August 1, 1975

To the Graduate Council:

I am submitting herewith a thesis written by Gary L. Wright entitled "Scalar Polynomial Functions on the n × n Matrices Over a Finite Field." I recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Mathematics.

Robert M. McConnel, Major Professor

We have read this thesis
and recommend its acceptance:

D. S. Jordan

Don Hinton

Accepted for the Council:
Graduate Studies and Research

THESIS
75
.W763
Cop.2

SCALAR POLYNOMIAL FUNCTIONS ON THE n × n MATRICES OVER A FINITE FIELD

A Thesis

Presented for the

Master of Science

Degree

The University of Tennessee

Gary L. Wright

August 1975

1265421

ACKNOWLEDGMENT

The author wishes to express sincere gratitude to Dr. Robert M. McConnel for his direction and advice at all stages of research, analysis, and compilation of the material presented in this work.

ABSTRACT

Let $f(x) \in F[x]$ where F is a field. Then $f(x)$ defines via substitution a function from the set of $n \times n$ matrices, $F_{n\times n}$, to itself. Any function from $F_{n\times n}$ to $F_{n\times n}$ which can be represented by a polynomial in $F[x]$ is called a scalar polynomial function. This paper deals with finding necessary and sufficient conditions for a polynomial $f(x) \in F[x]$ to define a permutation of

(i) $D_n(F)$, the diagonalizable matrices in $F_{n\times n}$,

(ii) $R_n(F)$, the root matrices in $F_{n\times n}$, and

(iii) the matric ring $F_{n\times n}$ itself

where in this case $F = GF(q)$, the finite field of order q.

TABLE OF CONTENTS

CHAPTER		PAGE
I.	INTRODUCTION AND ELEMENTARY OBSERVATIONS.	1
II.	SOME PRELIMINARY RESULTS.	3
III.	SCALAR POLYNOMIAL FUNCTIONS ON $F_{n\times n}$	7
IV.	SCALAR POLYNOMIAL FUNCTIONS WHICH PERMUTE THE DIAGONALIZABLE MATRICES	10
V.	SCALAR POLYNOMIAL FUNCTIONS WHICH PERMUTE THE ROOT MATRICES.	15
VI.	SCALAR POLYNOMIAL FUNCTIONS WHICH PERMUTE $F_{n\times n}$.	26
BIBLIOGRAPHY.		32
VITA.		35

CHAPTER I

INTRODUCTION AND ELEMENTARY OBSERVATIONS

Let $F = GF(q)$ denote the finite field of order q so that $q = p^r$ for some prime p and integer $r \geq 1$. It is well known that any function $f: F \to F$ can be represented by a polynomial of degree less than q with coefficients in F. It has also been shown [1] that a ring R with identity (not necessarily commutative) has the property that every function from R to R can be represented by a generalized polynomial, i.e., a finite sum of terms of the type

$$A_0 x^{e_0} A_1 x^{e_1} \cdots A_{k-1} x^{e_{k-1}} A_k \tag{1.1}$$

where $A_i \in R$, $e_i > 0$ and $k \geq 0$ but arbitrary, if and only if R is isomorphic to the ring $F_{n\times n}$ of matrices over F for some n and some finite field F.

If in (1.1) we replace each A_i by a scalar matrix $A_i = a_i I_n$ where $a_i \in F$ and I_n is the $n \times n$ identity matrix, we obtain an ordinary scalar polynomial which determines a function from $F_{n\times n}$ to $F_{n\times n}$. A function $f: F_{n\times n} \to F_{n\times n}$ will be called a scalar polynomial function if and only if there exists a polynomial $f(x) \in F[x]$ which represents f via substitution of x by a matrix $A \in F_{n\times n}$. A polynomial $f(x) \in F[x]$ is called a scalar polynomial. A scalar

polynomial is called a permutation polynomial on a set S if and only if it defines a one-one and onto function on S .

We will direct our attention now to scalar polynomial functions on $F_{n\times n}$. Throughout our discussion, unless otherwise stated, F will denote the finite field GF(q) . Let $f(x) \in F[x]$. If $A = aI_n$ is a scalar matrix, then clearly $f(aI_n) = f(a)I_n$. More generally, if $D = \text{diag}(d_1, \ldots, d_n)$, then $f(D) = \text{diag}(f(d_1), \ldots, f(d_n))$. It is also clear that the image of a symmetric matrix under f is symmetric, and that the image of an upper (lower) triangular matrix is upper (lower) triangular. Now since $P^{-1}f(A)P = f(P^{-1}AP)$ for all $A, P \in F_{n\times n}$, P nonsingular, it follows that if A is diagonalizable, then so is f(A) and if A has all its roots in F , then so does f(A) as A is similar to an upper triangular matrix. Moreover, if B commutes with A it commutes with f(A) . Also note that if A is diagonalizable, then so is $P^{-1}AP$ for any nonsingular $P \in F_{n\times n}$; that is, any similarity transformation maps the set of diagonalizable matrices of $F_{n\times n}$ onto itself. These facts will be used frequently throughout this paper.

CHAPTER II

SOME PRELIMINARY RESULTS

LEMMA 2.1. Let F be any field such that the characteristic of F is not equal to 2, and let m and n be positive integers. If X is an $m \times n$ matrix over F such that $XP = X$ for all $n \times n$ invertible matrices, P, over F, then X is the $m \times n$ zero matrix.

PROOF. If $X \in F_{m\times n}$ satisfies $XP = X$ for all $P \in F_{n\times n}$ such that $|P| \neq 0$, then, in particular, $XP = X$ for $P = 2I_n$. So that $2X = X$ or, equivalently, $2X - X = 0$ which implies $X = 0$. Similarly, it is easily shown that if $X \in F_{n\times m}$ and $PX = X$ for all $P \in F_{n\times n}$ such that $|P| \neq 0$, then X is the $n \times m$ zero matrix.

THEOREM 2.1. Let F be any field and let $f(x) \in F[x]$ be a permutation polynomial on $F_{n\times n}$. Then $f(x)$ is a permutation polynomial on $F_{m\times m}$ for all $m \leq n$. Moreover, if $n \geq 2$ then the coefficient of x in $f(x)$ is nonzero.

