LINEAR TRANSFORMATIONS ON ALGEBRAS OF MATRICES OVER THE CLASS OF INFINITE FIELDS

by

TONY TSUTOMU OISHI

B.A.Sc., University of British Columbia, 1959

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in the Department

of

Mathematics

We accept this thesis as conforming to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

June, 1967

In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the Head of my Department or by his representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of MATHEMATICS

The University of British Columbia
Vancouver 8, Canada

Date June 1967.

ABSTRACT

The problem of determining the structure of linear transformations on the algebra of n-square matrices over the complex field is discussed by M. Marcus and B. N. Moyls in the paper "Linear Transformations on Algebras of Matrices". The authors were able to characterize linear transformations which preserve one or more of the following properties of n-square matrices; rank, determinant and eigenvalues.

The problem of obtaining a similar characterization of transformations as given by M. Marcus and B. N. Moyls but for a wider class of fields is considered in this thesis. In particular, their characterization of rank preserving transformations holds for an arbitrary field. One of the results on determinant preserving transformations obtained by M. Marcus and B. N. Moyls states that if a linear transformation T maps unimodular matrices into unimodular matrices, then T preserves determinants. Since this result does not necessarily hold for algebras of matrices over finite fields, the discussion on the characterization of determinant preserving transformations is limited to algebras of matrices over infinite fields.

TABLE OF CONTENTS

		Page
CHAPTER ONE		
1.1	Introduction	1
1.2	Notation	1
1.3	Rank Preservers	2
CHAPTER TWO		
2.1	Introduction	3
2.2	A Counter-example for Finite Fields	4
2.3	Determinant Preservers	5
2.4	Comments and Further Problems for Investigation	13
BIBLIOGRAPHY		15

ACKNOWLEDGMENT

I take this opportunity to express my appreciation to Dr. Roy Westwick for the encouragement and the many hours of valuable assistance he gave to me during the research and writing of this thesis. Also I would like to thank Dr. B. N. Moyls for reading the thesis and offering helpful suggestions.

The financial support of the University of British Columbia and the National Research Council is much appreciated.

CHAPTER ONE

RANK PRESERVERS

1.1 INTRODUCTION

The purpose of this chapter is to establish some notation to be used in this paper and to present a characterization of linear transformations which preserve the rank of n-square matrices. Although the paper [1]* of M. Marcus and B. N. Moyls is concerned with the algebra of matrices over the complex field, their proofs of the lemmas and the theorem on rank preservers are not dependent on the characteristic nor the algebraic closure of the field. In fact, the proofs hold word for word for the algebra of matrices over an arbitrary field. No proofs are given in this chapter but the main result obtained in [1] is stated below in Theorem 1.3.2.

1.2 NOTATION

The notation used in [1] will be adopted. Let F denote a field. Let the following symbols denote the respective sets:

---

*Numbers in square brackets refer to the bibliography

M_n - the algebra of n-square matrices over F

U_n - the unimodular group of matrices in M_n (i.e., matrices in M_n with determinant 1)

Finally, A^t denotes the transpose of A .

1.3 RANK PRESERVERS

1.3.1 Definition Let $\sigma(A)$ denote the rank of the matrix A . A linear transformation T on M_n is said to be a rank preserver if $\sigma(T(A)) = \sigma(A)$ for all $A \in M_n$.

1.3.2 Theorem Let T be a linear transformation of M_n into M_n . T is a rank preserver if and only if there exist non-singular matrices U and V such that either:

$$T(A) = UAV \quad \text{for all } A,$$

$$\text{or} \quad T(A) = UA^tV \quad \text{for all } A.$$

CHAPTER TWO

DETERMINANT PRESERVERS

2.1 INTRODUCTION

The main result of this chapter is given in Theorem 2.3.8 which states that the following conditions are equivalent:

(1) T maps U_n into U_n.

(2) T preserves determinant; i.e., $\det T(A) = \det A$ for all $A \in M_n$.

