BAREKENG: Jurnal Ilmu Matematika dan Terapan
September 2020 Vol. 14 No. 3 Page 473–480
P-ISSN: 1978-7227 E-ISSN: 2615-3017
: https://doi.org/10.30598/barekengvol14iss3pp473-480
National Accredited in SINTA 3, Decree No.: 28/E/KPT/2019

FIELD FORMATION OF CIRCULANT MATRIX

Pembentukan Lapangan Atas Matriks Sirkulan

Mahfudz Reza Fahlevi*

SMA Al-Maahira IIBS Malang
Jl. Raya Karanglo, Kepuharjo, Kec. Karang Ploso, Malang, Jawa Timur 65153, Indonesia

*e-mail: *mahfudzrezafahlevi@gmail.com*
Corresponding Author

Abstract

The axioms of fields satisfy over sets of numbers such as $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Generally, a set matrix is not commutative for binary multiplication properties, such that cannot satisfy of field axioms. In this paper we will discuss the circulant matrix set $\mathbb{CIRN}_n(a)$ which satisfies the commutative properties of multiplication, then it will be shown that the definition of a field is satisfied by the circulant matrix $\mathbb{CIRN}_n^*(a)$. This can provide a new perspective on a field formed by matrix.

Keywords: *Circulant matrix, Field axioms*

Submitted: 08th Agustus 2020 *Accepted: 30th August 2020*

1. INTRODUCTION

The algebraic structure is defined as a non-empty set in which at least one equivalence relation (equality) and one or more binary operations are defined [7]. The number of operations and axioms that apply to a structure will be the difference between one algebraic structure with another. One form of algebraic structure is a field.

A field is another special type of ring. The axioms that must be satisfied by a field include the axioms of a commutative ring equipped with certain axioms, so that an algebraic structure of field will be more complex compared to the structure of group or ring. In many literatures, the fields that have been given and discussed are sets of numbers. An example is the set of numbers $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. In this paper we will discuss a set of matrix that can satisfy the axioms of a field, which is a set of circulant matrix.

Circulant matrix is one type of matrix that has special properties. The special properties possessed by the circulant matrix is the commutative multiplication. In addition, the circulant matrix also has a well-defined closure property [9]. A circulant matrix be defined as follows.

Definition 1. (Circulant Matrix)

Let $\boldsymbol{a} = (\boldsymbol{a_0}, \boldsymbol{a_1}, \cdots, \boldsymbol{a_{n-1}})$ *then the circulant matrix* $\boldsymbol{A} = \left(\boldsymbol{a_{i,i}}\right)_{\boldsymbol{i,j}}$ *where* $\boldsymbol{a_{i,j}} = \boldsymbol{a_{j-i(mod\ n)}}$.

The circulant matrix A with order n is denoted by $CIRC_n(a)$. An $n-$square circulant matrix is a matrix of the form.

$$CIRC_n(a) = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_0 \end{bmatrix}$$

The circulant matrix is definitively a square matrix that has the properties binary operations that apply the same the ordinary matrix. Circulant matrix satisfies the definition of the ring over addition and multiplication operations.

Proposition 1. $[\mathbb{CIRN}_n(a), +, \times]$ *is a ring.*
Proof. see in [4 - 6]

In this paper will be shown that the definition of a field is satisfied by set of the circulant matrix $\mathbb{CIRN}_n^*(a)$.

2. RESULT AND DISCUSSION

Generally, the matrix set satisfies the axiom of the abelian group over addition, but this is not the case for multiplication, especially in the commutative properties of multiplication. In the circulant matrix, the multiplicative commutative properties are well-defined, as are the closed properties. To prove the multiplication properties of a circulant matrix we need information about the diagonalization and determinant of the circulant matrix.

Eigenvalues, eigenvectors, and matrix diagonalization on the circulant matrix are related to diagonalization with the cyclic permutation matrix $[W_n]$ and the Fourier matrix $[F_n]$. The definition of cyclic permutation matrix $[W_n]$ and Fourier matrix has been defined by Davis [4].