PROOF. $f(x)$ is one-one on $F_{m\times m}$ since if $f(A) = f(B)$ for some $A, B \in F_{m\times m}$, $m \leq n$, then $f(\overline{A}) = f(\overline{B})$ for $\overline{A} = \text{diag}(A,0)$, and $\overline{B} = \text{diag}(B,0)$, where 0 is $(n-m) \times (n-m)$. Thus $\overline{A} = \overline{B}$, so $A = B$. If F is a finite field, then $f(x)$ is automatically onto. Otherwise, to see that $f(x)$ maps $F_{m\times m}$ onto $F_{m\times m}$, let $A \in F_{m\times m}$. There is a unique $X \in F_{n\times n}$ such that $f(X) = \text{diag}(A,0)$, where 0

is $(n-m) \times (n-m)$. Let $Q = \mathrm{diag}(I_m, P)$, where P is $(n-m) \times (n-m)$ and $|P| \neq 0$. Then $f(Q^{-1}XQ) = \mathrm{diag}(A, 0)$ which implies $Q^{-1}XQ = X$ or, equivalently, $QX = XQ$. Partition Q in the natural way and partition X in exactly the same way and then we have

$$\begin{bmatrix} I_m & 0 \\ 0 & P \end{bmatrix} \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix} = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix} \begin{bmatrix} I_m & 0 \\ 0 & P \end{bmatrix}$$

or, equivalently,

$$\begin{bmatrix} X_{11} & X_{12} \\ PX_{21} & PX_{22} \end{bmatrix} = \begin{bmatrix} X_{11} & X_{12}P \\ X_{21} & X_{22}P \end{bmatrix} .$$

Therefore we have $X_{12} = X_{12}P$ and $X_{21} = PX_{21}$ for all invertible P in $F_{(n-m)\times(n-m)}$. This implies that every entry in both X_{12} and X_{21} is $0 \in F$. So that $X = \mathrm{diag}(X_{11}, X_{22})$ where $X_{11} \in F_{m\times m}$. Thus $f(X_{11}) = A$ and $f(x)$ is onto. Now if $n \geq 2$ and if $f(x)$ is a permutation polynomial on $F_{n\times n}$, it is a permutation polynomial on $F_{2\times 2}$. Moreover $g(x) = f(x) - f(0)$, $0 \in F$, is a permutation polynomial on $F_{n\times n}$ and on $F_{2\times 2}$. Now if $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, we have $g(A) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $g(B) = \begin{bmatrix} 0 & a_1 \\ 0 & 0 \end{bmatrix}$ where a_1 is the coefficient of x in $f(x)$. Therefore $a_1 \neq 0$.

THEOREM 2.2. Let F be a field, let $n \geq 1$ be an integer and let $f(x) \in F[x]$ be a permutation polynomial on $F_{n\times n}$. Then $f(x)$ has exactly one linear factor (in $F[x]$) and no other factor of degree less than $n + 1$. If $n \geq 2$ the linear factor is of multiplicity 1.

PROOF. Since $f(x)$ is a permutation polynomial on $F = F_{1\times 1}$ the equation $f(x) = 0$ has exactly one root $r \in F$. Suppose that $f(x) = g(x)h(x)$ where $\deg h(x) \geq 1$ and $2 \leq \deg g(x) = m \leq n$. Set $A = rI_m$ and let B be the companion matrix of $g(x)$. Then $f(A) = f(B) = 0$, contradicting the fact that $f(x)$ is one-one on $F_{m\times m}$. Now if $n \geq 2$ and $f(x)$ has $(x-r)^m$ as a factor where $m \geq 2$, then $f(rI_2) = f(B) = 0$ where B is the companion matrix of $(x-r)^2$, another contradiction.

COROLLARY 2.1. Let F be a field. A polynomial $f(x) \in F[x]$ is a permutation polynomial on $F_{n\times n}$ for all n if and only if $f(x) = ax + b$ for some $a, b \in F$, $a \neq 0$.

PROOF. If $f(x) \in F[x]$ has degree $m > 1$, then $f(x)$ is not a permutation polynomial on $F_{m\times m}$ by Theorem 2.2.

Corollary 2.2. If $F = \mathbb{C}$ (complex field) then $f(x)$ is a permutation polynomial on $\mathbb{C}_{n\times n}$ if and only if $f(x)$ is linear.

PROOF. If $f(x)$ is a permutation polynomial on $\mathbb{C}_{n\times n}$, it is a permutation polynomial on $\mathbb{C}$, hence $f(x) = z$ has exactly one solution for each $z \in \mathbb{C}$. This implies $f(x)$ is linear.

COROLLARY 2.3. If $F = R$ (real field) there are no permutation polynomials on $F_{n\times n}$ for $n \geq 2$ except the linear polynomials.

PROOF. A real polynomial of degree greater than one factors into linear and irreducibly quadratic factors over $R[x]$. If $f(x)$ is a permutation polynomial on $R_{n\times n}$ $(n \geq 2)$, then by Theorem 2.2, $f(x)$ has exactly one linear factor and no quadratic factors.

CHAPTER III

SCALAR POLYNOMIAL FUNCTIONS ON $F_{n\times n}$

THEOREM 3.1. Let $F = GF(q)$, let $n > 0$ be an integer, and let

$$L_n(x) = \prod_{k=1}^{n} (x^{q^k} - x) \quad .$$

Then $L_n(A) = 0$ for all $A \in F_{n\times n}$ and $L_n(x)$ is the monic polynomial of least degree which has this property.

PROOF. For $A \in F_{n\times n}$ let $C_A(x) = \det(xI_n - A)$, and define $L(x)$ by

$$L(x) = \underset{A\in F_{n\times n}}{\text{L.C.M.}} \{C_A(x)\} \quad .$$

Then $L(A) = 0$ for all $A \in F_{n\times n}$ since $C_A(A) = 0$. Thus denote by $L_n(x)$ the monic of least degree satisfied by every $A \in F_{n\times n}$ so that $L_n(x) \mid L(x)$. Since deg $C_A(x) = n$ and since every polynomial $Q(x) \in F[x]$ of degree n with leading coefficient $(-1)^n$ is the characteristic polynomial for some $A \in F_{n\times n}$, we have

$$L(x) = \underset{\substack{\deg Q=n \\ Q \text{ monic}}}{\text{L.C.M.}} \{Q(x)\} \quad .$$

But every $Q(x)$ monic of degree n is the minimum polynomial of its companion matrix so that $Q(x) \mid L_n(x)$ for all such $Q(x) \in F[x]$; hence $L(x) \mid L_n(x)$. Therefore $L_n(x) = L(x)$.

