918, there has been considerable effort to study their structure and properties. Several conditions equivalent to normality over the complex field have been found. In addition a number of generalizations of normality over the complex field have been proposed and investigated. Recently there has been an increased interest in the study of normal matrices over arbitrary base fields.

According to a classical theorem the following conditions are equivalent over the complex field [2]:

(1) A is normal, that is $A^*A=AA^*$

(2) A^* can be expressed as a polynomial in A with scalar coefficients.

(3) A has a spectral representation with Hermitian idempotents, that is, if $s_1, s_2, \ldots, s_k$ are the distinct characteristic roots of A then there exist matrices $E_1, E_2, \ldots, E_k$ such that:

(a) $I=\sum_i E_i$

(b) $E_iE_j=0$ for $i\neq j$

AMS Subject Classification: Primary 1535, Secondary 1545.

*Present address: University of Maryland, College Park, Md. 20740.

The work in this paper forms a portion of the second author's doctoral dissertation presented to the University of Maryland at College Park in 1971.

[1] Figures in brackets indicate the literature references at the end of this paper.

(c) $E_i^* = E_i$

(d) $A = \sum_i s_i E_i$

(4) A is unitarily similar to a diagonal matrix.

Additional conditions which are equivalent to normality over the complex field are given in [12, p. 222], [2, 4].

Generalizations to normality over the complex field have been proposed by Williamson [14, 15] and Schwerdtfeger [12]. Williamson observed the equivalence of conditions (1) and (2) above and generalized the concept of normality as follows: a matrix is *normal with respect to the Hermitian matrix* H if there exists a polynomial with scalar coefficients, $f(x)$, such that $AH = Hf(A^*)$. Schwerdtfeger generalized normality by introducing the concept of an EPr matrix: a matrix A is EPr if A has rank r and A and A^* have the same null space. That this is a generalization of normality over the complex field is most easily seen by noting that A is EPr if and only if A is unitarily similar to the direct sum of a nonsingular $r \times r$ matrix and a zero matrix [6].

In [9, 10] the concept of a normal matrix was extended to an arbitrary field with an involutory automorphism. Over an arbitrary field the notions of EPr and normality are independent. Moreover, both normality and the EPr property are necessary for A^* to be expressable as a unitary multiple of A ($A^* = UA = AU$ where $UU^* = I$), a condition which is weaker than unitary diagonalizability. Katz and Pearl [6] extended the results on normal EPr matrices over arbitrary fields, and found necessary and sufficient conditions for such matrices to satisfy the condition that A^* be a unitary multiple of A.

In this paper normal matrices will be studied for two extreme but important cases. In section 4, a characterization of normal matrices which are unitarily similar to a diagonal matrix is given for base fields which are closed and of characteristic $\neq 2$. Conjugation is defined by an arbitrary involutory automorphism. In section 5, we study normal matrices which have a single elementary divisor of the form $(x-s)^i$. Again the base fields are of characteristic $\neq 2$, and conjugation is defined by an arbitrary involutory automorphism. It is shown in Theorem 10 that matrices of this second form are normal if and only if they satisfy condition (2). While condition (4) precludes the existence of normal matrices of this second form for $i > 1$ over the complex field, there exist base fields for which such normal matrices exist for all orders. It is demonstrated in section 6 that one example of such a field is the complex numbers with conjugation defined by the identity automorphism. In section 6 more extensive results for the second case are obtained when conjugation is restricted to be the identity automorphism.

2. The Structure of Normal Matrices

Conditions (2), (3), and (4) define several key features of the structure of normal matrices over the complex field. However, when arbitrary base fields with associated involutory automorphisms are considered each of these conditions is stronger than that of normality, and consequently can not be used to define a structure on the full set of normal matrices. The proof of the following theorem is known but is included for completeness. (The conjugate transpose of the matrix M is denoted by M^*; the conjugate, or automorphic image, of the scalar s is denoted by $\bar{s}$).

THEOREM 1: *The following implications hold for an arbitrary base field:*

$$(4) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1).$$

PROOF: (4) $\Rightarrow$ (3): There exists a diagonal matrix D and a unitary matrix U such that $A = UDU^*$. Consequently we can write A in the form

$$A = U \operatorname{diag}(s_1 I_{m_1}, s_2 I_{m_2}, \ldots, s_k I_{m_k}) U^*$$

where I_{m_j} is the unit matrix of order m_j. Let D_i denote the diagonal matrix obtained from diag $(s_1 I_{m_1}, s_2 I_{m_2}, \ldots, s_k I_{m_k})$ by replacing s_i by 1 and s_j by 0 for $j \neq i$. If we define $E_i = UD_iU^*$ then condition (3) is readily verified.

(3) $\Rightarrow$ (2): It is readily verified that $p(A) = \Sigma p(s_i)E_i$ for any polynomial $p(x)$. If we define $p_i(x) = (x-s_1)(x-s_2)\cdots(x-s_k)/(x-s_i)$ then we obtain $p_i(A) = p_i(s_i)E_i$. Consequently, E_i is expressible as a polynomial in A, and since $A^* = \Sigma \bar{s}_i E_i$ it follows that A^* is expressible as a polynomial in A.

(2) $\Rightarrow$ (1): Trivial. *Q.E.D.*

Counterexamples for the converse implications are given in Examples 1, 2, and 3.

EXAMPLE 1: Matrix satisfying (1) but not (2). Let the base field be $GF(7)$ with the identity automorphism. (Example taken from reference [9].) Let

$$B = \begin{pmatrix} 1 & 3 & 0 & 2 \\ 2 & -1 & 0 & 4 \\ 3 & 2 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

It is readily seen that $B^2 = 0$ and hence the only polynomials in B are of the form $pI + qB$. By considering the elements in the (1, 1) and (4, 4) positions of B, it is seen that if (2) holds, then $p = 0$ and $q = 1$ which in turn implies that B is symmetric. Since B is not symmetric (2) cannot hold. Condition (1) is verified by computation.

EXAMPLE 2: Matrix satisfying (2) but not (3). Let the base field be $GF(3)$ with the identity automorphism.
Let

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The matrix C is symmetric and consequently satisfies condition (2). However C is nilpotent and consequently not diagonalizable. It remains to observe that any matrix with a spectral representation (with or without Hermitian idempotents) is diagonalizable [2]. Hence C cannot satisfy condition (3).

EXAMPLE 3: Matrix satisfying (3) but not (4). Let the base field be $GF(5)$ with the identity automorphism.
Let

$$D = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

It is readily verified that the matrices:

$$\begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$$

satisfy the conditions for the spectral representation and are symmetric. The matrix D has eigenvalues 3 with an associated eigenspace generated by $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and 1 with an associated eigenspace generated by $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Since neither eigenspace has a vector with unit length, there cannot exist a unitary transform which carries D into a diagonal matrix.

It should be noted that the reason the matrix D of Example 3 is not unitarily diagonalizable is because the base field is not large enough. If, in fact, the base field were algebraically closed this type of situation could not occur.

THEOREM 2: *Let* F *be an algebraically closed field of characteristic* $\neq 2$ *and* A *a matrix over* F. *Then condition* (4) *and condition* (3) *are equivalent.*

PROOF: That (4) implies (3) was shown above. Assume that A has a spectral decomposition with Hermitian idempotents. Then A must be diagonalizable: $A=BDB^{-1}$. Assume that $D=\text{diag}(s_1I_{m_1}, s_2I_{m_2}, \ldots, s_kI_{m_k})$ and define, as in Theorem 1, D_i to be the matrix obtained by using 1 in place of s_i and 0 in place of s_j for $j \neq i$. If we let $E_i=BD_iB^{-1}$ we obtain a spectral representation. Since the principal idempotents are uniquely determined, [2] the E_i must be Hermitian. Hence:

$$E_i=BD_iB^{-1}=(B^{-1})^*D_iB^*.$$

Consequently, the matrix B^*B must commute with D_i for each i. Thus, B^*B has a block diagonal form with the ith block corresponding to, and having the same dimension as, D_i. The m_i vectors of B which correspond to the ith block of B^*B define the eigenspace associated with s_i. Since there exists an orthogonal basis to this eigenspace, [8] we can assume that the m_i vectors of B in question are orthogonal. There is no loss of generality in assuming that B^*B is diagonal by applying the above arguments to each eigenspace. The matrix B is nonsingular, so that each of the diagonal elements of B^*B must be nonzero. Since the base field is assumed to be large enough to contain the square roots of each diagonal element of B^*B, the eigenvectors can be assumed to be normalized so that B is unitary. *Q.E.D.*

In order to gain insight into the structure of normal matrices over an arbitrary field two problems are treated. The first is studied in section 4, namely, to characterize the normal matrices which are unitarily diagonalizable. Since this is a stronger condition than (1), (2), or (3) we already have several necessary conditions; if we assume the base field is closed and of characteristic $\neq 2$, then condition (3) also becomes sufficient. It thus appears that the set of unitarily diagonalizable matrices over a closed field of characteristic $\neq 2$ is sufficiently small to permit meaningful analysis and sufficiently large to include as a special case the normal matrices over the complex field. The concept of EPr has proven to be a useful tool in the analysis of normality, and will be a key element in the study.

