COMMUNICATIONS

DE LA FACULTÉ DES SCIENCES
DE L'UNİVERSİTÉ D'ANKARA

Série A: Mathématique, Physique et Astronomie

TOME 23 A ANNÉE 1974

On the Space of Matrices f_i (A)

by

E. KAYA

7

Faculté des Sciences de l'Université d'Ankara
Ankara, Turquie

Communications de la Faculté des Sciences de l'Université d'Ankara

---

La Revue "Communications de la Faculté des Sciences de l'Univereité d'Ankara" est un organe de publication englobant toutes les disciplines scientifiques représentées à la Faculté: Mathématiques pures et appliquées, Astronomie, Physique et Chimie théorique, expérimentale et techinique, Géologie, Botanique et Zoologie.

La Revue, á l'exception des tomes I, II, III, comprend de trois séries

Série A: Mathématiques, Physique et Astronomie.

Série B: Chimie.

Série C: Sciences naturelles.

En principe. la Revue est réservée aux mémoires originaux des membres de la Faculté. Elle accepte cependant, dans la mesure de la place disponible, les communications des auteurs étrangers. Les langues allemande, anglaise et française sont admises indifféremment. Les articles devront être accompagnés d'un bref sommaire en langue turque.

Adres: Fen Fakültesi Tebliğler Dergisi Fen Fakültesi, Ankara, Turquie

On the Space of Matrices f_i (A)

E. KAYA*

Department of Mathematics, University of Ankara

(Received oct. 10, 1974)

SUMMARY

In this article A will be a fixed nxn matrix and $\Psi(x)$ its minimal polynomial of degree m. The set of matrices f_i (A), where f_i (A) is a polynomial, is an m-dimensional subspace of the n^2 –dimensional space of all nxn matrices [1]. The set of matrices $r_i(A)$, where

$$(f_i(x), \Psi(x)) = 1 \text{ and } f_i(x) \equiv r_i(x) \pmod{\Psi(x)}$$

is a commutative group under matrix multiplication which is isomorphic to the group of polynomials r_i (x) under multiplication modΨ (x). We also characterize properties of the matrices f_i (A) in terms of properties of the polynomials f_i (x).

I. INTRODUCTION

I.1. Let F be a field. By the ring of polynomials in the indeterminate, x, written as F[x], we mean the set of all symbols

$$a_0 + a_1 x + \ldots\ldots + a_n x^n$$

where n can be any nonnegative integer and where the coefficient $a_0, a_1, \ldots\ldots, a_n$ are all in F.

Definition I.1. If the greatest common divisor of f(x), g(x) εF[x] is 1, they are then said to be relatively prime and any polynomial p(x) ε F[x] of positive degree is called prime (or irreducible) over F if it cannot be expressed as a product of two polynomials of positive degree over F.

Definition I.2. If g(x) and h(x) are polynomials whose difference is divisible by a third polynomial f(x), we say that g(x) and h(x) are congruent modulo f(x) and write

$$g(x) \equiv h(x) \pmod{f(x)} .$$

* Department of Mathematics, Ankara University, Ankara-Turkey.

In terms of these definitions we may obtain:

Lemma I.1. If $g_1(x) \equiv h_1(x) \pmod{f(x)}$ and

$$g_2(x) \equiv h_2(x) \pmod{f(x)} \text{ then}$$

$$\text{(i)} \quad g_1(x) + g_2(x) \equiv h_1(x) + h_2(x) \pmod{f(x)}$$

$$\text{(ii)} \quad g_1(x)\, g_2(x) \equiv h_1(x)\, h_2(x) \pmod{f(x)} .$$

We designate by $[g(x)]$ the equivalence class consisting of all polynomials congruent to $g(x)$ modulo $f(x)$. We call $[g(x)]$ a congruence class modulo $f(x)$ and denote by $F[x]/f(x)$ the set of all congruence classes $[g(x)]$.

The binary operations for $F[x]/f(x)$ are defined as follows [2].