(3) There exist non-singular matrices U and V with $\det UV = 1$ such that either:

$$T(A) = UAV \qquad \text{for all } A$$

$$\text{or} \qquad T(A) = UA^tV \qquad \text{for all } A .$$

When the base field F is an arbitrary infinite field, the major difficulty encountered in obtaining the above results lies in showing that condition (1) implies condition (2). The solution of this problem is to a large extent the point of this thesis. When F is a finite field, condition (1) does not necessarily imply condition (2). A counterexample will be given to show this.

2.2 A COUNTEREXAMPLE FOR FINITE FIELDS

The following example is a linear transformation which maps unimodular matrices into unimodular matrices but does not preserve determinant.

Consider the algebra M_2 of 2×2 matrices over the finite field of characteristic two with elements $\{0,1\}$. Let G_1 and G_2 be the following subspaces of M_2:

$$G_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \quad \text{and}$$

$$G_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}.$$

Let T be a linear transformation on M_2 such that $T(G_1) = G_1$ and kernel $T = G_2$. Such a transformation is possible since M_2 is the direct sum of G_1 and G_2 (that is, $G_1 \cap G_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ and dimension M_2 = dimension G_1 + dimension G_2).

The transformation T maps U_n into itself; that is, $T(U_n) \subset U_n$. For each unimodular matrix A there exists a matrix $B \in G_2$ and a matrix $C \in \left[G_1 - \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \right]$.

such that $A = B + C$ (+ denotes the usual matrix addition). Since T is linear and $B \in G_2$, then $T(A) = T(B+C) = T(B) + T(C) = T(C)$. But by the hypothesis $T(C) \in \left[G_1 - \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}\right]$ all of whose members are unimodular. Thus $T(A)$ is unimodular, and $T(U_n) \subset U_n$.

On the other hand, T does not preserve zero determinant. Consider $E = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Since $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $T\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = T\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. And since T preserves unimodular matrices, $\det T\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \det T\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$. But $\det E = 0$, therefore T does not preserve zero determinant. Thus the transformation T maps unimodular matrices into unimodular matrices but does not preserve determinant.

2.3 DETERMINANT PRESERVERS

<u>2.3.1 Definition</u> A linear transformation T on M_n is said to be a determinant preserver if $\det T(A) = \det A$ for all $A \in M_n$.

<u>2.3.2 Lemma</u> If F is an infinite field, then the n-th root of an element of F exists in F for an infinite number of elements of F.

<u>Proof</u>: Let a_1 be a non-zero element of F and $b_1 = a_1^n$. Consider the equation $x^n = b_1$. Now a_1 is one solution and there are at most n solutions of the equation in F. But since there are an infinite number of elements in F, there exists a non-zero element $a_2 \in F$ such that $a_2^n = b_2$ and $b_2 \neq b_1$. Suppose N distinct elements $b_1, b_2, \ldots, b_N$ have been found, each of which has an n-th root. Then there are at most nN solutions of the equations $x^n = b_i$, $i = 1, 2, \ldots, N$. Since F is an infinite field, there exist non-zero elements a_{N+1} and b_{N+1} belonging to F such such that $a_{N+1}^n = b_{N+1}$ and $b_{N+1} \neq b_i$, $i = 1, 2, \ldots, N$. Therefore there are an infinite number of elements in F with an n-th root in F.

<u>2.3.3 Notation</u> Let $A = (a_{ij}) \in M_n$.

(1) A_{ij} denotes the cofactor of a_{ij} in A.

(2) $A(s,t)(x) = (\alpha_{ij})$ where $\alpha_{ij} = a_{ij}$ when $(i,j) \neq (s,t)$ and $\alpha_{st} = x$. (That is, $A(s,t)(x)$ is the $n \times n$ matrix obtained from A by replacing the entry a_{st} by the indeterminate x.)

<u>2.3.4 Lemma</u> If $A = (a_{ij}) \in M_n$ and $\det A \neq 0$, then for some j, $a_{1j}A_{1j} \neq 0$. Consequently, $a_{1j} \neq 0$ and $A_{1j} \neq 0$ for this j.