At the other extreme, normal matrices need not be diagonalizable, no less unitarily diagonalizable (see Example 2). The second problem, treated in section 5, is a characterization of the most fundamental matrices of this extremity, namely, those matrices which are normal and similar to a single Jordan block. It is shown in section 5 that when conjugation is defined by the identity such matrices have a well-defined structure dependent on the parity of the order: those matrices which are of even order must be symmetric; those of odd order may be nonsymmetric but must adhere to a specified form. In addition the existence of such matrices yields interesting conclusions about the geometry of the underlying vector space.

3. EP Matrices

A matrix A which satisfies the condition:

$$Ax=0 \qquad \text{if and only if} \qquad A^*x=0$$

is called an EP matrix. If A has rank r, then A is an EPr matrix.

It has been shown that the EP condition is necessary for unitary diagonalizability [12]. However, every nonsingular matrix is EP. Consequently, this condition is not sufficient. In this section the known results on EP matrices are reviewed and a more restrictive class of matrices, the universal EP matrices, will be defined. Finally, the known characterization of normal EP matrices will be reviewed and a characterization of normal universal EP matrices will be given.

THEOREM 3 [6, 7]: *The following statements are equivalent over an arbitrary field:*

(1) A *is an* EP *matrix.*

(2) A *is congruent to the direct sum of a nonsingular matrix* D *and a zero matrix.*

(3) *There exists a matrix* N *such that* $A^* = NA$.

(4) *There exists a nonsingular matrix* N *such that* $A^* = NA$.

(5) A *can be represented as:*

$$A = P\begin{pmatrix} D & DX^* \\ XD & XDX^* \end{pmatrix} P^* = P\begin{pmatrix} I & 0 \\ X & I \end{pmatrix}\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} I & X^* \\ 0 & I \end{pmatrix} P^*$$

where P *is a permutation matrix and* D *is a square nonsingular matrix.*

(6) A *and* A^* *have the same range space.*

From the definition of *EP* and condition (2) of Theorem 3 it follows that:

THEOREM 4: *Let* F *and* K *be fields,* $F \subseteq K$, *and let* A *be a matrix with entries from* F. *Then* A *is* EP *with respect to* F *if and only if* A *is* EP *with respect to* K.

When normality and *EP* are combined the following is obtained:

THEOREM 5 [10]: *A necessary and sufficient condition that* A *be a normal* EP *matrix is that there exists a nonsingular matrix* M *such that:*

$$A^* = MA = AM.$$

It is convenient to use the following variant of *EP*:

DEFINITION 1: Let *A* be a matrix with entries from a field *F* which contains all the characteristic roots of *A*. If every polynomial in *A* with coefficients from *F* is an *EP* matrix, then *A* is a *universal* EP *matrix.*

Example 4 demonstrates that universal *EP* is more restrictive than *EP*. However, from condition (2) of Theorem 3 it is readily seen that universal *EP* is still necessary for unitary diagonalizability.

EXAMPLE 4: Matrix *EP* but not universal *EP*. Let the base field be the algebraic closure of *GF*(5) with identity automorphism.

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

The matrix *E* is nonsingular, hence *EP*. However, $E+I$ is not *EP*.

The following theorem characterizes the normal universal *EP* matrices:

THEOREM 6: *Let* A *be a normal matrix with entries from a field* F *which contains all of the characteristic roots* $s_1, s_2, \ldots, s_k$ *of* A. *If each of the polynomials*

$$A - s_i I \qquad i = 1, 2, \ldots, k$$

is an EP *matrix then* A *is a universal* EP *matrix.*

PROOF: Let

$$p(x) = p_m x^m + p_{m-1} x^{m-1} + \ldots + p_0$$

be an irreducible polynomial and set

$$\bar{p}(x) = \bar{p}_m x^m + \bar{p}_{m-1} x^{m-1} + \ldots + \bar{p}_0.$$

Then

$$[p(A)]^* = \bar{p}(A^*).$$

479-206 O - 73 - 3

CASE 1: Let $p(x)=c(x-s_i)$ for some i, $1 \leq i \leq k$, $c \in F$, $c \neq 0$. Then

$$p(A)=c(A-s_iI)$$

$$[p(A)]^*=\bar{c}(A^*-\bar{s}_iI).$$

By Theorem 5, there exists a nonsingular matrix M_i such that

$$A^*-\bar{s}_iI=M_i(A-s_iI)=(A-s_iI)M_i.$$

Clearly

$$[p(A)]^*=\bar{c}c^{-1}M_ip(A)=p(A)\bar{c}c^{-1}M_i.$$

Set $M_p=\bar{c}c^{-1}M_i$. Then M_p commutes with A and

$$[p(A)]^*=M_pp(A)=p(A)M_p.$$

CASE 2: Let $p(x)$ not be a multiple of any of the polynomials $x-s_i$, $i=1, 2, \ldots, k$. Then $p(A)$ is nonsingular. Set

$$M_p=[p(A)]^*[p(A)]^{-1}.$$

Since A is normal

$$[p(A)]^*=M_pp(A)=p(A)M_p$$

and M_p commutes with A.

Now let $f(x)$ be any polynomial and express $f(x)$ as a product of irreducible polynomials

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\ \ldots\ p_r(x)^{e_r}.$$

Then

$$[f(A)]^*=[p_1(A)^{e_1}]^*[p_2(A)^{e_2}]^*\ \ldots\ [p_r(A)^{e_r}]^*.$$

Defining M_{p_i} as in Case 1 we obtain

$$[f(A)]^*=M_ff(A)$$

where

$$M_f=M_{p_1}^{e_1}M_{p_2}^{e_2}\ \ldots\ M_{p_r}^{e_r}.$$

Clearly M_f is nonsingular and $f(A)$ is an EP matrix. *Q.E.D.*

4. Unitarily Diagonalizable Matrices

In this section criteria are given which, when combined with the universal EP property, form necessary and sufficient conditions for unitary diagonalizability over an arbitrary algebraically closed field of characteristic $\neq 2$.

Let A be a square matrix of order n with entries from F, and let $m(x)$ be the minimal polynomial of A. Express $m(x)$ as

$$m(x)=p_1(x)^{e_1}p_2(x)^{e_2}\ \ldots\ p_s(x)^{e_s} \tag{4-1}$$

where $p_1(x)$, $p_2(x)$, $\ldots$, $p_s(x)$ are distinct irreducible polynomials. Let us denote the vector space of all n dimensional column vectors with entries in F by F^n and let $N(B)$ denote the column null space of the matrix B, that is,

$$N(B)=\{x \mid x \in F^n,\ Bx=0\}.$$

According to the Primary Decomposition Theorem [5]

$$F^n = N[p_1(A)^{e_1}] \oplus N[p_2(A)^{e_2}] \oplus \cdots \oplus N[p_s(A)^{e_s}].$$

For vectors x and y belonging to F^n, we say that x and y are orthogonal if $x^*y = 0$. Two subspaces U and V of F^n are orthogonal if $x^*y = 0$ for all $x \in U$, $y \in V$. When U and V are orthogonal and have a zero intersection, we write

$$U \perp V.$$

LEMMA 1: *Let* A *be a normal matrix, let* r(x) *and* q(x) *be relatively prime polynomials and let* q(A) *be an* EP *matrix. Then*

$$N[r(A)] \perp N[q(A)].$$

PROOF: Since $r(x)$ and $q(x)$ are relatively prime, it is clear that

$$N[r(A)] \cap N[q(A)] = 0. \tag{4-2}$$

It remains to show that $N[r(A)]$ and $N[q(A)]$ are orthogonal. Let $x \in N[r(A)]$, $y \in N[q(A)]$. Then

$$0 = x^*[q(A)y] = [x^*q(A)]y = [q(A)^*x]^*y.$$

Thus $q(A)^*N[r(A)]$ is orthogonal to $N[q(A)]$. Since A is a normal matrix, it follows that $N[r(A)]$ is A^*-invariant and hence

$$q(A)^*N[r(A)] = \bar{q}(A^*)N[r(A)] \subset N[r(A)]. \tag{4-3}$$

Since $q(A)$ is an EP matrix there exists a nonsingular matrix M such that

$$q(A)^* = Mq(A).$$

Thus,

$$q(A)^*N[r(A)] = Mq(A)N[r(A)]. \tag{4-4}$$

However, because $N[r(A)]$ is A-invariant, we have

$$q(A)N[r(A)] \subset N[r(A)]. \tag{4-5}$$

Also, it follows from (4-2) that

$$\dim \{q(A)N[r(A)]\} = \dim \{N[r(A)]\}. \tag{4-6}$$

Combining (4-5) and (4-6) we have

$$q(A)N[r(A)] = N[r(A)]. \tag{4-7}$$

Substituting (4-7) into (4-4) yields

$$q(A)^*N[r(A)] = MN[r(A)]. \tag{4-8}$$

Since M is nonsingular it follows that

$$\dim \{MN[r(A)]\} = \dim \{N[r(A)]\}. \tag{4-9}$$

Finally, combining (4–3), (4–8) and (4–9) we have

$$q(A)^{*}N[r(A)]=N[r(A)].$$

and hence $N[r(A)]$ is orthogonal to $N[q(A)]$. *Q.E.D.*

An immediate consequence of Lemma 1 is:

THEOREM 7: *Let* A *be a normal, universal* EP *matrix whose minimal polynomial is given by (4–1). Then*

$$\mathrm{F^n=N[p_1(A)^{e_1}]\perp N[p_2(A)^{e_2}]\perp\ldots\perp N[p_s(A)^{e_s}].} \tag{4–10}$$

EXAMPLE 5: Normal *EP* matrix for which Theorem 7 is false. The matrix E of Example 4 is readily verified to be normal *EP* with minimal polynomial $m(x)=(x-3)(x-4)$. The null spaces of the two irreducible factors are spanned by the isotropic vectors $\begin{pmatrix}1\\2\end{pmatrix}$ and $\begin{pmatrix}1\\3\end{pmatrix}$ respectively. Clearly, these null spaces are not orthogonal.