A matrix can be diagonalized by a matrix with its columns in the form of eigenvectors on the matrix [1]. The W_n matrix can be diagonalized by a Q_n matrix with the following form:

$$Q_n = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^1 & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix}$$

matrix Q_n has the following inverse:

$$Q_n{}^{-1} = \frac{1}{n}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix}$$

to prove it, it will be shown that $Q_n Q_n{}^{-1} = I_n$:

$$Q_n Q_n{}^{-1} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{1} & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \frac{1}{n} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix}$$

$$Q_n Q_n{}^{-1} = \frac{1}{n}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{1} & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix}$$

$$Q_n Q_n{}^{-1} = \frac{1}{n}\begin{bmatrix} 1+1+\cdots+1 & 1+\omega^{-1}+\cdots+\omega^{-(n-1)} \\ 1+\omega^{1}+\cdots+\omega^{(n-1)} & 1+\omega\omega^{-1}+\cdots+\omega^{(n-1)}\omega^{-(n-1)} \\ \vdots & \vdots \\ 1+\omega^{(n-1)}+\omega^{(n-1)(n-1)} & 1+\omega^{(n-1)-1}+\cdots+\omega^{(n-1)((n-1)-1)} \end{bmatrix}$$

$$\begin{matrix} \cdots & 1+\omega^{-(n-1)}+\omega^{-(n-1)(n-1)} \\ \cdots & 1+\omega^{1-(n-1)}+\cdots+\omega^{(n-1)(1-(n-1))} \\ \ddots & \vdots \\ \cdots\cdots & 1+\omega^{(n-1)}\omega^{-(n-1)}+\cdots+\omega^{(n-1)^2}\omega^{-(n-1)^2} \end{matrix}\Bigg]$$

Brown and Churchill [2] stated in their book the results of the matrix above relate to the theorem of complex number identity equations, so that:

$$Q_n Q_n{}^{-1} = \frac{1}{n}\begin{bmatrix} 1+1+\cdots+1 & 0 & \cdots & 0 \\ 0 & 1+1+\cdots+1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1+1+\cdots+1 \end{bmatrix}$$

$$Q_n Q_n{}^{-1} = \begin{bmatrix} \dfrac{1+1+\cdots+1}{n} & 0 & \cdots & 0 \\ 0 & \dfrac{1+1+\cdots+1}{n} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \dfrac{1+1+\cdots+1}{n} \end{bmatrix}$$

$$Q_n Q_n{}^{-1} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = I_n.$$

it is proven that $Q_n Q_n{}^{-1} = I_n$. So the diagonalization of the W_n matrix by the Q_n matrix is as follows:

$$Q_n{}^{-1} W_n Q_n = D \tag{1}$$

where D is a diagonal matrix [10]. The matrix in Equation (1) are similar [11], so the diagonal matrix D which is a matrix with consecutive diagonal entries, the eigenvalue associated with the $\boldsymbol{u}_k$ eigenvector in the

matrix W_n. The eigenvalue matrix W_n is the $n-$square root of units, so that the D matrix is a matrix with the following form:

$$D = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{n-1} \end{bmatrix} = diag(1, \omega, \cdots, \omega^{n-1})$$

RECALL the matrix form in Equation (1):

$$Q_n{}^{-1} W_n Q_n = D$$

$$\frac{1}{n}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix} W_n \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{1} & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} = D \tag{2}$$

by factoring $\frac{1}{n}$ in to $\frac{1}{\sqrt{n}}\frac{1}{\sqrt{n}}$ so that the matrix form in Equation (2), can be written as follows:

$$\frac{1}{\sqrt{n}}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix} W_n \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{1} & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} = D \tag{3}$$

Equation (3) satisfies the Fourier matrix form, it can be expressed in following form:

$$F_n{}^{-1} W_n F_n = D$$

$$W_n = F_n D F_n{}^{-1} \tag{4}$$

with applying the polynomial function in (4), then:

$$P(W_n) = P(F_n D F_n{}^{-1})$$

$$P(W_n) = F_n P(D) F_n{}^{-1} \tag{5}$$

Zhang [12] stated that equations in (5) is theorem of polynomial diagonalization.