<u>Proof</u>: Suppose $a_{1j}A_{1j} = 0$ for all j, $1 \leq j \leq n$. Then $\det A = \sum_{j=1}^{n} (-1)^{1+j} a_{1j}A_{1j} = 0$ which contradicts the hypothesis that $\det A \neq 0$. Therefore $a_{1j}A_{1j} \neq 0$ for some j. And since a_{1j} and A_{1j} are elements of F, then $a_{1j}A_{1j} \neq 0$ implies that $a_{1j} \neq 0$ and $A_{1j} \neq 0$.

<u>2.3.5 Lemma</u> If $\det A \neq 0$, then for some fixed j and for each $b \in F$ there exists an element $a \in F$ such that $\det A(1,j)(a) = b$.

<u>Proof</u>: By Lemma 2.3.4 there exists a j, $1 \leq j \leq n$, such that $A_{1j} \neq 0$. Let this value of j be k. If

$$\sum_{j=1,\, j\neq k}^{n} (-1)^{1+j} a_{1j}A_{1j} = c \,, \quad \text{then} \quad \det A(1,k)(x) = xA_{1k} + c \,.$$

For any $b \in F$, the polynomial $xA_{1k} + c - b$ in the indeterminate x has a root, namely $x = (b-c)A_{1k}^{-1}$. Denote this root by a. Thus, for any $b \in F$ there exists an $a \in F$ such that $\det A(1,k)(a) = b$.

<u>2.3.6 Lemma</u> Let F be an infinite field. If $T(U_n) \subset U_n$, then for any $A \in M_n$ such that $\det A \neq 0$, $\det T(A) = \det A$.

<u>Proof</u>: Let $A \in M_n$ and $\det A \neq 0$. Let B be an infinite subset of F such that if $b \in B$, then $b \neq 0$ and b has an n-th root in F. By Lemma 2.3.2 such a set exists. Since $\det A \neq 0$, by Lemma 2.3.5 there exists a k such that for each $b \in B$ there is an $a \in F$ for which $\det A(1,k)(a) = b$. Let S be the subset of F such that for each $a \in S$ there corresponds a $b \in B$ for which $b = \det A(1,k)(a)$. In other words, for each $a \in S$ $\det A(1,k)(a) \neq 0$ and $[\det A(1,k)(a)]^{1/n} \in F$. Since B contains an infinite number of distinct elements then so does S. For each $a \in S$, $\det[A(1,k)(a)/(\det A(1,k)(a))^{1/n}] = 1$. And since $T(U_n) \subset U_n$, for each $a \in S$, $\det T(A(1,k)(a)) = \det A(1,k)(a)$.

Denote by E_{ij} the $n \times n$ matrix whose (i,j)-th position contains the element 1 and is zero elsewhere. Then $\det T(A(1,k)(x)) = \det T(xE_{1k} + \sum_{(i,j)\neq(1,k)} a_{ij}E_{ij}) = \det (xT(E_{1k}) + \sum_{(i,j)\neq(1,k)} a_{ij}T(E_{ij})) = p(x)$, where $p(x)$ is a polynomial in x of degree $\leq n$. In the proof of Lemma 2.3.5 it was shown that $\det A(1,k)(x) = xA_{1k} + C$ for some $c \in F$. Since for each $x \in S$ $\det A(1,k)(x) = \det T(A(1,k)(x))$, then $xA_{1k} + c = p(x)$ for each $x \in S$.

But S contains an infinite number of distinct elements, therefore $xA_{1k} + c = p(x)$ identically in x. Thus for any $x \in F$, $\det T(A(1,k)(x)) = \det A\,(1,k)(x)$. In particular, the equality holds for $x = a_{1k}$; and since $A(1,k)(a_{1k}) = A$, then $\det T(A) = \det A$.

2.3.7 Corollary. Let F be an infinite field. If $T(U_n) \subset U_n$, then for any $A \in M_n$, $\det T(A) = \det A$.

Proof: Let A be any matrix belonging to M_n, and let $A(u)$ be the matrix obtained by replacing a_{ii} in A by $a_{ii} + u$, for $i = 1, 2, 3, \ldots, n$, where u is an indeterminate.