Since F^n is nonsingular and (4–10) is an orthogonal decomposition of F^n, each of the subspaces $N[p_i(A)^{e_i}]$, $i=1, 2, \ldots, s$ is also nonsingular [1]. Hence, if F is a field of characteristic $\neq 2$ then each $N[p_i(A)^{e_i}]$ has a basis of mutually orthogonal nonisotropic vectors. If we form the matrix U by taking for its columns the vectors of the bases for the subspaces $N[p_i(A)^{e_i}]$, $i=1, 2, \ldots, s$, then $UU^{*}=U^{*}U$ is a nonsingular diagonal matrix and

$$U^{-1}AU=B_1\oplus B_2\oplus\ldots\oplus B_s$$

where B_i is a square matrix whose order is equal to $\dim N[p_i(A)^{e_i}]$ and whose minimal polynomial is $p_i(x)^{e_i}$. In order that U be a unitary matrix it is necessary to be able to normalize each of the vectors in the bases of the subspaces $N[p_i(A)^{e_i}]$. If A is diagonalizable then each B_i has unit dimension, and A is unitarily diagonalizable.

THEOREM 8: Let F be an algebraically closed field of characteristic $\neq 2$ and let A be a square matrix with entries from F. Then a set of necessary and sufficient conditions that A be unitarily similar to a diagonal matrix is:

(1) A is similar to a diagonal matrix.

(2) A is normal.

(3) A is universal *EP*.

PROOF: The sufficiency follows from the above arguments. The necessity of (1) and (2) is clear. Since a diagonal matrix is an *EP* matrix, and since the *EP* property is invariant under congruence, it follows that every polynomial in A is an *EP* matrix. *Q.E.D.*

For a matrix A with entries from the complex field, Schwerdtfeger [12] has called the matrix $A^{*}A$ the *Gram matrix* of A, and has shown that the Gram matrix of A always has the same rank as A. When the entries of A are from an arbitrary field, it is possible for A to have a greater rank than its Gram matrix (see Example 2).

We are now able to characterize the unitarily-diagonalizable matrices over suitable base fields without hypothesizing diagonalizability.

THEOREM 9: *Let* F *be an algebraically closed field of characteristic* $\neq 2$, *and let* A *be a square matrix with entries from* F. *Then a set of necessary and sufficient conditions that* A *be unitarily similar to a diagonal matrix is:*

(1) A *is universal* EP

(2) *For every* $\mathrm{c}\in\mathrm{F}$, $\mathrm{A}-\mathrm{cI}$ *has the same rank as its Gram matrix.*

PROOF: The necessity of (1) was shown in Theorem 8; the necessity of (2) is clear.

Let A be a matrix satisfying (1) and (2). Each of the polynomials $p_i(x)$ of (4–1) is linear since F is algebraically closed. Let $s_1, s_2, \ldots, s_k$ be the characteristic roots of A. By Theorem 3 there exists, for each i, a nonsingular matrix M_i such that:

$$(A - s_i I)^* = M_i (A - s_i I).$$

Hence:

$$(A - s_i I)^* (A - s_i I) = M_i (A - s_i I)^2.$$

Consequently, by (2), the matrices $(A - s_i I)^2$ and $(A - s_i I)$ have the same rank. Thus s_i is a simple characteristic root of A, and each of the exponents e_i of (4–1) is one. Hence A is diagonalizable, and F^n has a basis consisting of characteristic vectors of A. However, if x is a characteristic vector of A corresponding to any characteristic root s then:

$$(A^* - \bar{s} I) x = (A - sI)^* x = 0.$$

Thus:

$$AA^* x = \bar{s} A x = \bar{s} s x = A^* (sx) = A^* A x$$

from which we have:

$$(AA^* - A^* A) x = 0$$

and consequently A is normal. *Q.E.D.*

5. Normal Matrices Similar to a Single Jordan Block

In this section normal matrices having a single elementary divisor of the form $(x-s)^i$ are characterized and studied. The base field, F, is of characteristic $\neq 2$, and has an arbitrary involutory automorphism defining conjugation.

DEFINITION 2: A matrix, A, is *indecomposable* if A has a single elementary divisor of the form $(x-s)^i$. That is, if A is similar to a single Jordan block of the following form:

$$K = \begin{pmatrix} s & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & s & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & s & 1 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & s & \cdots & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & s & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & s & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & s & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & s \end{pmatrix} \tag{5–1}$$

Note that in the above definition of indecomposability the matrix A not only has a single elementary divisor over the base field but also has a single elementary divisor over all extension fields. This is, therefore, a more restrictive definition than is sometimes found where indecomposability assumes only a single elementary divisor over the base field [11].

EXAMPLE 6: Normal indecomposable matrix. Let the base field be $GF(5)$ with indentity automorphism. Let

$$F = \begin{pmatrix} 0 & 3 & 4 & 2 & 1 \\ 2 & 1 & 3 & 4 & 2 \\ 1 & 3 & 4 & 0 & 0 \\ 2 & 1 & 0 & 1 & 3 \\ 1 & 3 & 0 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 3 & 4 \\ 0 & 2 & 3 & 4 & 4 \\ 0 & 1 & 4 & 1 & 0 \\ 2 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 3 & 4 \\ 0 & 2 & 3 & 4 & 4 \\ 0 & 1 & 4 & 1 & 0 \\ 2 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}^{-1}$$

The normality of F is readily verified.

THEOREM 10: *Let* A *be an indecomposable matrix over* F. *Then the following are equivalent:*

(1) A *is normal.*

(2) *There exists a polynomial with scalar coefficients such that* $A^* = p(A)$.

PROOF: That condition (2) implies (1) is clear. It remains to prove the converse. Let K be the upper Jordan block corresponding to A, and let H be a similarity transform which carries A to K:

$$H^{-1}AH = K.$$

The normality of A implies that

$$(HKH^{-1})^*(HKH^{-1}) = (HKH^{-1})(HKH^{-1})^*$$

which can be written as

$$[(H^*H)^{-1}K^*(H^*H)]K = K[(H^*H)^{-1}K^*(H^*H)].$$

Hence the matrix $(H^*H)^{-1}K^*(H^*H)$ commutes with the Jordan block matrix K and equivalently commutes with the matrix U having 1's on the first superdiagonal and 0's elsewhere. However, the only matrices which commute with U are upper triangular and constant on the diagonal and all superdiagonals [3]. Such a matrix has the following form:

$$\begin{pmatrix} a & b & c & d & . & . & . & y & z \\ 0 & a & b & c & . & . & . & . & y \\ 0 & 0 & a & b & c & . & . & . & . \\ 0 & 0 & 0 & a & b & . & . & . & . \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & 0 & a & b & c \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \end{pmatrix} \tag{5-2}$$

But a matrix of the form (5–2) also has the form of a polynomial in the matrix K where:

$$a = p(\lambda) \qquad b = p'(\lambda) \qquad c = \frac{p''(\lambda)}{2!} \qquad \text{etc.}$$

Thus the matrix $(H^*H)^{-1}K^*(H^*H)$ is expressible as a polynomial in K:

$$(H^*H)^{-1}K^*(H^*H) = p(K). \tag{5-3}$$

From eq (5–3) we obtain:

$$A^* = p(A). \qquad \textit{Q.E.D.}$$

EXAMPLE 7: Polynomial transform for normal indecomposable matrix. The matrix F of Example 6 satisfies the following equality:

$$F^* = F^4 + F^3 + 2F^2 - F.$$

On the basis of Theorem 10 we can characterize the indecomposable normal matrix A by the polynomial transformation which carries A into A^*. To a certain extent matrices have long been

characterized by this transformation; symmetric and skew-symmetric matrices are those in which the polynomial is the identity and negative identity, respectively. The following generalization of symmetry and skew-symmetry will be useful in the ensuing discussion:

DEFINITION 3: A matrix A is *unit-symmetric* if $A = uA^*$ for some scalar $u \neq 0$.

If the matrix A is not the zero matrix then $A = uA^*$ implies $A = (u\bar{u})A$ and consequently the scalar u must have unit modulus.

If the automorphism is the identity then a unit-symmetric matrix is either symmetric or skew-symmetric since the only scalars with unit modulus are $+1$ and -1; if, however, the automorphism is not the identity then the scalar u can lie anywhere on the "unit circle."

While the indecomposable matrix A can have as its eigenvalue an arbitrary scalar in the field, it will be convenient to always assume that the eigenvalue is 0. The next lemma shows that any results obtained under this assumption can be readily translated to the case where the eigenvalue is arbitrary.

LEMMA 2: *Let the matrix* A *be indecomposable and let* a *be an arbitrary scalar in the field. Then* A *is normal if and only if* (A−aI) *is normal. Consequently,* A* *is expressible as a polynomial in* A *if and only if* (A−aI)* *is expressible as a polynomial in* (A−aI).

PROOF: The proof consists of verifying the equivalence of the two equations:

(1) $A^*A = AA^*$

(2) $(A - aI)^*(A - aI) = (A - aI)(A - aI)^*$.