If $P(x)$ is a prime factor of $Q(x)$ where $\deg Q(x) = n$, $\deg P(x) = k$, $P(x)$, $Q(x) \in F[x]$, then $P(x)$ is a factor of $Q(x)$ of multiplicity at most $[n/k]$. Moreover, the degree n polynomial $x^{n-k[n/k]}P(x)^{[n/k]}$ where $P(x)$ is an arbitrary irreducible polynomial of degree $k \leq n$ has $P(x)^{[n/k]}$ as a factor; thus

$$L_n(x) = \underset{\substack{\deg Q=n \\ Q \text{ monic}}}{\text{L.C.M}} \{Q(x)\} = \prod_{\deg P=k\leq n} P(x)^{[n/k]}$$

where $P(x)$ is prime. Now let $r \in GF(q^k)$ be a root of $P(x) = 0$ where $P(x)$ is an irreducible of degree $k \leq n$ in $F[x]$. Then r is also a root of $L_n(x)$ exactly $[n/k]$ times. But r is also a root of $\prod_{i=1}^{n} (x^{q^i} - x)$ exactly $[n/k]$ times as r satisfies exactly once each of $x^{q^k} - x$, $x^{q^{2k}} - x$, ..., $x^{q^{[n/k]k}} - x$ and these are the only factors satisfied by r . Hence

$$L_n(x) = \prod_{k=1}^{n} (x^{q^k} - x)$$

as both sides of the equation have exactly the same roots with the same multiplicities and both are monic.

THEOREM 3.2. Let $F = GF(q)$. Each scalar polynomial function from $F_{n\times n}$ to $F_{n\times n}$ is representable by a unique polynomial $f(x) \in F[x]$ of degree less than $\delta = q^n + \ldots + q^2 + q$. The number

of scalar polynomial functions on $F_{n\times n}$ is q^{δ} .

PROOF. Let $g(x) \in F[x]$. Then $g(x) = L_n(x)h(x) + f(x)$ where $\deg f(x) < \deg L_n(x) = \delta$. By Theorem 3.1, $g(A) = f(A)$ for all $A \in F_{n\times n}$ so that the scalar polynomial function defined by $g(x)$ is representable by a polynomial $f(x)$ of degree less than δ . If $f_1(x)$ and $f_2(x)$ are of degree less than δ and represent the same scalar polynomial function, then the polynomial $d(x) = f_1(x) - f_2(x)$ satisfies $d(A) = 0$ for all $A \in F_{n\times n}$ so that $L_n(x) \mid d(x)$ implying $d(x) = 0$ or $f_1(x) = f_2(x)$. The number of polynomials in $F[x]$ of degree less than δ is clearly q^{δ} .

CHAPTER IV

SCALAR POLYNOMIAL FUNCTIONS WHICH PERMUTE THE DIAGONALIZABLE MATRICES

If $f(x) \in F[x]$, $F = GF(q)$, is a permutation polynomial on $F_{n\times n}$ then $f(x)$ necessarily permutes the diagonalizable matrices in $F_{n\times n}$, denoted $D_n(F)$. Thus as a first step in giving necessary and sufficient conditions on $f(x)$ in order that it permute $F_{n\times n}$ we find conditions on $f(x)$ in order that permute $D_n(F)$. Here F is an arbitrary field.

LEMMA 4.1. Let F be any field and let $A = \text{diag}(a_1 I_{k_1}, \ldots, a_t I_{k_t}) \in F_{n\times n}$ with $a_i \neq a_j$ for $i \neq j$. Then if $Q \in F_{n\times n}$ commutes with A, Q has the partitioned form $Q = \text{diag}(Q_1, \ldots, Q_t)$ where Q_i is $k_i \times k_i$.

PROOF. Let $A_{ii} = a_i I_{k_i}$, $i = 1, \ldots, t$, and let A_{ij} denote the $k_i \times k_j$ zero matrix for $i \neq j$. So we have $A = [A_{ij}]$ partitioned in the natural manner. Let $Q = [Q_{ij}]$ be partitioned in exactly the same way. Now $QA = AQ$ implies that $Q_{ij}A_{jj} = A_{ii}Q_{ij}$, $i = 1, \ldots, t$, $j = 1, \ldots, t$. So that for $i \neq j$ we have $Q_{ij}(a_j I_{k_j}) = (a_i I_{k_i})Q_{ij}$ where Q_{ij} is of course $k_i \times k_j$. From which it follows that $a_j(Q_{ij} I_{k_j}) = a_i(I_{k_i} Q_{ij})$ or $a_j Q_{ij} = a_i Q_{ij}$. So that $(a_j - a_i)Q_{ij} = 0$ which implies $Q_{ij} = 0$ as $a_i \neq a_j$ for $i \neq j$.

THEOREM 4.1. Let F be any field and let $f(x) \in F[x]$. Then the following are equivalent:

1. $f(x)$ is a permutation polynomial on $D_n(F)$ for all n;
2. $f(x)$ is a permutation polynomial on $D_n(F)$ for some $n \geq 1$;
3. $f(x)$ is a permutation polynomial on F.

PROOF. Clearly 1 implies 2. To see that 2 implies 3, let $f(x)$ be a permutation polynomial on $D_n(F)$ for some $n \geq 1$ and suppose $f(a) = f(b)$, $a, b \in F$. Set $A = aI_n$ and $B = bI_n$ and note that $A, B \in D_n(F)$. Moreover, we have

$$f(A) = \operatorname{diag}(f(a), \ldots, f(a)) = \operatorname{diag}(f(b), \ldots, f(b)) = f(B)$$

which implies $A = B$ as $f(x)$ is a permutation polynomial on $D_n(F)$. Therefore $a = b$ and $f(x)$ is one-one. To see that $f(x)$ maps F onto F, let $a \in F$ and set $A = aI_n \in D_n(F)$. There exists $B \in D_n(F)$ such that $f(B) = A$. Moreover, there exists a nonsingular matrix $P \in F_{n\times n}$ such that $P^{-1}BP = \operatorname{diag}(b_1, \ldots, b_n)$. Therefore we have

$$\operatorname{diag}(f(b_1), \ldots, f(b_n)) = f(P^{-1}BP) = P^{-1}f(B)P = P^{-1}(aI_n)P = aI_n$$

or $f(b_i) = a$, $i = 1, \ldots, n$. So that $f(x)$ is onto. (Note that $b_i = b_j$ since we have shown that $f(x)$ is one-one.)