Definition I.3.

$$\text{(i)} \quad [g_1(x)] + [g_2(x)] = [g_1(x) + g_2(x)]$$

$$\text{(ii)} \quad [g_1(x)]\, [g_2(x)] = [g_1(x)\, g_2(x)]$$

Lemma I.2. If $f(x), g(x) \varepsilon F[x]$ and $(f(x), g(x))=1$ then there exists $p(x) \varepsilon F[x]$ such that

$$p(x)\, g(x) \equiv 1 \pmod{f(x)}$$

i.e. $[p(x)]\, [g(x)] = [1]$

Proof. If $(f(x), g(x)) = 1$, then there exists

$p(x), q(x) \varepsilon F[x]$ such that

$$p(x\; g(x) + q(x)\, f(x) = 1$$

By Definition 1.2 and 1.3 this implies $p(x)\, g(x) \equiv 1 \pmod{f(x)}$ i. e. $[p(x)]\, [g(x)] = [1]$ which in turn implies the existence of a multiplicative inverse of $[g(x)]$.

In this way the elements $[g_i(x)]$ $(i = 1,2\ldots)$

$(g_i(x), f(x)) = 1$ form a commutative group under the definition of multiplication given in Definition 1.3.

2.1. If A is an nxn matrix over a field F we may take the n^2 elements a_{ik} $(i, k = 1,2\ldots,n)$ in some fixed order so obtaining a row or column vector. In this way we see that the vector space of all nxn matrices over F has dimension n^2.

Lemme 2.1. If E is the nxn unit matrix, the matrices

$$E, A, A^2, \dots, A^{n^2}$$

are linearly dependent.

Proof. Suppose $c_0E + c_1A + \dots + c_{n^2} A^{n^2} = O$ then we obtain n^2 homogeneous equations $n^2 + 1$ unknowns. Such a system always has a non trivial solution which completes the proof. Thus given any nxn matrix A there is always a non-zero polynomial

$$f(x) = c_0 + c_1 x + \dots + c_{n^2} x^{n^2}$$

with $f(A) = O$.

Definition 2.1. A polynomial f(x) is called an annihilating polynomial of the matrix if

$$f(A) = O$$

By Lemma 2.1. we see that a non-zero annihilating polynomial always exists.

Definition 2.2. For i, k = 1,2....,n, we denote by E_{ik} the matrix whose (i,k) the element is equal to 1 and all of whose remaining elements are equal to O.

We now give various results concerning the matrices E_{ik} (i, k = 1,2,..n).

Lemma 2.2. The matrices E_{ik} (i, k = 1, 2,...., n) are linearly independent.

Proof. Suppose $\sum_{k=1}^{n} \sum_{i=1}^{n} c_{ik}E_{ik} = O$. It follows at once from the definition of the matrices E_{ik} that $c_{ik} = O$ (i, k = i, 2,...,n) and the result follows.

Lemma 2.3. (i) $E^2_{ii} = E_{ii}$ (idempotent)

$$\text{(ii) } E_{ij} E_{rk} = \begin{cases} E_{ik}, \text{ if } j = r \\ O, \text{ if } j \neq r \end{cases}$$

Proof. This follows at once from the definition of the matrices E_{ik}.

3.1. A given matrix A has several annihilating polynomials. For example it follows from the Cayley-Hamilton theorem that every matrix satisfies its own characteristic equation. Among all the annihilating polynomials is a monic one with least degree called the minimal polynomial. Every annihilating is divisivble by the minimal polynomial.

So further our study of matrices f(A) we need the following lemma in polynomials.

Lemma 3.1. The greatest common divisor of f(x) and g(x) is $d(x) \neq 1$ if and only if there exist non-zero polynomials p(x) and q(x) such that

$$p(x)\, f(x) = q(x)\, g(x)$$

$$\deg p(x) < \deg g(x),\ \deg q(x) < \deg f(x)$$

Proof. Let the g. c. d. of f(x) and g(x) be $d(x) \neq 1$, then

$$f(x) = d(x)\, f_1(x) \text{ and } g(x) = d(x)\, g_1(x)$$

where $\deg f_1(x) < \deg f(x)$ and $\deg g_1(x) < \deg g(x)$.

from this, we have

$$g_1(x)\, f(x) = f_1(x)\, g(x)$$

Thus, taking $g_1(x) = p(x)$ and $f_1(x) = q(x)$ we have

$$p(x)\, f(x) = q(x)\, g(x)$$

Conversly suppose f(x) and g(x) relatively prime and $p(x) f(x) = q(x)\, g(x)$ holds. Then there exist polynomials h(x) and k(x) such that

$$h(x)\, f(x) + k(x)\, g(x) = 1$$

Then using $p(x)\, f(x) = q(x)\, g(x)$ we have

$$p(x) = p(x)\, h(x)\, f(x) + p(x)\, k(x)\, g(x)$$

$$p(x) = (h(x)\, q(x) + p(x)\, k(x)\,)\, g(x)$$

and g(x) divides p(x). But this impossible. Hence f(x) and g (x) cannot be relatively prime, i.e., $d(x) \neq 1$.