The next lemma establishes a relatively weak but important set of necessary conditions on the polynomials which transform a normal indecomposable matrix with 0 eigenvalue into its conjugate transpose.

LEMMA 3: *Let* A* = p(A) *where* A *is an* n × n *normal indecomposable matrix with* 0 *eigenvalue. Then the polynomial* p(x) *has the following form:*

$$p(x) = a_{n-1}x^{n-1} + \ldots + a_1 x$$

where $a_1 \neq 0$.

PROOF: Since $A^n = 0$ it is not necessary to consider any term in the polynomial beyond x^{n-1}. Since the eigenvalue 0 is in the fixed field of the involutory automorphism, the matrix A is similar to A^*. Consider A^* in the following form:

$$A^* = p(A) = p(HKH^{-1}) = Hp(K)H^{-1} \tag{5-4}$$

where K is the upper Jordan block corresponding to A, and H is the similarity transform which carries A into K. Since A^* is similar to A, it follows from equation (5−4) that $p(K)$ is also similar to A. Hence, $p(K)$ is indecomposable with 0 eigenvalue. The matrix $p(K)$ has the upper triangular form shown in (5−2). Since the eigenvalue of $p(K)$ is zero it follows that the diagonal element is zero. But the diagonal element of $p(K)$ assumes the value $p(0)$. Then

$$p(0) = 0.$$

Since $p(K)$ is indecomposable it has rank $n-1$, and consequently the element defining the first superdiagonal is nonzero. But this superdiagonal is defined by $p'(0)$.

$$p'(0) \neq 0. \qquad \textit{Q.E.D.}$$

DEFINITION 4: A polynomial $p(x)$ which is of the form

$$p(x) = a_{n-1}x^{n-1} + \ldots + a_1 x$$

where $a_1 \neq 0$ is called an *nth order admissible polynomial*, or where the order is understood, simply an *admissible polynomial.*

It should be kept in mind that the term *n*th order refers to the dimension of the matrix A upon which the polynomial acts, and that an *n*th order admissible polynomial has degree at most $(n-1)$. The identity polynomial is an *n*th order admissible polynomial for all *n*. If $p(x)$ is admissible then $\bar{p}(x)$ is also admissible where $\bar{p}(x)$ is obtained from $p(x)$ by taking the conjugate of each coefficient.

It is possible to modify the usual concept of composition of polynomials in such a way that it is unchanged on the class of admissible polynomials, but it is better behaved as an algebraic structure. This is the basis of the next definition.

DEFINITION 5: Let $p(x)$ and $q(x)$ be the *n*th order admissible polynomials. Then the n *modular composition of* p(x) *and* q(x) is defined to be the polynomial obtained by first taking the ordinary composition of $p(x)$ and $q(x)$ as polynomials over the base field, and then dropping all terms of degree greater than $(n-1)$. The modular composition of $p(x)$ and $q(x)$ is denoted by $(p(x) \cdot q(x))$ or $(p \cdot q)(x)$.

It is clear from the definition that the modular composition of two *n*th order admissible polynomials is again an *n*th order admissible polynomial. Moreover, if $p(x)$ and $q(x)$ are *n*th order admissible polynomials, and if A is an $n \times n$ indecomposable matrix with 0 eigenvalue then:

$$p(q(A)) = (p \cdot q)(A).$$

THEOREM 11: *For any integer* n > 1, *the* n*th order admissible polynomials under the operation of* n *modular composition form a group.*

PROOF: It has already been noted that the admissible polynomials are closed under the modular composition. Associativity follows from the associativity of polynomials under ordinary composition. The polynomial x acts as the identity and is admissible. Let $p(x)$ and $q(x)$ be admissible polynomials:

$$p(x) = p_{n-1}x^{n-1} + \ldots + p_1 x \qquad p_1 \neq 0$$

$$q(x) = q_{n-1}x^{n-1} + \ldots + q_1 x \qquad q_1 \neq 0.$$

In order that $q(x)$ be the left inverse of $p(x)$ the following equation must hold:

$$q_{n-1}(p_{n-1}x^{n-1} + \ldots + p_1 x)^{n-1} + \ldots + q_1(p_{n-1}x^{n-1} + \ldots + p_1 x) \doteq x \qquad (5\text{–}5)$$

where the symbol $\doteq$ refers to a congruent equality in which all terms above $(n-1)$ are ignored. Equation (5–5) is equivalent to the system of $(n-1)$ equations:

$$q_1 p_1 = 1$$

$$q_i p_1^i + f_i\,(q_1, \ldots, q_{i-1}, p_1, \ldots, p_{i-1}) + q_1 p_i = 0 \qquad i = 2, \ldots, (n-1) \qquad (5\text{–}6)$$

where f_i is a well-defined function of q_j, p_j for $j < i$.

From the form of eq (5–6) it is clear that for a given polynomial $q(x)$, the polynomial $p(x)$ is uniquely determined by a simple recursive relationship. Conversely, given $p(x)$, then the polynomial $q(x)$ is uniquely determined. Thus the left and right inverses of a given admissible polynomial exist and are unique. Hence the set of admissible polynomials under modular composition form a group. *Q.E.D.*

EXAMPLE 8: Group of admissible polynomials. The following is the group table of the third order admissible polynomials over $GF(3)$.

	x	$2x$	x^2+x	x^2+2x	$2x^2+x$	$2x^2+2x$
x	x	$2x$	x^2+x	x^2+2x	$2x^2+x$	$2x^2+2x$
$2x$	$2x$	x	$2x^2+2x$	$2x^2+x$	x^2+2x	x^2+x
x^2+x	x^2+x	x^2+2x	$2x^2+x$	$2x^2+2x$	x	$2x$
x^2+2x	x^2+2x	x^2+x	$2x$	x	$2x^2+2x$	$2x^2+x$
$2x^2+x$	$2x^2+x$	$2x^2+2x$	x	$2x$	x^2+x	x^2+2x
$2x^2+2x$	$2x^2+2x$	$2x^2+x$	x^2+2x	x^2+x	$2x$	x

Since this group is nonabelian it is isomorphic to S_3. In general, the group of jth order admissible polynomials over $GF(n)$ has order $n^{j-2}(n-1)$.

The admissible polynomials, having been structured as a group, can now be partitioned according to the following equivalence relationship:

DEFINITION 6: The admissible polynomials $p(x)$ and $q(x)$ are *equivalent admissible polynomials* if there exists an admissible polynomial $r(x)$ such that

$$\bar{r}(x)^{-1} \cdot p(x) \cdot r(x) = q(x).$$

EXAMPLE 9: Equivalence classes of admissible polynomials. The following equivalence classes result from the third order admissible polynomials over $GF(3)$ (see Example 8).

(1) $\{x\}$
(2) $\{2x, x^2+2x, 2x^2+2x\}$
(3) $\{x^2+x, 2x^2+x\}$.

If a polynomial is to transform an indecomposable matrix with 0 eigenvalue into its conjugate transpose it must be admissible. However, this necessary condition can be strengthened considerably; that is, the group of admissible polynomials includes many polynomials which are incapable of transforming such a matrix into the conjugate transpose.

LEMMA 4: *Let the* n × n *matrix* A *be indecomposable with* 0 *eigenvalue and let* p(x) *be a polynomial such that* A* = p(A). *Then the polynomial* $(\bar{p} \cdot p)(x)$ *is the identity polynomial. Consequently* p′(0) *has unit modulus.*

PROOF: Since $A^* = p(A)$ it follows that $A = \bar{p}(A^*)$. Hence:

$$A = \bar{p}(p(A)) = (\bar{p} \cdot p)(A).$$

This same polynomial identity holds for all matrices similar to A. In particular, it holds for the upper Jordan block matrix U consisting of 1's on the first superdiagonal and 0's elsewhere:

$$U = (\bar{p} \cdot p)(U). \tag{5-7}$$

From eq (5–7) it is seen that the first order term of $(\bar{p} \cdot p)$ has a unit coefficient and that all higher order terms are zero; hence, $(\bar{p} \cdot p)(x) = x$. Since $p(0) = 0$ (Lemma 3) it follows that:

$$(\bar{p} \cdot p)'(0) = \bar{p}'(0) \cdot p'(0).$$

Hence $p'(0)$ has unit modulus. *Q.E.D.*

THEOREM 12: *Let the* n × n *matrix* A *be indecomposable with* 0 *eigenvalue and let* p(x) *be a polynomial such that* A* = p(A). *Then* p(x) *is equivalent to the polynomial* r(x) = x/p′(0) *where* p′(0) *has unit modulus.*

PROOF: Define a polynomial $q(x)$ as follows:

$$q(x)=p(x)+p'(0)x.$$

Since the first order term of $q(x)$ has the coefficient $2p'(0)\neq 0$ it follows that $q(x)$ is admissible. From Lemma 4 it is known that $(\bar{p}\cdot p)(x)=x$. Hence:

$$(\bar{q}(x)-\overline{p'(0)}x)\cdot(p(x))=x.$$

Applying the left distributive law which follows from this distributive property of polynomials, we obtain:

$$\bar{q}(x)\cdot p(x)=x+(\overline{p'(0)}x)\cdot(p(x))=(\overline{p'(0)}x)\cdot(q(x)). \tag{5-8}$$