Now to see that 3 implies 1, let $f(x) \in F[x]$ be a permutation polynomial on F and let $n \geq 1$ be arbitrary. If $A \in D_n(F)$, there

exists a nonsingular $P \in F_{n\times n}$ such that $P^{-1}AP = D = \text{diag}(d_1, \ldots, d_n)$ and since $f(x)$ is a permutation polynomial on F, there are elements $c_1, \ldots, c_n$ in F such that $f(c_i) = d_i$. Thus let $C = \text{diag}(c_1, \ldots, c_n)$ and it follows that $f(C) = D$; hence $f(PCP^{-1}) = Pf(C)P^{-1} = A$. Thus $f(x)$ maps $D_n(F)$ onto $D_n(F)$. (In case F is finite the proof is complete as onto implies one-one.) It remains to prove $f(x)$ is one-one; suppose for $A, B \in D_n(F)$, $f(A) = f(B)$. There exists a nonsingular matrix $P \in F_{n\times n}$ such that

$$P^{-1}BP = \text{diag}(b_1 I_{k_1}, \ldots, b_t I_{k_t}), \tag{4.1}$$

where $\sum k_i = n$ and $b_i \neq b_j$ for $i \neq j$. Also there exists a nonsingular matrix $Q \in F_{n\times n}$ such that

$$Q^{-1}(P^{-1}AP)Q = \text{diag}(a_1 I_{r_1}, \ldots, a_m I_{r_m}), \tag{4.2}$$

where $\sum r_i = n$ and $a_i \neq a_j$ for $i \neq j$. Now $f(A) = f(B)$ implies $f(Q^{-1}P^{-1}APQ) = Q^{-1}f(P^{-1}BP)Q$ or

$$\text{diag}(f(a_1)I_{r_1}, \ldots, f(a_m)I_{r_m}) = Q^{-1}\,\text{diag}\,(f(b_1)I_{k_1}, \ldots, f(b_t)I_{k_t})Q. \tag{4.3}$$

Now since similar matrices have the same characteristic roots, $m = t$ and there is some ordering of the a_i's such that $a_{s_i} = b_i$ and $r_{s_i} = k_i$, $i = 1, \ldots, t$. (Note we have used the fact that $f(x)$ is one-one on F.) Without loss of generality, we may assume the

matrix Q was selected so that $a_i = b_i$ and $r_i = k_i$, $i = 1, \ldots, t$; therefore (4.2) and (4.3) become, respectively,

$$Q^{-1}P^{-1}APQ = \operatorname{diag}(b_1 I_{k_1}, \ldots, b_t I_{k_t}) = D \tag{4.4}$$

and

$$f(D) = Q^{-1}f(D)Q\,, \tag{4.5}$$

where D is the diagonal matrix defined by (4.4). It follows that Q commutes with $f(D) = \operatorname{diag}(f(b_1)I_{k_1}, \ldots, f(b_t)I_{k_t})$ so that by Lemma 4.1 we have that Q has the partitioned form

$$Q = \operatorname{diag}(Q_1, \ldots, Q_t)$$

where Q_i is $k_i \times k_i$. Hence Q commutes with D. So from (4.4) we have that $P^{-1}AP = QDQ^{-1} = DQQ^{-1} = D$. But $P^{-1}BP = D$, so it follows that $A = B$. Therefore $f(x)$ is one-one on $D_n(F)$.

COROLLARY 4.1. The number of scalar polynomial functions from $D_n(F)$ to $D_n(F)$ where $F = GF(q)$ is q^q and of these $q!$ are permutations of $D_n(F)$.

PROOF. Since $x^q - x$ is the monic of least degree satisfied by every $A \in D_n(F)$, if $g(x) \in F[x]$ and $g(x) = f(x) + (x^q - x)h(x)$ where $\deg f(x) < q$, then $g(x)$ and $f(x)$ represent the same function when restricted to $D_n(F)$. Moreover, $g(x)$ is a permutation

polynomial on F if and only if $f(x)$ is a permutation polynomial on F, and if $f(x)$ and $f_1(x)$ represent different functions on F, they represent different functions on $D_n(F)$.

COROLLARY 4.2. The number of different scalar polynomial functions on $F_{n\times n}$ which permute $D_n(F)$ is $q!q^{\rho}$ where $\rho = q^n + q^{n-1} + \ldots + q^2$.

PROOF. Note that two polynomials $g(x)$ and $h(x)$ may act differently on $F_{n\times n}$ but the same on $D_n(F)$. To obtain the number of scalar polynomial functions on $F_{n\times n}$ which permute the elements of $D_n(F)$, consider

$$f_1(x) + (x^q - x)f_2(x)$$

where $\deg f_2(x) < q^n + q^{n-1} + \ldots + q^2$. For a fixed $f_1(x)$ we see that as $f_2(x)$ varies we obtain all the different functions on $F_{n\times n}$ which behave like $f_1(x)$ on $D_n(F)$.

CHAPTER V

SCALAR POLYNOMIAL FUNCTIONS WHICH PERMUTE THE ROOT MATRICES

Let F be an arbitrary field and let $A \in F_{n\times n}$. The matrix A is called a root matrix if and only if all n of its characteristic roots lie in F. The set of all root matrices is denoted by $R_n(F)$. We will now find conditions on $f(x) \in F[x]$ in order that it permute $R_n(F)$. Notice also that $D_n(F) \subseteq R_n(F)$. After we conclude that if $f(x)$ is a permutation polynomial on $R_n(F)$, then it is a permutation polynomial on F, we have that if $f(x)$ is a permutation polynomial on $R_n(F)$, then it is a permutation polynomial on $D_n(F)$.

First consider the square matrix whose elements are zero except on the principal diagonal, which are all equal, and those on the first superdiagonal, which are all equal to unity. Such a matrix

$$J = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{bmatrix}$$

is called a Jordan block. If $A \in R_n(F)$ then there exists a non-singular matrix $P \in F_{n\times n}$ such that

$$P^{-1}AP = \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & J_k \end{bmatrix} = \bar{A}$$

where each of the characteristic values of A appears in at least one of the Jordan block's, J_i. The same characteristic value may occur in different blocks but the number of distinct blocks corresponding to a given characteristic value is equal to the number of independent characteristic vectors corresponding to that characteristic value. The matrix $\bar{A}$ is called the Jordan normal form of the matrix A. It is sometimes called the Jordan canonical form of the matrix A. The Jordan form is unique up to the order in which the blocks appear down the diagonal. Moreover, if two matrices are in Jordan form and they are similar, then they can differ only in that the order of the blocks is different.

LEMMA 5.1. Let $a_0, a_1, a_2, \ldots$ be elements of F with $a_1 \neq 0$ and for each integer $n \geq 1$, let

$$A_n = a_0 I_n + a_1 N_n + a_2 N_n^2 + \ldots + a_{n-1} N_n^{n-1}, \tag{5.1}$$

where N_n is the $n \times n$ Jordan matrix with 1's on the superdiagonal and 0's elsewhere. Then a $t \times k$ matrix X over F satisfies

$A_t X = XA_k$ if and only if X satisfies $N_t X = XN_k$.