Det $A(u) = u^n + p_1(u) = p(u)$, where $p_1(u)$ is a polynomial in u of degree $\leq n-1$. But $\det T(A(u)) = \det\left(\sum_{i=1}^{n}(u+a_{ii})\,T(E_{ii}) + \sum_{i\neq j} a_{ij}\,T(E_{ij})\right)$, thus $\det T(A(u)) = q(u)$ where $q(u)$ is a polynomial in u of degree $\leq n$. Since $p(u) = 0$ has at most n solutions, then $\det A(u) = p(u) \neq 0$ for infinitely many values of u in F. But if $\det A(u) \neq 0$, then by Lemma 2.3.6 $\det A(u) = \det T(A(u))$ and consequently $p(u) = q(u)$ for infinitely many values of u in F. Thus $p(u) = q(u)$ identically in u and $\det A(u) = \det T(A(u))$ for all values of u in F. In particular, the equality holds for $u = 0$. But since $A(0) = A$, then $\det A = \det T(A)$. A was an arbitrary element in M_n and therefore $\det A = \det T(A)$ for all $A \in M_n$.

The proofs of Lemma 2.3.8 and Lemma 2.3.9 are those given by M. Marcus and B. N. Moyls in the paper [1] . The proofs are included in this paper for the sake of completeness.

<u>2.3.8 Lemma</u> If T preserves determinant, then T is non-singular and hence onto.

<u>Proof</u>: Suppose $T(A) = 0$. Since $\det A = \det T(A) = 0$, then the rank of A , denoted by $\sigma(A)$, is less than n . There exist non-singular matrices M and N such that $MAN = I_r \dot{+} 0_{n-r}$ where $r = \sigma(A)$, I_r the $r \times r$ unit matrix and 0_{n-r} the $(n-r)\times(n-r)$ zero matrix and $\dot{+}$ denotes the direct sum. For any $X \in M_n$, $[\det(MAN+X)][\det M^{-1}N^{-1}] =$ $\det M^{-1}(MAN+X)N^{-1} = \det(A+M^{-1}XN^{-1}) = \det T(M^{-1}XN^{-1}) =$ $\det M^{-1}XN^{-1} = \det X \det M^{-1}N^{-1}$. Therefore $\det(MAN+X) = \det X$. Set $X = 0_r \dot{+} I_{n-r}$. Then $\det(MAN+X) = \det I = 1$. But $\det X = 0$ unless $r = 0$. But $r = 0$ implies $A = 0$. Thus T is non-singular.

<u>2.3.9 Lemma</u> Let F be an infinite field. If T preserves determinant, then T preserves rank.

<u>Proof</u>: Let $A \in M_n$ be an arbitrary matrix. There exist non-singular matrices M_1, N_1, M_2 and N_2 such that $M_1AN_1 = Y_1 = I_r \dot{+} O_{n-r}$ and $M_2T(A)N_2 = Y_2 = I_s \dot{+} O_{n-s}$ where $r = \sigma(A)$ and $s = \sigma(T(A))$.

$$\text{Define } \emptyset : M_n \longrightarrow M_n \text{ by } \emptyset(X) = M_2T(M_1^{-1}XN_1^{-1})N_2 .$$

The mapping $\emptyset$ has the following properties:

(1) $\emptyset$ is linear since T is linear.

(2) $\det \emptyset(X) = k \det X$, where $k = \det(M_2M_1^{-1}N_1^{-1}N_2)$.

This results from $\det \emptyset(X) =$

$\det M_2 \cdot \det T(M_1^{-1}XN_1^{-1}) \cdot \det N_2 =$

$\det M_2 \cdot \det M_1^{-1}XN_1^{-1} \cdot \det N_2 =$

$\det(M_2M_1^{-1}N_1^{-1}N_2) \cdot \det X$

(3) $\emptyset(Y_1) = Y_2$ since $\emptyset(Y_1) = M_2T(M_1^{-1}(M_1AN_1)N_1^{-1})N_2$ $= M_2T(A)N_2 = Y_2$.