Theorem 3.1. Let ψ (x) be the minimal polynomial of a matrix A over F, and let g(x) be a polynomial over F. Then g(A) is non singular if and only if g(x) is relatively prime to ψ (x).

Proof. Let g(x) and ψ (x) be relatively prime. Then there exist polynomials p(x) and q(x) over F such that

$$p(x)\ g(x) + q(x)\ \psi(x) = 1$$

is identically satisfied.

Hence

$$p(A)\ g(A) + q(A)\ \psi(A) = E, \text{ i. e.,}$$

$$p(A)\ g(A) = g(A)\ P(A) = E$$

from which we see g(A) is non-singular.

Conversly, let g(A) be non-singular but suppose g(x) and ψ (x) are not relatively prime. Then by Lemma 3.1. there are polynomial h(x) and k(x) with

$$h(x)\ g(x) = k(x)\ \psi(x)$$

Thus

$$h(A)\ g(A) = k(A)\ \psi(A) = 0$$

$$h(A)\ g(A) = 0$$

i.e. $$h(A) = 0$$

since g(A) is non-singular. But degh(x) < deg ψ(x) and this contradicts the definition of the minimal polynomial. Hence $(g(x), \psi(x)) = 1$.

Theorem 3.2. Let $\psi(x) = (x-x_1)^{m_1}\ (x-x_2)^{m_2} \ldots (x-x_s)^{m_s}$, $m = \sum_{i=1}^{s} m_i$, be the minimal polynomial of a matrix A. If the polynomials $f_1(x), f_2(x), \ldots$ are relatively prime to ψ (x) and

$$f_i(x) \equiv r_i(x) \pmod{\psi(x)}$$

then

(i) $r_h(A)\ r_k(A) = r_k(A)\ r_h(A)$, $(h,k = 1,2,\ldots)$

(ii) For each h there exists a p(A) matrix such that

$$r_h(A)\ p(A) = p(A)\ r_h(A) = E$$

Proof. (i). Since $f_i(x) \equiv r_i(x) \pmod{\psi(x)}$ we have the following

$$f_h(x) = q_h(x)\,\psi(x) + r_h(x)$$

and

$$f_k(x) = q_k(x)\,\psi(x) + r_k(x)\ .$$

Being $f_h(A) = r_h(A)$ and $f_k(A) = r_k(A)$ we get

$$r_h(A)\ r_k(A) = r_k(A)\ r_h(A)$$

(ii) Since the polynomials $f_h(x)$ and $\psi(x)$ are relatively prime, there exist $p(x)$ and $q(x)$ polynomials.

such that

(1)$p(x)\ f_h(x) + q(x)\ \psi(x) = 1$

is identically safisfied.

where $\deg p(x) < \deg \psi(x)$ and $\deg q(x) < \deg f_h(x)$.

On the other hand, if we use $f_h(x) \equiv r_h(x) \pmod{\psi(x)}$ or $f_h(x) = k(x)\,\psi(x) + r_h(x)$ on the above relation, we get

$$p(x)\ [k(x)\,\psi(x) + r_h(x)] + q(x)\,\psi(x) = 1$$

$$p(x)\ r_h(x) + [p(x)\ k(x) + q(x)\ ]\,\psi(x) = 1$$

$$p(x)\ r_h(x) \equiv 1 \pmod{\psi(x)}$$

This means

(2) $p(A)\ r_h(A) = r_h(A)\ p(A) = E$

From (1) and (2) we have shown the existence of inverse of $r_h(A)$ matrix.

Comparing the results, we have

$$p(A)\,f_h(A) = f_h(A)\,p(A) = E \text{ and } p(A)\,r_h(A) = r_h(A)\,p(A) = E$$

$$r_h(A)\ p(A)\ f_h(A) = r_h(A)\ p(A)\ f_h(A)$$

$$Ef_h(A) = r_h(A)E$$

$$f_h(A) = r_h(A).$$

This shows that the uniqueness of the inverse of $r_h(A)$ matrix.