PROOF. Suppose $N_t X = XN_k$. If $X = [x_{ij}]$ we have

$$N_t X = \begin{bmatrix} x_{21} & x_{22} & \cdots \\ x_{31} & x_{32} & \cdots \\ \cdot & \cdot & \cdots \\ x_{t1} & x_{t2} & \cdots \\ 0 & 0 & \cdots \end{bmatrix} = \begin{bmatrix} 0 & x_{11} & x_{12} & \cdots \\ 0 & x_{21} & x_{22} & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ 0 & x_{t1} & x_{t2} & \cdots \end{bmatrix} = XN_k$$

Equating elements standing at the ij^{th} position of these matrices we have

$$x_{i+1,j} = x_{i,j-1} \ , \ 0 < i < t \ , \ 1 < j < k + 1 \ ,$$

and $x_{21} = x_{31} = \cdots = x_{t1} = x_{t2} = \cdots = x_{t,k-1} = 0$. On writing x_k for $x_{1,k+1}$ we conclude that

$$X = (x_0 I_t + x_1 N_t + x_2 N_t^2 + \cdots + x_{t-1} N_t^{t-1}) I_{tk}$$

where by I_{tk} we mean

$$I_{tk} = [0 \ I_t] \text{ if } t < k \ , \ I_{tk} = \begin{bmatrix} I_k \\ 0 \end{bmatrix} \text{ if } t > k \ .$$

The number of arbitrary parameters, x_i , is equal to the smaller of t and k and all others are illusory. Clearly any such matrix X

will also satisfy $A_t X = XA_k$. Similarly, it can be shown that any $t \times k$ matrix X satisfying $A_t X = XA_k$ satisfies $N_t X = XN_k$.

LEMMA 5.2. Let $A = \operatorname{diag}(A_{k_1}, \ldots, A_{k_t})$ and let $B = \operatorname{diag}(B_{k_1}, \ldots, B_{k_t})$ where each of the A_{k_i} have the form (5.1) based on a sequence $a_0, a_1, a_2, \ldots$, with $a_1 \neq 0$ and the B_{k_i} have the same form as (5.1) but based on a possibly different sequence $b_0, b_1, b_2, \ldots$, where $b_1 \neq 0$. Then X commutes with A if and only if X commutes with B .

PROOF. The proof is obvious using partitioned matrices and Lemma 5.1.

Now consider the n-square matrix

$$A(\lambda) = \begin{bmatrix} a_{11}(\lambda) & a_{12}(\lambda) & \cdots & a_{1n}(\lambda) \\ a_{21}(\lambda) & a_{22}(\lambda) & \cdots & a_{2n}(\lambda) \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1}(\lambda) & a_{n2}(\lambda) & \cdots & a_{nn}(\lambda) \end{bmatrix}$$

where λ is a scalar variable and the $a_{ij}(\lambda)$ are polynomials in λ with coefficients in a field F . A matrix of this form will be called a λ-matrix. A λ-matrix $A(\lambda)$ of rank r can be reduced by elementary transformations over $F[\lambda]$ to the Smith normal form

$$N(\lambda) = \begin{bmatrix} e_1(\lambda) & 0 & \cdots & 0 & \cdots & 0 \\ 0 & e_2(\lambda) & \cdots & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & e_r(\lambda) & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{bmatrix}$$

where the leading coefficient of each $e_i(\lambda)$ is unity and $e_i(\lambda)$ is a divisor of $e_{i+1}(\lambda)$, $i = 1, \ldots, r-1$. Let $d_m(\lambda)$ be the greatest common divisor of the m-rowed minor determinants of $A(\lambda)$, written with unity as the coefficient of the highest power of λ, and adopt the convention that $d_0(\lambda) = 1$. Then

$$e_m(\lambda) = \frac{d_m(\lambda)}{d_{m-1}(\lambda)}, \quad m = 1, \ldots, r.$$

These $e_m(\lambda)$ are called the invariant factors. It is well known that two matrices $A, B \in F_{n\times n}$ are similar if and only if $(\lambda I_n - A)$ and $(\lambda I_n - B)$ can be reduced to the same Smith normal form. These facts will be used in the next lemma.

LEMMA 5.3. Let A_n be given by (5.1) (with $a_1 \neq 0$). Then A_n is similar to the Jordan matrix

(5.2) $$J_n(a_0) = a_0 I_n + N_n .$$

PROOF. Clearly both A_n and $J_n(a_0)$ have the same rank and if $n = 1$, A_n is obviously similar to $J_n(a_0)$; indeed, in that case they are equal. Suppose then that $n \geq 2$. It is easily seen that for each integer m such that $1 \leq m < n$ the greatest common divisor of all the m-rowed minor determinants of $(\lambda I_n - J_n(a_0))$ is 1. Moreover, we have $\det(\lambda I_n - J_n(a_0)) = (\lambda - a_0)^n$. So it follows that the Smith normal form for $(\lambda I_n - J_n(a_0))$ is $\operatorname{diag}(1, 1, \ldots, 1, (\lambda - a_0)^n)$. Now let m , $1 \leq m < n$, be arbitrary. Consider the two $m \times m$ submatrices of $(\lambda I_n - A_n)$ given by

$$B = \begin{bmatrix} \lambda - a_0 & -a_1 & \cdot & \cdot & -a_{m-1} \\ 0 & \lambda - a_0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -a_1 \\ 0 & 0 & \cdot & \cdot & \lambda - a_0 \end{bmatrix}$$

and

$$C = \begin{bmatrix} -a_1 & -a_2 & \cdot & \cdot & -a_m \\ \lambda - a_0 & -a_1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -a_1 & -a_2 \\ 0 & 0 & \cdot & \lambda - a_0 & -a_1 \end{bmatrix}$$

Clearly $\det B = (\lambda - a_0)^m$. Expanding down the first column of C ,

we find that $\det C = (-a_1)^m + f(\lambda)$ for some polynomial $f(\lambda)$ such that $f(a_0) = 0$. But as $a_1 \neq 0$, we see that the greatest common divisor of $\det B$ and $\det C$ is unity. Hence the greatest common divisor of all m-rowed minor determinants of $(\lambda I_n - A_n)$ for $1 \leq m < n$ is unity. It follows then that the Smith normal form for $\lambda I_n - A_n$ is also $\operatorname{diag}(1, 1, \ldots, (\lambda - a_0)^n)$. Therefore A_n is similar to $J_n(a_0)$ and the lemma is proved.

THEOREM 5.1. Let $f(x) \in F[x]$, F a field. The following are equivalent:

1. $f(x)$ is a permuation polynomial on $R_n(F)$ for some $n \geq 2$;
2. $f(x)$ is a permutation polynomial on $R_n(F)$ for all $n \geq 1$;
3. (i) $f(x)$ is a permutation polynomial on F, and
   (ii) $f'(x)$ has no roots in F.