Hence:

$$p(x)=(\bar{q}(x))^{-1}\cdot(\overline{p'(0)}x)\cdot(q(x)). \qquad Q.E.D.$$

EXAMPLE 10: Equivalence of transforming polynomial to polynomial of form $x/p'(0)$. The transforming polynomial of Example 7, $p(x)=x^4+x^3+2x^2-x$, is equivalent to the polynomial $-x$:

$$(x^3+x^2+x)^{-1}\cdot p(x)\cdot(x^3+x^2+x)=-x.$$

EXAMPLE 11: Examples of normal indecomposable matrices corresponding to polynomials of form $x/p'(0)$. For base field $GF(3)$ the only polynomials equivalent to polynomials of the form $x/p'(0)$ are in equivalence classes (1) and (2) of Example 9. Matrices corresponding to these four polynomials are:

$$G_1=\begin{pmatrix}1&0&1\\0&2&2\\1&2&0\end{pmatrix}=\begin{pmatrix}1&1&2\\1&2&2\\2&0&2\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}1&1&2\\1&2&2\\2&0&2\end{pmatrix}^{-1} \qquad G_1^t=G_1$$

$$G_2=\begin{pmatrix}0&2&1\\1&0&2\\2&1&0\end{pmatrix}=\begin{pmatrix}1&1&1\\1&2&1\\1&0&2\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}1&1&1\\1&2&1\\1&0&2\end{pmatrix}^{-1} \qquad G_2^t=-G_2$$

$$G_3=\begin{pmatrix}2&1&0\\0&2&1\\1&0&2\end{pmatrix}=\begin{pmatrix}1&2&2\\1&0&1\\1&1&1\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}1&2&2\\1&0&1\\1&1&1\end{pmatrix}^{-1} \qquad G_3^t=G_3^2+2G_3$$

$$G_4=\begin{pmatrix}1&2&0\\0&1&2\\2&0&1\end{pmatrix}=\begin{pmatrix}1&2&1\\1&1&2\\1&0&1\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}1&2&1\\1&1&2\\1&0&1\end{pmatrix}^{-1} \qquad G_4^t=2G_4^2+2G_4.$$

In the above development, a normal indecomposable matrix with 0 eigenvalue is characterized by the polynomial which transforms the given matrix into the conjugate transpose. In the following development the attention is switched to the matrix itself.

LEMMA 5: *Let* A *be an* n × n *matrix and* p(x) *be an* n*th order admissible polynomial.*

(1) *If* A *is indecomposable with* 0 *eigenvalue then* p(A) *is also indecomposable with* 0 *eigenvalue.*

(2) *If* A *is normal then* p(A) *is also normal.*

PROOF: If A is indecomposable with 0 eigenvalue then A is similar to the matrix U having 1's on the first superdiagonal and 0's elsewhere. Hence $p(A)$ is similar to $p(U)$ where $p(U)$ has the form shown in (5–2). Since $p(0)=0$ it follows that the diagonal of $p(U)$ is zero and that the only eigenvalue of $p(U)$ is zero. Since $p'(0)\neq 0$ it follows that the first superdiagonal of $p(U)$ is nonzero and consequently, that $p(U)$ is indecomposable. Finally, since $p(A)$ is similar to $p(U)$ it follows that $p(A)$ is also indecomposable with 0 eigenvalue.

If A is normal then it is readily verified that $p(A)$ is normal for any polynomial $p(x)$. *Q.E.D.*

LEMMA 6: *Let the* n × n *matrix* A *be indecomposable normal with* 0 *eigenvalue. Then there exists an* n × n *unit-symmetric indecomposable matrix* B *with* 0 *eigenvalue and an admissible polynomial* r(x) *such that* A = r(B) *and* B = r^{-1}(A).

PROOF: Define the admissible polynomial $q(x)$ as in Theorem 12:

$$q(x)=p(x)+p'(0)x$$

where $p(x)$ is the polynomial which transforms A into A^*. Evaluating eq (5–8) at $x=A$ the following is obtained:

$$\overline{q}(p(A))=\overline{p'(0)}\overline{q}(A). \tag{5–9}$$

Define the matrix B as follows:

$$B=q(A).$$

Since $q(x)$ is admissible the matrix B is indecomposable with 0 eigenvalue and normal by Lemma 5. The actual form of B^* can be evaluated as follows:

$$B^*=\overline{q}(A^*)=\overline{q}(p(A)). \tag{5–10}$$

From eqs (5–9) and (5–10) and the definition of B it follows that:

$$B^*=\overline{p'(0)}B.$$

Hence B is unit-symmetric.

Since $q(x)$ is admissible and the matrices B and A are indecomposable with 0 eigenvalue, it follows that $q^{-1}(x)$ can be applied to both sides of the equation defining B to obtain

$$A=q^{-1}(B).$$

The lemma is proved if we define the polynomial $r(x)=q^{-1}(x)$. *Q.E.D.*

EXAMPLE 12: Transformation of normal indecomposable matrix into unit-symmetric indecomposable matrix. The matrix F of Example 6 can be obtained from or transformed to the following skew-symmetric indecomposable matrix:

$$H=\begin{pmatrix}0&3&4&0&0\\2&0&0&0&0\\1&0&0&3&4\\0&0&2&0&0\\0&0&1&0&0\end{pmatrix}=\begin{pmatrix}0&0&1&0&1\\0&2&0&2&0\\0&1&0&0&0\\2&0&0&0&0\\1&0&0&0&1\end{pmatrix}\begin{pmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&0&0&0&0\end{pmatrix}\begin{pmatrix}0&0&1&0&1\\0&2&0&2&0\\0&1&0&0&0\\2&0&0&0&0\\1&0&0&0&1\end{pmatrix}^{-1}$$

The transformations are as follows:

$$F=H^3+H^2+H$$

$$H=F^3-F^2+F.$$

The results of Lemma 6 can be readily extended to obtain a complete characterization of normal indecomposable matrices with arbitrary eigenvalues.

THEOREM 13: *Let the matrix* A *be indecomposable. Then* A *is normal if and only if* A *can be represented in the form* A = r(B) *where the matrix* B *is unit-symmetric indecomposable with* 0 *eigenvalue and* $r'(0) \neq 0$.

PROOF: Assume first that A is normal indecomposable with eigenvalue s. Then $(A-sI)$ is normal indecomposable with 0 eigenvalue. By Lemma 6 there exists a unit-symmetric indecomposable matrix B with 0 eigenvalue and an admissible polynomial $q(x)$ such that:

$$(A-sI)=q(B).$$

Hence:

$$A=q(B)+sI=r(B).$$

Since $q(x)$ is admissible it follows that $q'(0) \neq 0$. Hence $r'(0) \neq 0$. The converse follows from the fact that any polynomial in a normal matrix is again normal. *Q.E.D.*

On the basis of Theorem 13 we can readily obtain all the indecomposable normal matrices from the set of indecomposable unit-symmetric matrices with 0 eigenvalue.

If the involutory automorphism which defines conjugation is the identity, then the problem is greatly simplified. For this special case the only unit-symmetric matrices are those which are either symmetric or skew-symmetric. Section 6 of this paper treats this case in detail.

6. Indecomposable Normal Matrices With Entries From a Field in Which Conjugation Is Defined by the Identity Mapping

In this section the results of section 5 are extended for the special case in which the involutory automorphism defining conjugation is the identity mapping. To distinguish the present results from those obtained for an arbitrary involutory automorphism the transpose of a matrix will be denoted by A^t rather than by A^*.

The analog to Theorem 12 assumes the following form:

THEOREM 14: *Let the matrix* A *be indecomposable with* 0 *eigenvalue and let* p(x) *be a polynomial such that* $A^t = p(A)$. *Then* p'(0) *is either* $+1$ *or* -1. *If* $p'(0) = -1$ *then* p(x) *is equivalent to the negative identity polynomial,* $-x$. *If* $p'(0) = +1$ *then* p(x) *is the identity polynomial,* x.

PROOF: From Lemma 4, $p'(0)$ has unit modulus. Since the automorphism is the identity the only scalars with unit modulus are $+1$ and -1.

If $p'(0) = -1$ then $p(x)$ is equivalent to the negative identity by Theorem 12. If $p'(0) = +1$ then $p(x)$ is equivalent to the identity by the same theorem; however, the only polynomial which is equivalent to the identity polynomial is the identity itself. *Q.E.D.*

The characterization of the normal indecomposable matrices in terms of unit-symmetric matrices assumes the following form:

THEOREM 15: *Let the matrix* A *be indecomposable. Then* A *is normal if and only if one of the following conditions is satisfied:*

(1) A *is symmetric.*

(2) *There exists a skew-symmetric indecomposable matrix* B *with* 0 *eigenvalue and a polynomial* r(x) *where* $r'(0) \neq 0$ *such that:*

$$A = r(B).$$

Conditions (1) and (2) cannot be simultaneously satisfied.

PROOF: Assume first that A is normal. By Theorem 13 there exists a unit-symmetric indecomposable matrix B with 0 eigenvalue and a polynomial $r(x)$, $r'(0) \neq 0$, such that:

$$A=r(B).$$

Since the automorphism is the identity, the matrix B is either symmetric or skew-symmetric. If B is symmetric then A is symmetric; if B is skew-symmetric then condition (2) is satisfied.

The converse follows from the fact that a polynomial in a normal matrix is again normal.