4. We seperate the polynomaials $f_i(x) \in F[x]$, $(i=1, 2, \ldots)$ into three sets.

(i) We denote the set of polynomials with $f_i(x) \equiv 0 \pmod{\psi(x)}$ by M. If For each $f_i(x) \in M$, we have.

$$f_i(x) = q_i(x)\ \psi(x)$$

$$f_i(A) = q_i(A)\ \psi\ (A) = 0,\ f_i(A) = 0$$

This means that M contains all annihilating polynomials of A and minimal polymnomial of matrix A.

(ii) Let $(f_i(x), \psi\ (x)\ ) = 1$ and $f_i(x) \equiv r_i(x)\ (\text{mod}\ \psi\ (x)\ )$

This set will be shown by N. If for any $f_i(x)\ \varepsilon\ N.\ f_i(x) = q_i(x)\ \psi(x) + r_i(x)$ and $(f_i(x), \psi\ (x)) = 1$, then we have

$$(f_i(x), \psi\ (x)\ ) = (q_i\ (x)\ \psi\ \ (x) + r_i\ (x), \psi\ (x)) = (r_i\ (x), \psi\ (x)\ ) = 1$$

$$p(x)\ r_i(x) + q(x)\ \psi\ (x) = 1$$

$$p(A)\ r_i(A) = r_i(A)\ p(A) = E$$

According to the Theorem 3.1. and 3.2., the matrices which are in the set N form a commutative group. Using Definition 1.2, 1.3 and Lemma 1.2 we see that this commutative group and $r_i(x)$ (mod ψ (x)) are isomorphic.

(iii) Let $(f_i(x), \psi(x)\ ) = d_i(x) \neq 1$ and

$f_i(x) \equiv r_i(x)\ (\text{mod}\ \psi\ (x)\ )$. This set will be shown by Q. For any $f_i(x)\ \varepsilon\ Q$ we have $(f_i(x), \psi\ (x)\ ) = d_i(x)$ as it is done similarly in (ii). Hence

$$p(x)\ r_i(x) + q(x)\ \psi(x) = d_i(x)$$

$$p(A)\ r_i(A) = r_i(A)\ p(A) = d_i(A)$$

On the other hand, since the degrees of each polynomials p(x), $r_i(x)$ and $d_i(x)$ are less than degree of minimal polynomial ψ (x). We have

$$p_i(A) \neq 0,\ r_i(A) \neq 0\ ,\ d_i(A) \neq 0$$

In addition; being deg $h(x) < \deg \psi\ (x)$ and by Lemma 3.1., we get

$$h(x)\ r_i(x) = k\ (x)\ \psi\ (x)$$

$$h\ (A)\ r_i\ (A) = r_i\ (A)\ h(A) = 0$$

A non-zero square matrix is a divisor of zero if and only if its is singular. In this case, for any polynomial $f_i(x)$ the $r_i(A)$ matrices are singular in the set Q.

ÖZET

Bu çalışmada A, nxn mertebeden bir matris ile bunun m ninci dereceden $\Psi(x)$ minimal polinomu göz önüne alınıyor. n^2 –boyutlu f_i (A) matrisler uzayında

$$(f_i(x), \Psi(x)) = 1 \text{ ve } f_i(x) \equiv r_i(x) \ (\text{mod}\, \Psi(x))$$

olan bütün f_i(A) matrislerinin m-boyutlu alt uzayında r_i(A) matrislerinin r_i(x) (mod Ψ(x) polinomlarına izomorf bir komutatif grup teşkil ettiği gösterilmiş ve ayrıca bu uzayın f_i (A) matrislerinin sıfır, singüler ve singüler olmamasına göre f_i (x) polinomlarının bir tasnifi yapılmıştır.

REFERENCES

[1] F. R. Gantmacher, The Theory of Matrices, Chelsea Pub. Co., Vol I, pp. 110 (1960).

[2] Robert M. Thrall and Leonard Tornheim, Vector Space and Matrices, John Wiley and Sons, inc., pp. 213 (1957).

Prix de l'abonnement annuel

Turquie : 15 TL; Étranger: 30 TL.

Prix de ce numéro : 5 TL (pour la vente en Turquie).

Prière de s'adresser pour l'abonnement à : Fen Fakültesi

Dekanlığı Ankara, Turquie.

Ankara Üniversitesi Basımevi. Ankara – 1975