PROOF. Clearly if $f(x)$ is a permutation polynomial on $R_n(F)$ for all $n \geq 1$, it is a permutation polynomial on $R_n(F)$ for some $n \geq 2$. Suppose $f(x)$ is a permutation polynomial on $R_n(F)$ for some $n \geq 2$. Then $f(x)$ is a permutation polynomial on F by essentially the same argument used in Theorem 4.1. Hence, we have that (i) is valid. Moreover, since $f(x)$ is a permutation polynomial on $R_n(F)$, $f'(x)$ can have no roots in F; otherwise, if $f'(a) = 0$ for some $a \in F$, then define matrices $A, B \in F_{2\times 2}$ by $A = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$ and $B = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and consider the matrices $C, D \in R_n(F)$ given by $C = \operatorname{diag}(A, 0, \ldots, 0)$ and $D = \operatorname{diag}(B, 0, \ldots, 0)$. Then we have that,

$$f(C) = \begin{bmatrix} f\left(\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}\right) & 0 & . & 0 \\ 0 & f(0) & . & 0 \\ . & . & . & . \\ 0 & 0 & . & f(0) \end{bmatrix} = \begin{bmatrix} f(a) & f'(a) & 0 & . & 0 \\ 0 & f(a) & 0 & . & 0 \\ 0 & 0 & f(0) & . & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & . & f(0) \end{bmatrix} = f(D)$$

which contradicts the fact that $f(x)$ is one-one on $R_n(F)$.

Now assume (i) and (ii) hold and let $n \geq 1$ be arbitrary. To see that $f(x)$ maps $R_n(F)$ onto $R_n(F)$, consider first an arbitrary Jordan matrix $J_m(a)$ of the form (5.2). By (i) there exists $b \in F$ such that $f(b) = a$ and by (ii) $f'(b) \neq 0$ so that

$$f(J_m(b)) = b_0 I_m + b_1 N_m + \ldots + b_{m-1} N_m^{m-1} ,$$

where $J_m(b) = bI_m + N_m$, $b_0 = f(b) = a$ and $b_1 = f'(b) \neq 0$. By Lemma 5.3, there is a nonsingular matrix $P \in F_{m\times m}$ such that

$$P^{-1} f(J_m(b)) P = b_0 I_m + N_m = J_m(a) .$$

Hence, $f(B) = J_m(a)$ where $B = P^{-1} J_m(b) P$. Now let $A \in R_n(F)$ and let $Q \in F_{n\times n}$ be a nonsingular matrix such that

$$Q^{-1} A Q = \overline{A} = \operatorname{diag}(J_{k_1}(a_1), \ldots, J_{k_t}(a_t)) .$$

Let $B_1, \ldots, B_t$ be matrices such that $f(B_i) = J_{k_i}(a_i)$, and set

$$B = Q\,\mathrm{diag}(B_1, \ldots, B_t)Q^{-1} \quad .$$

Then we have $f(B) = Q\,\mathrm{diag}(f(B_1), \ldots, f(B_t))Q^{-1} = Q\bar{A}Q^{-1} = A$, so that $f(x)$ is onto. (Again if F is finite the proof is complete.)

To see that $f(x)$ is one-one let $A, B \in R_n(F)$ be such that $f(A) = f(B)$. There exists nonsingular matrices $P, Q \in F_{n\times n}$ such that

$$P^{-1}BP = \mathrm{diag}(J_{k_1}(b_1) , \ldots, J_{k_r}(b_r)) = \bar{B} \quad ,$$

$$Q^{-1}P^{-1}APQ = \mathrm{diag}(J_{\ell_1}(a_1) , \ldots, J_{\ell_s}(a_s)) = \bar{A} \quad ,$$

where, of course, $\sum_{i=1}^{r} k_i = \sum_{j=1}^{s} \ell_s = n$. Now since $f(A) = f(B)$, we have $f(Q^{-1}P^{-1}APQ) = Q^{-1}f(P^{-1}BP)Q$ or $f(\bar{A}) = Q^{-1}f(\bar{B})Q$. So that $f(\bar{A})$ is similar to $f(\bar{B})$. Now

$$f(\bar{B}) = \mathrm{diag}(f(J_{k_1}(b_1)) , \ldots, f(J_{k_r}(b_r)))$$

where $f(J_{k_i}(b_i)) = f(b_i)I_{k_i} + f'(b_i)N_{k_i} + \ldots$ has the form (5.1) with $f'(b_i) \neq 0$, $i = 1, \ldots, r$. Similarly,

$$f(\bar{A}) = \mathrm{diag}(f(J_{\ell_1}(a_1)) , \ldots , f(J_{\ell_s}(a_s)))$$

where $f(J_{\ell_j}(a_j)) = f(a_j)I_{\ell_j} + f'(a_j)N_{\ell_j} + \ldots$ also has the form (5.1) with $f'(a_j) \neq 0$, $j = 1, \ldots, s$. Now Lemma 5.3 implies that $f(J_{k_i}(b_i))$ is similar to $J_{k_i}(f(b_i))$, $i = 1, \ldots, r$ and $f(J_{\ell_j}(a_j))$

is similar to $J_{\ell_j}(f(a_j))$, $j = 1, \ldots, s$. But $f(\overline{A})$ being similar to $f(\overline{B})$, the fact that $f(x)$ is one-one on F , and the fact that an $n \times n$ matrix is similar to one and only one matrix in Jordan canonical form implies that $r = s$ and that there is a reordering so that $J_{k_i}(b_i) = J_{\ell_i}(a_i)$, $i = 1, \ldots, r$. Assume now that the matrix Q was selected so that $J_{k_i}(b_i) = J_{\ell_i}(a_i)$, $i = 1, \ldots, r$. Then we have that $\overline{B} = \overline{A}$. Now since $f(\overline{A}) = Q^{-1}f(\overline{B})Q = Q^{-1}f(\overline{A})Q$, that is Q commutes with $f(\overline{A})$, it follows from Lemma 5.2 that Q commutes with $\overline{A}$. So that

$$P^{-1}AP = Q\overline{A}Q^{-1} = QQ^{-1}\overline{A} = \overline{A} = \overline{B} = P^{-1}BP$$

or $A = B$ and the proof is complete.

THEOREM 5.2. Let $F = GF(q)$ and let $E = GF(q^m)$ where $m = \text{L.C.M.}\{1, 2, \ldots, n\}$. Let $f(x) \in F[x]$ be such that

(i) $f(x)$ is a permutation polynomial on E , and

(ii) $f'(x)$ has no roots in E .

Then $f(x)$ is a permutation polynomial on $F_{n\times n}$.

PROOF. Note E is the splitting field of $L_n(x) = \prod_{k=1}^{n} (x^{q^k} - x)$. Thus the characteristic polynomial of any matrix $A \in F_{n\times n}$ has all its roots in E ; that is, $F_{n\times n} \subseteq R_n(E)$. Now by the previous theorem we have that $f(x)$ is a permutation polynomial on $R_n(E)$, and since $f(F_{n\times n}) \subseteq F_{n\times n}$, it follows that $f(x)$ is a permutation polynomial on $F_{n\times n}$.