It remains to show that conditions (1) and (2) can not be simultaneously satisfied. Suppose the matrix A satisfies both conditions. If A has order n then $B^n=0$ and we can assume that $r(x)$ has degree less than or equal to $n-1$:

$$A=r_{n-1}B^{n-1}+\ \ .\ .\ .+r_2B^2+r_1B^1+r_0I. \tag{6-1}$$

Since A is symmetric and B skew-symmetric the following equation is obtained by taking the transpose of eq (6-1):

$$A=\pm r_{n-1}B^{n-1}\mp .\ .\ .+r_2B^2-r_1B^1+r_0I. \tag{6-2}$$

If n is an odd integer subtract eq (6-2) from (6-1); if n is an even integer add the two equations to obtain:

$$0=2\{r_{n-2}B^{n-2}+r_1B\ (r_0I)\}. \tag{6-3}$$

Since B is indecomposable with 0 eigenvalue its minimal polynomial is given by x^n. But eq (6-3) implies that B is annihilated by a polynomial of degree $n-2$. Contradiction. *Q.E.D.*

It should be noted that any skew-symmetric indecomposable matrix has zero eigenvalue when conjugation is defined by the identity. For if B is skew-symmetric indecomposable with eigenvalue s, then B^t also has eigenvalue s. But $B^t=-B$, and consequently B^t has eigenvalue $-s$. Hence $s=0$.

The polynomials which relate a normal indecomposable matrix with 0 eigenvalue to its transpose are completely defined by the following set: the identity polynomial plus the set of polynomials in the equivalence class of the negative identity. A more explicit representation of this set of polynomials is desirable but has not been obtained.

THEOREM 16: *Let* A *be normal indecomposable. If* A *is not symmetric then* A *is of odd order. Symmetric indecomposable matrices exist for both odd and even orders.*

PROOF: The existence of symmetric matrices of odd and even orders and nonsymmetric matrices of odd order is shown by Examples 13, 14, 15. If A is normal indecomposable but not symmetric then by Theorem 15 there exists a skew-symmetric indecomposable matrix with 0 eigenvalue, say B, of the same order. The rank of B is clearly one less than the order since it is similar to a matrix having all 0's except 1's on the first superdiagonal. It remains to observe that any skew-symmetric matrix has even rank [11]. *Q.E.D.*

EXAMPLE 13: Example of symmetric indecomposable matrix of even order. Base field $GF(5)$.

$$\begin{pmatrix}1&3\\3&4\end{pmatrix}=\begin{pmatrix}2&2\\1&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}2&2\\1&0\end{pmatrix}^{-1}.$$

EXAMPLE 14: Example of symmetric indecomposable matrix of odd order. Base field $GF(5)$.

$$\begin{pmatrix}0&0&2\\0&0&1\\2&1&0\end{pmatrix}=\begin{pmatrix}2&0&0\\1&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}2&0&0\\1&0&1\\0&1&0\end{pmatrix}^{-1}.$$

EXAMPLE 15: Example of skew-symmetric indecomposable matrix of odd order. Base field. $GF(5)$.

$$\begin{pmatrix}0&0&2\\0&0&1\\3&4&0\end{pmatrix}=\begin{pmatrix}2&0&0\\1&0&4\\0&1&0\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}2&0&0\\1&0&4\\0&1&0\end{pmatrix}^{-1}.$$

Theorem 16 indicates a fundamental difference between the symmetric and nonsymmetric normal indecomposable matrices. Since any polynomial of a symmetric matrix is clearly symmetric, polynomial transforms are not useful for studying the interrelationship between the symmetric and the nonsymmetric matrices. More complex tools are needed for any coexistence theorems for these two classes.

Theorem 16 also demonstrates a fundamental difference between normal indecomposable matrices of odd and even order. Since this parity effect is one which is often apparent in geometric structures, a study of the geometric implications of the underlying vector space is indicated. Several definitions and preliminary results are needed for the discussion of geometric properties.

DEFINITION 7: For a vector space V, the *radical* of V, rad V, is the subspace of all vectors of V which are orthogonal to V. If U^* denotes the subspace of V orthogonal to U then rad $U = U \cap U^*$. We say that V is *nonsingular* if rad $V = 0$. If rad $V = V$ then V is *isotropic*.

DEFINITION 8: A 2-dimensional nonsingular vector space which contains an isotropic vector is called a *hyperbolic plane*. An orthogonal sum of hyperbolic planes is a *hyperbolic space*.

A hyperbolic space is nonsingular and has even dimension. As in section 4, we will use the symbol $V \perp W$ to denote the orthogonal sum of the spaces V and W.

THEOREM 17 [1]: *Let* V *be nonsingular and* U *any subspace of* V. *Write* $\mathrm{U} = rad\ \mathrm{U} \perp \mathrm{W}$ *and let* $\mathrm{N}_1, \mathrm{N}_2, \ldots, \mathrm{N}_r$ *be a basis of rad* U. *Then we can find in* V *vectors* $\mathrm{M}_1, \mathrm{M}_2, \ldots, \mathrm{M}_r$ *such that each* $\mathrm{N}_1, \mathrm{M}_i$ *is a hyperbolic pair and such that the hyperbolic planes* $\mathrm{P}_i = (\mathrm{N}_i, \mathrm{M}_i)$ *are mutually orthogonal and also orthogonal to* W. V *will therefore contain the nonsingular space:*

$$\overline{\mathrm{U}} = \mathrm{P}_1 \perp \mathrm{P}_2 \perp \ldots \perp \mathrm{P}_r \perp \mathrm{W}$$

which, in turn, contains U.

THEOREM 18: *If* n *is an even integer then the following statements are equivalent:*

(1) F^n *is a hyperbolic vector space.*

(2) *There exist* $\mathrm{n} \times \mathrm{n}$ *symmetric indecomposable matrices over* F.

If n *is an odd integer, the following statements are equivalent:*

(1′) F^n *contains an* $\mathrm{n}-1$ *dimensional hyperbolic subspace.*

(2′) *There exist* $\mathrm{n} \times \mathrm{n}$ *symmetric indecomposable matrices over* F.

(3′) *There exist* $\mathrm{n} \times \mathrm{n}$ *skew-symmetric indecomposable matrices over* F.

(4′) *There exist* $\mathrm{n} \times \mathrm{n}$ *normal indecomposable matrices over* F.

PROOF: We will show first that the existence of any normal indecomposable matrix implies (1) for n even, or (1′) for n odd. Let A be a normal indecomposable matrix. If A is symmetric with eigenvalue s then $A - sI$ is indecomposable symmetric with 0 eigenvalue. If A is not symmetric then there exists, by Theorem 15, an indecomposable skew-symmetric matrix B which must have 0 eigenvalue. In either case we are assured of the existence of an indecomposable normal matrix with 0 eigenvalue.

Let $p(x)$ denote the polynomial transformation that carries the matrix B into B^t. Since B is either symmetric or skew-symmetric, the polynomial $p(x)$ will be correspondingly either the identity or the negative identity.

If H is the similarity transformation which carries B into the single Jordan block K:

$$B = HKH^{-1}$$

then the following is readily obtained:

$$(HKH^{-1})^t = B^t = p(B) = Hp(K)H^{-1}.$$

Hence:

$$(H^tH)p(K) = K^t(H^tH).$$

The matrix (H^tH) is the Gram matrix of the matrix H. Let L denote this Gram matrix so that the above assumes the form:

$$Lp(K)=K^tL.$$

Note that since H is a similarity transform it must be nonsingular; consequently the Gram matrix L is also nonsingular.

Since $p(x)$ is either the identity or the negative identity, the matrix $p(K)$ consists of all 0's except $+1$ or -1 on the first superdiagonal. Hence the first column of $Lp(K)$ is identically 0, and the first column of K^tL consists of 0 in the first place and $L_{i-1,1}$ in the ith place, $i>1$. Thus:

$$L_{1,1}=L_{2,1}=\ldots=L_{n-1,1}=0. \tag{6-4}$$

Since L is nonsingular, $L_{n,1}$ is nonzero.

Examining the second column of $Lp(K)$ it is found that eqs (6–4) imply that there are 0's in the first $n-1$ places. Comparing this to the second column of K^tL the following is obtained:

$$L_{1,2}=L_{2,2}=\ldots=L_{n-2,2}=0.$$

Continuing through the n-1st column we obtain:

$$(H^tH)_{i,j}=L_{i,j}=0 \text{ whenever } i+j\leq n. \tag{6-5}$$

If we consider a basis of F^n defined by the columns of the similarity transform H, h_i, $i=1, 2, \ldots, n$, then the length square of the basis vector h_i is given by the ith element along the diagonal of the Gram matrix L. If n is an even integer then eq (6–5) implies that the first $\frac{n}{2}$ vectors of this ordered basis are isotropic. If n is an odd integer then the first $\frac{(n-1)}{2}$ vectors of this ordered basis are isotropic.

If we define the subspace U to be generated by the first $\frac{n}{2}$ vectors in the basis h_i $\left(\frac{(n-1)}{2}\text{ if } n \text{ odd}\right)$, then the space F^n is seen to be hyperbolic (contain an $n-1$ dimensional hyperbolic subspace if n odd).

Next assume that n is even and F^n is a hyperbolic space. Then there exists $\frac{n}{2}$ orthogonal hyperbolic planes, say P_i, $i=1, 2, \ldots, \frac{n}{2}$. Associated with each P_i there is a basis of two isotropic vectors whose product is unity; let one of these vectors be designated h_i and the other designated h_{n+1-i}. When we run through the $\frac{n}{2}$ planes we obtain an ordered basis of n vectors, h_j, $j=1, 2, \ldots, n$, with the special property that for each j the vector h_j has a unit product with h_{n+1-j} and is orthogonal to the remainder of the basis. If a matrix H is formed by letting h_j be the jth column of H then the following is obtained:

$$H^tH=\begin{pmatrix}
0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & \cdot & \cdot & 1 & 0 & 0 & 0\\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\
0 & 0 & 0 & 1 & \cdot & \cdot & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0
\end{pmatrix}$$

i.e., the Gram matrix H^tH has 1's on the second diagonal and 0's elsewhere.