Set $Y_3 = O_r \dot{+} I_{n-r}$. For each scalar λ, $\det(\lambda Y_1 + Y_3) = \lambda^r$ and $\det \emptyset(\lambda Y_1 + Y_3) = \det(\lambda\emptyset(Y_1) + \emptyset(Y_3)) = \det(\lambda Y_2 + \emptyset(Y_3)) = p(\lambda)$, where $p(\lambda)$ is a polynomial in λ of degree $\leq s$. But $\det \emptyset(\lambda Y_1 + Y_3) = k \det(\lambda Y_1 + Y_3) = k\lambda^r$, therefore $p(\lambda) = k\lambda^r$ for any $\lambda \in F$. Since

$k \neq 0$, $p(\lambda) = k\lambda^r$ identically in λ . Therefore $r \leq s$ and $\sigma(A) \leq \sigma(T(A))$.

By Lemma 2.3.8, T^{-1} exists; and since T preserves determinant, $\det B = \det(TT^{-1}(B)) = \det T^{-1}(B)$ for all $B \in M_n$. Therefore T^{-1} preserves determinant. Thus $\sigma(T(A)) \leq \sigma(T^{-1}T(A)) = \sigma(A)$ and since it has previously been shown that $\sigma(A) \leq \sigma(T(A))$, then $\sigma(A) = \sigma(T(A))$. That is, T preserves rank.

The statement of the following theorem differs from that given by M. Marcus and B. N. Moyls only in part (3). In particular, when F is the field of complex numbers, they were able to find unimodular matrices U and V which satisfy conditions in part (3) of Theorem 2.3.10.

<u>2.3.10 Theorem</u> Let F be an infinite field and T a linear transformation on M_n . The following conditions are equivalent:

(1) T maps U_n into U_n .

(2) T preserves determinant.

(3) There exist non-singular matrices U and V with $\det UV = 1$ such that either

$$T(A) = UAV \qquad \text{for all } A$$

or $$T(A) = UA^tV \qquad \text{for all } A .$$

Proof: (1) holds if and only if (2) holds by Corollary 2.3.7. (3) implies (2) since det $T(A)$ = det UAV = det $A \cdot$ det UV = det A .

(2) implies (3) . If T preserves determinant, then by Lemma 2.3.9 and Theorem 1.3.2, there exist non-singular matrices U and V such that either $T(A) = UAV$ or $T(A) = UA^tV$ for all $A \in M_n$. Det $T(I)$ = det $I = 1$, therefore 1 = det $T(I)$ = det UIV = det UV . That is, det $UV = 1$.

2.4 COMMENTS AND FURTHER PROBLEMS FOR INVESTIGATION

The hypothesis of Theorem 2.3.10 requires the field F to contain an infinite number of elements, but the infinite field is not a necessary condition. In order to show that two polynomials of degree $\leq n$ are identically equal, it is sufficient that the equality holds for $n + 1$ distinct elements of the field. The proof of Lemma 2.3.6 requires these $n + 1$ elements to be non-zero and to possess an n-th root. If the field contains $n(n+1)$ non-zero elements, then there exist at least $n + 1$ distinct non-zero elements each possessing an n-th root (see the proof of Lemma 2.3.2). Therefore, for a given n , it is sufficient that the field F of Theorem 2.3.10 contains at least $n(n+1)$ non-zero elements. Again this is not a necessary condition on the field F since for some given n there exist fields such that each element of the field has a n-th root; for example, for $n = 3$ take $F = Z_5 = Z/5Z$.

The paper [1] gives a characterization of linear transformations which preserve eigenvalues for all matrices in the algebra of $n \times n$ matrices over the complex numbers. A further problem would be to see if the same characterization holds for the algebra of matrices over a larger class of fields.

Another problem which may be considered is the following. In order to obtain the characterization of rank preservers given in [1] it is sufficient that the linear transformations preserve ranks 1, 2 and n . It may be possible to find other sufficient conditions on a linear transformation T such that T is a rank preserver. For example, if $\sigma(T(A)) = \sigma(A)$ for all symmetric matrices, A , in the algebra of matrices over a field F , then is T a rank preserver?

BIBLIOGRAPHY

[1] Marvin Marcus and B. N. Moyls, Linear Transformations on Algebras of Matrices, Canadian Journal of Mathematics, Volume 11 (1959).