As a result of Theorem 5.2 we may find scalar permutation polynomials on $F_{n\times n}$ other than the linear polynomials. As an example consider $F = GF(2)$ and $n = 2$. Then $L_n(x) = (x^4 - x)(x^2 - x)$ so that all scalar polynomial functions may be assumed to have degree less than 6. Consider the polynomial $f(x) = x^4 + x^2 + x$. It is clearly a permutation polynomial on $F = GF(2)$ and is easily seen to be a permutation polynomial on $GF(2^2)$. Since $f'(x) = 1$, $f(x)$ satisfies the conditions of Theorem 5.2 and hence is a permutation polynomial on $F_{2\times 2}$. Similarly, $f(x) + 1 = x^4 + x^2 + x + 1$ is a permutation polynomial on $F_{2\times 2}$. (Note it is known that of the 16! permutations of $F_{2\times 2}$ only four are representable by polynomials and these are the functions defined by x, $x + 1$, $x^4 + x^2 + x$, $x^4 + x^2 + x + 1$.)

CHAPTER VI

SCALAR POLYNOMIAL FUNCTIONS WHICH PERMUTE $F_{n\times n}$

We now find two necessary and sufficient conditions on $f(x) \in F[x]$ in order that it be a permutation polynomial on $F_{n\times n}$. Here $F = GF(q)$.

LEMMA 6.1. Let $F = GF(q)$, let $f(x) \in F[x]$ be a permutation polynomial on $F_{n\times n}$, and let $K = GF(q^t)$ where $1 \leq t \leq n$ so that $F \subseteq K$. Then $f(x)$ is a permutation polynomial on K.

PROOF. Clearly $f(K) \subseteq K$; hence we need only to show that $f(x)$ is one-one. Since K is a finite extension of F, there exists $\theta \in K$ whose irreducible polynomial $m(x)$ over F has degree t. Moreover, each $\alpha \in K$ is uniquely expressible in the form $\alpha = \sum_{i=0}^{t-1} a_i\theta^i$ where $a_i \in F$. Now since $f(x)$ is a permutation polynomial on $F_{n\times n}$, it is a permutation polynomial on $F_{t\times t}$ as $t \leq n$; in particular, if C is the subalgebra of $F_{t\times t}$ generated by the companion matrix C of $m(x)$, then $f(x)$ is a permutation polynomial on C as $f(C) \subseteq C$. Suppose then that $f(\alpha) = f(\beta)$, $\alpha, \beta \in K$. Since $\alpha = \sum_{i=0}^{t-1} a_i\theta^i$, we may compute modulo $m(\theta)$ to get

$$f(\alpha) = \sum_{i=0}^{t-1} c_i\theta^i$$

for some $c_i \in F$. Likewise, $\beta = \sum_{i=0}^{t-1} b_i\theta^i$ for some $b_i \in F$ and $f(\beta) = \sum_{i=0}^{t-1} c_i\theta^i = f(\alpha)$. Now define matrices $A, B \in C$ by

$A = \sum_{i=0}^{t-1} a_i C^i$ and $B = \sum_{i=0}^{t-1} b_i C^i$. Then $f(A) = f(B) = \sum_{i=0}^{t-1} c_i C^i$, since the computations involved are modulo $m(C)$. Since $f(x)$ is a permutation polynomial on C , we have that $A = B$. But this implies $a_i = b_i$, $i = 0, 1, \ldots, t-1$; hence, $\alpha = \beta$.

LEMMA 6.2. Let A and B be $n \times n$ matrices over a field F and let K be a field containing F . If A and B are similar over K , then they are similar over F .

PROOF. Since the elements of $(xI_n - A)$ and $(xI_n - B)$ lie in $F[x]$, the greatest common divisors of the m-rowed minor determinants of $(xI_n - A)$ and $(xI_n - B)$ do not change when $(xI_n - A)$ and $(xI_n - B)$ are regarded as matrices over $K[x]$. Thus the invariant factors do not change either and since A and B are similar over K if and only if $xI_n - A$ and $xI_n - B$ have the same invariant factors over K which implies, as we have just shown, that $xI - A$ and $xI - B$ have the same invariant factors over F , we may conclude that A and B are similar over F .

LEMMA 6.3. Let $f(x) \in F[x]$ be a permutation polynomial on $F_{n\times n}$ where $F = GF(q)$, and let $K = GF(q^t)$ with $1 \leq t \leq [n/2]$ where $[n/2]$ is the greatest integer in $n/2$. Then $f'(x)$ has no roots in K .

PROOF. Suppose to the contrary that $f'(\lambda) = 0$ for some $\lambda \in K = GF(q^t)$ where $2t \leq n$. Let $m(x)$ be the minimum polynomial of λ over F , let $d = \deg m(x)$, and let C be the companion

matrix of $m(x)$. Then $d|t$ as $F(\lambda) = GF(q^d) \subseteq GF(q^t)$. Set

$$A = \begin{bmatrix} C & 0 \\ 0 & C \end{bmatrix} \quad ; \quad B = \begin{bmatrix} C & N \\ 0 & C \end{bmatrix} \quad ,$$

where $N = (n_{ij})$ is $d \times d$ with $n_{d1} = 1$ and $n_{ij} = 0$ otherwise. Then $A, B \in F_{2d\times 2d}$. Since $2d \leq 2t \leq n$, $f(x)$ is a permutation polynomial on $F_{2d\times 2d}$. Moreover, all the roots of the characteristic equations of both A and B lie in K . Thus, there exist nonsingular matrices $P, Q \in K_{2d\times 2d}$ which bring A and B to their respective Jordan forms; namely,

$$P^{-1}AP = \text{diag}(\lambda_1 I_2 , \lambda_2 I_2 , \ldots, \lambda_d I_2)$$

$$Q^{-1}BQ = \text{diag}(J(\lambda_1) , J(\lambda_2) , \ldots, J(\lambda_d))$$

where $\lambda_1 , \ldots, \lambda_d$ are the roots of $m(x) = 0$ in K and $J(\lambda_i) = \lambda_i I_2 + N_2$. Since $f'(\lambda_i) = 0$, $i = 1, \ldots, d$, it follows that $f(P^{-1}AP) = f(Q^{-1}BQ)$ or $(QP^{-1})f(A)(PQ^{-1}) = f(B)$. Thus, $f(A)$ and $f(B)$ are similar over K . But then $f(A)$ and $f(B)$ must be similar over F , so there exists a nonsingular matrix $R \in F_{2d\times 2d}$ such that $R^{-1}f(A)R = f(B) = f(R^{-1}AR)$. Hence $R^{-1}AR = B$ as $f(x)$ is a permutation polynomial on $F_{2d\times 2d}$. This is a contradiction as A and B are not similar over F . Therefore $f'(x)$ has no roots in K .