If K is an $n \times n$ single Jordan block then the following identity is readily obtained:

$$(H^tH)\, K = K^t\, (H^tH).$$

Hence:

$$HKH^{-1} = (HKH^{-1})^t. \tag{6–6}$$

The matrix HKH^{-1} is symmetric and indecomposable.

Finally, assume that n is an odd integer and that there exists an $n-1$ dimensional hyperbolic subspace of F^n. Call this subspace U, and let U^* denote the space of vectors orthogonal to U. Since F^n is nonsingular it follows that:

$$\dim U + \dim U^* = \dim F^n = n.$$

Hence U^* is generated by a single vector k. The subspace U is also nonsingular since it is hyperbolic; consequently, U and U^* must be disjoint. Thus we can write:

$$F^n = U \perp k$$

Suppose the vector k has length square c; that is, $k^tk = c$. As in the first part of the proof we separate the space U into a system of orthogonal hyperbolic planes, P_i, $i = 1, 2, \ldots, \frac{(n-1)}{2}$. Associated with each plane there is a basis of two isotropic vectors whose product is unity; let one of these vectors be designated h_i, and multiply the second vector by the scalar c and designate the resultant vector by h_{n+1-i}. Finally define the vector $h_{(n+1)/2}$ to be the vector k, so that we obtain an ordered basis, h_j, $j = 1, 2, \ldots, n$, with the special property that for each j the vector h_j has a product with h_{n+1-j} equal to the scalar c, and is orthogonal to the remainder of the basis. The matrix H is defined to have the jth column equal to the basis vector h_j so that the Gram matrix H^tH consists of c's on the second diagonal and 0's elsewhere. Equation (6–6) continues to hold, and the matrix HKH^{-1} is symmetric and indecomposable.

To obtain a skew-symmetric indecomposable matrix we modify the matrix H used immediately above in the following way: negate columns $\frac{(n+1)}{2} - i$ where i runs through the odd integers less than $\frac{(n+1)}{2}$. Call this new matrix M. Then the Gram matrix M^tM consists of an alternation of $+c, -c, +c, -c, \ldots$ along the second diagonal and 0's elsewhere:

$$M^tM = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & \pm c \\ 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & \mp c & 0 \\ 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & \pm c & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdot & \cdot & \mp c & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \mp c & \cdot & \cdot & 0 & 0 & 0 & 0 \\ 0 & 0 & \pm c & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 \\ 0 & \mp c & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 \\ \pm c & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 \end{pmatrix}.$$

If K is a single Jordan block with 0's along the diagonal then the following holds:

$$(M^tM)K = -K^t(M^tM).$$

Hence the matrix MKM^{-1} is skew-symmetric indecomposable. *Q.E.D.*

COROLLARY: *The existence of any normal indecomposable matrix over* F *implies the existence of both symmetric and nonsymmetric normal indecomposable matrices of odd order over* F.

PROOF: Let B be the given normal indecomposable matrix. If B is of odd order then the existence of symmetric and nonsymmetric normal indecomposable matrices follows from the equivalence of conditions (2′), (3′) and (4′). If B is of even order, say $2n$, then F^{2n} must be hyperbolic. Consequently, F^{2n+1} contains a $2n$ dimensional hyperbolic subspace. The existence of symmetric and nonsymmetric normal indecomposable matrices of order $2n + 1$ now follows from the equivalence of conditions (1′), (2′), and (3′). *Q.E.D.*

If n is an even number we have shown that normal indecomposable matrices must be symmetric (Theorem 16), and that such matrices exist if and only if the underlying vector space is hyperbolic (Theorem 18).

If n is odd we have demonstrated that a normal matrix B with eigenvalue s must satisfy one of the following (Theorem 14):

(1) B is symmetric

(2) $(B-sI)^t = p(B-sI)$ for some polynomial p equivalent to the negative identity.

Furthermore there exist matrices satisfying (1) if and only if there exist matrices satisfying (2) if and only if the underlying vector space is the direct product of a one dimensional space and a hyperbolic space (Theorem 18).

It remains to show that condition (2) above is the most restrictive condition which can be placed on the nonsymmetric normal indecomposable matrices of odd order. This is proven in the following theorem.

THEOREM 19: *If for some polynomial equivalent to the negative identity, say* p(x), *there exists an indecomposable matrix with* 0 *eigenvalue,* A, *such that* $A^t = p(A)$, *then for any polynomial equivalent to the negative identity there exists such an associated matrix.*

PROOF: Let $q(x)$ be an arbitrary polynomial in the equivalence class of $-x$. Then $q(x)$ and $p(x)$ are equivalent, and there exists an admissible polynomial $r(x)$ such that:

$$p(x) = (r^{-1} \cdot q \cdot r)(x).$$

Evaluating at A we obtain:

$$A^t = p(A) = (r^{-1} \cdot q \cdot r)(A).$$

Or equivalently:

$$r(A^t) = (q \cdot r)(A).$$

The left side of the above equation is equal to $(r(A))^t$ and the right side is equal to $q(r(A))$. Hence we obtain:

$$B^t = q(B)$$

where $B = r(A)$. Since $r(x)$ is admissible the matrix B is indecomposable with 0 eigenvalue. *Q.E.D.*

The preceding discussion demonstrates that if there are any normal indecomposable matrices over F then there is an abundant supply of such matrices: the corollary to Theorem 18 proves the existence of nonsymmetric normal indecomposable matrices, and Theorem 19 proves the existence of the full spectrum, in terms of the transposing polynomials, of such matrices.

479-206 O - 73 - 4

On the basis of Theorem 18 we are also able to establish the existence of normal indecomposable matrices of higher order by considering the orthogonal sum of hyperbolic spaces. Suppose that there exist $n \times n$ symmetric indecomposable matrices and $m \times m$ symmetric indecomposable matrices over F where both n and m are even integers. Since F^n and F^m are hyperbolic, it follows that $F^n \perp F^m$ is hyperbolic. Since the space $F^n \perp F^m$ is isomorphic to F^{n+m} it follows that there must exist $(n+m) \times (n+m)$ symmetric indecomposable matrices over F. If the integer n is even but m is odd then the vector space $F^n \perp F^m$ must contain a hyperbolic subspace of dimension $n+m-1$, and consequently there must exist normal indecomposable matrices of this order.

Of particular interest are those fields which contain 2-dimensional isotropic vectors. Examples of such fields are $GF(5)$ and the complex numbers (with, of course, identity automorphism). Since there exists a 2-dimensional isotropic vector there must exist 2×2 symmetric indecomposable matrices, for if (a, b) is isotropic then such a matrix is given by the following:

$$S = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} = \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}^{-1}.$$

Consequently, there must also exist 3×3 normal indecomposable matrices. Thus the vector space F^2 is hyperbolic and F^3 contains a 2-dimensional hyperbolic subspace. Now let n represent an arbitrary integer greater than 1. If n is even then the vector space F^n is hyperbolic since it is expressible in the form $F^2 \perp F^2 \perp \ldots \perp F^2$; consequently, there exist $n \times n$ normal indecomposable matrices over F. If, on the other hand, n is odd then the vector space F^n contains an $n-1$ dimensional hyperbolic subspace since it is expressible in the form $F^2 \perp F^2 \perp \ldots \perp F^2 \perp F$; consequently, there again exist $n \times n$ normal indecomposable matrices over the given field. Since any matrix of order 1 is normal indecomposable the following holds: If the base field has a 2-dimensional isotropic vector then there exist normal indecomposable matrices of all orders.

It should be noted that while the existence of normal indecomposable matrices of order $2n$ implies the existence of such matrices of order $2n+1$, the converse is not true. As a counterexample let F be a field for which there exists 3-dimensional isotropic vectors but there do not exist 2-dimensional isotropic vectors (e.g., $GF(7)$). Since there are no 2-dimensional isotropic vectors over F, the space of 2-dimensional vectors is not hyperbolic, and according to Theorem 18 there exist no 2×2 normal indecomposable matrices. However, since there do exist 3-dimensional isotropic vectors, the space of 3-dimensional vectors does contain a hyperbolic plane. Consequently, there must exist 3×3 normal indecomposable matrices (Theorem 18). Example 16 is a 3×3 normal indecomposable matrix over $GF(7)$.

EXAMPLE 16: Normal indecomposable matrix of order 3 where no such matrix of order 2 exists. Let the base field be $GF(7)$.

$$\begin{pmatrix} 0 & 3 & 5 \\ 4 & 0 & 6 \\ 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 0 \\ 1 & 1 & 0 \\ 5 & 0 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 2 & 0 \\ 1 & 1 & 0 \\ 5 & 0 & 6 \end{pmatrix}^{-1}.$$

While the existence of normal indecomposable matrices of even order imply the existence of such matrices of the next highest odd order, we are unable to go from odd order to the next highest even order. In other words, given that there exist normal indecomposable matrices of order n, it is not necessarily true that there exist such matrices of order m for $m > n$. As a counterexample we can again consider $GF(7)$. The vector space F^4 contains the following two independent, isotropic, orthogonal vectors

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 4 \\ 2 \\ 1 \end{pmatrix}.$$

Consequently F^4 is hyperbolic and there exist 4×4 and 5×5 indecomposable normal matrices. However, there do not exist any 6×6 normal indecomposable matrices over $GF(7)$. The proof of this is lengthy and has been put in section 7. Since F^7 can be expressed as the orthogonal sum of F^4 (which is hyperbolic) and F^3 (which contains a 2-dimensional hyperbolic subspace), it follows that F^7 contains a 6-dimensional hyperbolic subspace; consequently, there do exist 7×7 normal indecomposable matrices over this field.

7. Proof of Nonexistence of 6×6 Normal Indecomposable Matrices over $GF(7)$

If there exist normal indecomposable 6×6 matrices over $GF(7)$ then $GF(7)^6$ is hyperbolic and contains three independent, isotropic, orthogonal vectors. The following modifications of such a triplet of vectors does not affect the independence, orthogonality, or isotropicity:

(1) Addition of a multiple of one vector to a second vector.
(2) Permutation of the elements of each vector, always using the same permutation.
(3) Multiplication of any vector by a nonzero constant.

Using modification of types (1) and (2), the existence of any such triplet ensures the existence of three isotropic, orthogonal vectors having the following form:

$$\begin{pmatrix} x_1 \\ 0 \\ 0 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \quad \begin{pmatrix} 0 \\ y_2 \\ 0 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \end{pmatrix} \tag{7-1}$$

where x_1, y_2, and z_3 are nonzero. Since each of the three vectors are nonzero and since the spaces of one and two dimensional vectors over $GF(7)$ contain no isotropic vectors, each of these vectors must contain at least three nonzero elements.

LEMMA 7: *At most one vector of the triplet (7–1) contains exactly three nonzero elements.*

PROOF: Assume $x_6=0$, and suppose y_6 also equals zero. Since $x\cdot z=y\cdot z=0$ the following homogeneous equations hold:

$$x_4\cdot z_4+x_5\cdot z_5=0$$

$$y_4\cdot z_4+y_5\cdot z_5=0.$$

Consequently, (x_4, x_5) and (y_4, y_5) are linearly dependent (z contains at least three nonzero elements so that z_4 and z_5 cannot be simultaneously zero). Thus:

$$0=x\cdot y=s(x_4^2+x_5^2)$$

for some scalar s. But this is impossible since there are no 2-dimensional isotropic vectors over this base field. Hence $y_6\neq0$. Similarly $z_6\neq0$.

Since $x\cdot y=x_4\cdot y_4+x_5\cdot y_5=0$ where $x_4\neq0$, $x_5\neq0$, and since y_4 and y_5 cannot be simultaneously zero, it follows that y_4 and y_5 must be nonzero. Similarly, z_4 and z_5 are nonzero. *Q.E.D.*

LEMMA 8: *No vector of the triplet (7–1) has exactly three nonzero elements.*

PROOF: Assume $x_6=0$. Since $x\cdot y=x\cdot z=0$ the following homogeneous equations hold:

$$x_4\cdot y_4+x_5\cdot y_5=0$$

$$x_4\cdot z_4+x_5\cdot z_5=0.$$

Hence (y_4, y_5) and (z_4, z_5) must be dependent. We can thus consider the three vectors (7–1) to be in the following normalized form:

$$\begin{pmatrix} x_1 \\ 0 \\ 0 \\ 1 \\ x_5 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y_2 \\ 0 \\ 1 \\ -\frac{1}{x_5} \\ y_6 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ z_3 \\ 1 \\ -\frac{1}{x_5} \\ z_6 \end{pmatrix} \tag{7–2}$$

where the orthogonality of x and y and of x and z have been explicitly accounted for.

Since the vector $\mathbf{x}$ is isotropic the following holds:

$$x_1^2+1+x_5^2=0.$$

Hence:

$$x_5^2=6-x_1^2.$$

Since the only squares over $GF(7)$ are 1, 2, 4 it follows that x_5^2 must assume the value 2 or 4.

From the orthogonality of y and z we obtain:

$$1+\frac{1}{x_5^2}+y_6 \cdot z_6=0.$$

Substituting the two possible values of x_5^2 we obtain:

$$y_6 \cdot z_6 = x_5^2.$$

CASE 1: $x_5^2 = 2$.

Since y and z are isotropic the following equations hold:

$$y_2^2 + 1 + 4 + y_6^2 = 0$$

$$z_3^2 + 1 + 4 + z_6^2 = 0.$$

Hence:

$$y_2^2 = 2 - y_6^2 \neq 0.$$

$$z_3^2 = 2 - z_6^2 \neq 0.$$

Again using the fact that the only squares are 1, 2, 4 it follows that $y_6^2=z_6^2=1$. Hence $y_6 \cdot z_6=\pm 1=x_5^2$. Contradiction.

CASE 2: $x_5^2 = 4$.

In a similar way we obtain:

$$y_2^2 = 4 - y_6^2 \neq 0$$

$$z_3^2 = 4 - z_6^2 \neq 0.$$

Hence $y_6^2 = z_6^2 = 2$, and as a result: $y_6 \cdot z_6 = \pm 2 \neq x_5^2$. Contradiction. *Q.E.D.*

As a result of the above lemma if there are to exist three independent, isotropic, orthogonal vectors over $GF(7)$, they can be assumed to be of the form (7–1) where all terms written with letters are, in fact, nonzero. Assume that these vectors are normalized so that $x_1=y_2=z_3=2$. Then the following vectors are orthogonal, and have length 3:

$$\begin{pmatrix} x_4 \\ x_5 \\ x_6 \end{pmatrix}, \begin{pmatrix} y_4 \\ y_5 \\ y_6 \end{pmatrix}, \begin{pmatrix} z_4 \\ z_5 \\ z_6 \end{pmatrix}.$$

The following is a complete list of 3-dimensional vectors over $GF(7)$ having length 3:

$$\begin{pmatrix} \pm 1 \\ \pm 1 \\ \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 2 \\ \pm 2 \\ \pm 3 \end{pmatrix}, \begin{pmatrix} \pm 2 \\ \pm 3 \\ \pm 2 \end{pmatrix}, \begin{pmatrix} \pm 3 \\ \pm 2 \\ \pm 2 \end{pmatrix}.$$

It can be shown that there do not exist three orthogonal vectors in this set.

Hence there do not exist three orthogonal, isotropic, independent vectors over $GF(7)^6$, and consequently there do not exist any 6×6 normal indecomposable matrices over $GF(7)$.

8. Some Open Questions

1. Identify the group of the jth order admissible polynomials with entries from the field $GF(n^k)$.

2. Find the polynomials conjugate to $-x$. It can be shown that if

$$p(x)=p_{n-1}x^{n-1}+\ .\ .\ .+p_1x$$

is conjugate to $-x$ then

$$\begin{aligned} p_1&=-1, \\ p_3&=-p_2^2, \\ p_5&=2p_2^4-3p_2p_4, \\ p_7&=-13p_2^6+18p_2^3p_4-4p_2p_6. \end{aligned}$$

We conjecture that all odd numbered coefficients can be expressed in terms of the preceding even numbered coefficients.

3. Characterize the normal matrices over an arbitrary field of characteristic $\neq 2$ which are expressable as a polynomial in their conjugate transpose.

4. Characterize the normal matrices over an arbitrary field of characteristic $\neq 2$ which are neither unitarily similar to a diagonal matrix nor have a single elementary divisor.

9. References

[1] Artin, E., Geometric Algebra (Interscience, New York, 1957).
[2] Drazin, M. P., On diagonable and normal matrices, Quart. J. Math. (Oxford) **2**, 189–198 (1951).
[3] Gantmacher, F. R., The Theory of Matrices (Chelsea, New York, 1959).
[4] Hoffman, A. J., and Taussky, O., A characterization of Normal Matrices, J. Res. Nat. Bur. Stand. (U.S.), **52**, No. 1, 17–19 (1954).
[5] Jacobson, N., Lectures in Abstract Algebra, Vol. **II**, (Van Nostrand, Princeton, 1953).
[6] Katz, I. J., and Pearl, M., On *EPr* and Normal *EPr* Matrices, J. Res. Nat. Bur. Stand. (U.S.), **70B** (Math. Phys.), No. 1, 47–77 (1966). RP 2467.
[7] Katz, I. J., and Pearl, M., Solutions of the Matrix Equation $A^*=XA=AX$, J. London Math. Soc. **41**, 443–452 (1966).
[8] Lang, S., Algebra (Addison Wesley, Reading, 1965).
[9] Pearl, M., On normal and *EPr* matrices, Mich. Math. J. **6**, 1–5 (1959).
[10] Pearl, M., On normal *EPr* matrices, Mich. Math. J. **8**, 33–37 (1961).
[11] Perlis, S., Theory of Matrices (Addison Wesley, Reading, 1952).
[12] Schwerdtfeger, H., Introduction to Linear Algebra and the Theory of Matrices (P. Noorhoff, Groningen, 1961).
[13] Toeplitz, O., Das algebraische Analogen zu einen Satz von Fejer, Math. Zeitschrift. **2**, 187–197 (1918).
[14] Williamson, J., Matrices normal with respect to an Hermitian matrix, Amer. J. Math. **60**, 355–373 (1938).
[15] Williamson, J., Normal matrices over an arbitrary field of characteristic zero, Amer. J. Math. **61**, 335–356 (1939).

(Paper 76B3&4–366)