THEOREM 6.1. Let $f(x) \in F[x]$, $F = GF(q)$. Then $f(x)$ is a permutation polynomial on $F_{n\times n}$ if and only if

(i) $f(x)$ is a permutation polynomial on $GF(q)$, $GF(q^2)$, ..., $GF(q^n)$, and

(ii) $f'(x)$ does not vanish on $GF(q)$, $GF(q^2)$, ..., $GF(q^{[n/2]})$, where $[n/2]$ is the greatest integer in $n/2$.

PROOF. The necessity is clear from the previous lemmas; thus assume (i) and (ii) hold and suppose $f(A) = f(B)$ for $A, B \in F_{n\times n}$. Let $E = GF(q^m)$ be the splitting field of $L_n(x) = \prod_{k=1}^{n} (x^{q^k} - x)$ so that $m = $ L.C.M. $\{1, 2, \ldots, n\}$ and both A and B have their roots in E . Note that each of the roots of A and B lie in one of $GF(q^i)$, $i = 1, \ldots, n$. Now there exists nonsingular $P, Q \in E_{n\times n}$ such that

$$P^{-1}AP = \operatorname{diag}(A_1, \ldots, A_s) = \overline{A}$$

and

$$Q^{-1}P^{-1}BPQ = \operatorname{diag}(B_1, \ldots, B_r) = \overline{B}$$

where $\overline{A}$ and $\overline{B}$ are the Jordan canonical forms of A and B, respectively. Here each A_i has the form

$$\operatorname{diag}(J_1(\lambda), \ldots, J_{t(i)}(\lambda)) \tag{6.1}$$

where each $J_j(\lambda)$ is of the form

$$J(\lambda) = \lambda I_v + N_v ,$$

N_v being $v \times v$ with 1's on the superdiagonal and zeros elsewhere. Also A_i and A_j correspond to different roots if $i \neq j$. A like statement holds for the B_i's.

Since $f(A) = f(B)$, we have $Q^{-1}f(\overline{A})Q = f(\overline{B})$ or

$$(6.2) \quad Q^{-1} \operatorname{diag}(f(A_1), \ldots, f(A_s))\, Q = \operatorname{diag}(f(B_1), \ldots, f(B_r)) .$$

Now $f(J(\lambda)) = f(\lambda)I_v + f'(\lambda)N_v + c_2N_v^2 + \ldots + c_{v-1}N_v^{v-1}$ for some $c_2, \ldots, c_{v-1} \in E$. Here, if $J(\lambda)$ is not 1×1, then there is an elementary divisor of A over $GF(q)$ of the form $p(x)^k$ where $p(x)$ is the minimum polynomial of λ over $GF(q)$ and $k \geq 2$. This means $\deg p(x) \leq [n/2]$ so that λ is in one of $GF(q)$, ..., $GF(q^{[n/2]})$. Therefore $f'(\lambda) \neq 0$. Therefore, $f(J(\lambda))$ has Jordan form,

$$f(\lambda)I_v + N_v$$

(which is true even if $v = 1$). This means that the Jordan form of either $f(A_i)$ or $f(B_i)$ when A_i or B_i is given by (6.1) is

$$\operatorname{diag}(J_1(f(\lambda)), \ldots, J_{t(i)}(f(\lambda))) \ .$$

Hence from (6.2) and (i) it follows that $s = r$ and that there is a reordering of the B_i's so that $\overline{A} = \overline{B}$ and thus

$$f(\overline{A}) = f(\overline{B}) \quad \text{and} \quad Qf(\overline{A}) = f(\overline{A})Q \ .$$

Now from (6.2) and Lemma 5.2 it follows that $\overline{A}Q = Q\overline{A}$; therefore

$$P^{-1}BP = Q\overline{A}Q^{-1} = \overline{A} = P^{-1}AP$$

implying $A = B$. Since one-one implies onto, the proof is complete.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. J. V. Brawley and L. Carlitz, "A characterization of the n × n matrices over a finite field," Amer. Math. Mo. 80 (1973), 670-672.

2. E. T. Browne, Theory of Determinants and Matrices, Chapel Hill: University of North Carolina Press, 1958.

3. L. Carlitz, "On polynomials in a Galois field," Bull. Amer. Math. Soc. 38 (1932), 736-744.

4. A. R. Collar, W. J. Duncan, and R. A. Frazer, Elementary Matrices, Cambridge: Cambridge Press, 1960.

5. L. E. Dickson, Linear Groups with an Exposition of Galois Field Theory, New York: Dover Publications, Inc., 1958.

6. K. Hoffman and R. Kunze, Linear Algebra, Englewood Cliffs, N. J.: Prentice Hall, Inc., 1971.

7. S. Lange, Algebra, Reading: Addison-Wesley, 1971.

8. C. C. MacDuffee, Theory of Matrices, New York: Chelsea Publishing Co., 1946.

9. B. Noble, Applied Linear Algebra, Englewood Cliffs, N. J.: Prentice Hall, Inc., 1969.

10. O. Ore, "On a special class of polynomials," Amer. Math. Soc. Trans. 35 (1933), 559-584.

11. O. Ore, "Contributions to the theory of finite fields," Amer. Math. Soc. Trans. 36 (1934), 243-274.

12. L. J. Paige and J. D. Swift, Elements of Linear Algebra, Waltham, Mass.: Blaisdell Publishing Co., 1961.

13. H. Paley and P. M. Weichel, A First Course in Abstract Algebra, New York: Holt, Rinehart and Winston, Inc., 1966.

14. S. Perlis, Theory of Matrices, Reading: Addison-Wesley, 1952.

15. L. Redei, Algebra, Vol. 1, Oxford: Pergamon Press, 1967.

16. M. F. Smiley, Algebra of Matrices, Boston: Allyn and Bacon, Inc., 1965.

17. H. W. Turnbull and A. C. Aitken, An Introduction to the Theory of Canonical Matrices, New York: Dover Publications, Inc., 1961.

VITA

Gary L. Wright was born in Copperhill, Tennessee on December 1, 1950. He was graduated from Copper Basin High School in 1968. In August, 1973, he received a Bachelor of Science degree in Mathematics from the University of Tennessee at Knoxville.

In September, 1973, he accepted a teaching assistantship at the University of Tennessee and began study toward a Master of Science degree. He received this degree with a major in Mathematics in August, 1975.