Among the permutation matrix, the matrix W_n plays a fundamental role in the theory of circulants. Goldberg [8] state that $CIRC_n(a) = P(W_n)$, then Equation (4) and Equation (5) can be related, such that:

$$CIRC_n(a) = P(W_n)$$

$$CIRC_n(a) = F_n\, P(D) F_n{}^{-1}$$

$$F_n{}^{-1}\, CIRC_n(c)\, F_n = P(D) \tag{6}$$

matrix $P(D)$ symbolized by matrix Λ then equation (6) can be expressed in following form:

$$F_n{}^{-1}\, CIRC_n(c)\, F_n = \Lambda \tag{7}$$

such that,

$$F_n{}^{-1}\, CIRC_n(a)\, F_n = \begin{bmatrix} \lambda_0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{n-1} \end{bmatrix}$$

Goldberg [8] stated in their book that λ_k is eigenvalues on permutation matrix Wn was using to decomposition of circulant matrix, therefore the circulant matrix $CIRC_n(a)$ can be diagonalized by a Fourier matrix. Equation (7) can also be expressed in following form:

$$CIRC_n(a) = F_n \cdot \Lambda \cdot F_n{}^{-1} \tag{8}$$

where Λ is a diagonal matrix. To prove the distributive properties in $CIRC_n(a)$, the following theorem are obtained.

Theorem 1. *Two distributive laws hold in* $[\mathbb{CIRN}_n(a), +, \times]$.
Proof. Let circulant matrix:

$$A = CIRC_n(a)\ ;\ B = CIRC_n(b)\ ;\ C = CIRC_n(c)$$

to prove the circulant matrix set satisfies the distributive properties, it will be shown that $A(B + C) = AB + AC$. The matrix A, B, and C can be expressed in the following form:

$$A = F\,\Lambda_A\,F^{-1} \quad ; \quad B = F\,\Lambda_B\,F^{-1} \quad ; \quad C = F\,\Lambda_C\,F^{-1}$$

will be proven:

$$A(B + C) = AB + AC$$

First side:

$$A(B + C) = F\,\Lambda_A\,F^{-1}(F\,\Lambda_B\,F^{-1} + F\,\Lambda_C\,F^{-1})$$

$$A(B + C) = F\,\Lambda_A\,F^{-1}(F(\Lambda_B\ + \Lambda_C)F^{-1})$$

$$A(B + C) = F\,\Lambda_A\ I\ (\Lambda_B\ + \Lambda_C)F^{-1}$$

$$A(B + C) = F\,\Lambda_A\,(\Lambda_B\ + \Lambda_C)F^{-1}$$

with the diagonal matrix properties, then:

$$A(B + C) = F(\,\Lambda_A\,\Lambda_B\ +\ \Lambda_A\,\Lambda_C)F^{-1} \tag{9}$$

In the second side:

$$AB + AC = (F\,\Lambda_A\,F^{-1}F\,\Lambda_B\,F^{-1}) + (F\,\Lambda_A\,F^{-1}F\,\Lambda_C\,F^{-1})$$

$$AB + AC = (F\,\Lambda_A\ \Lambda_B\,F^{-1}) + (F\,\Lambda_A\ \Lambda_C\,F^{-1})$$

$$AB + AC = F\,\Lambda_A\ \Lambda_B\,F^{-1} + F\,\Lambda_A\ \Lambda_C\,F^{-1}$$

$$AB + AC = F(\,\Lambda_A\ \Lambda_B\ +\ \Lambda_A\ \Lambda_C)\,F^{-1} \tag{10}$$

since $A\,(B\ +\ C)\ =\ AB\ +\ AC$, this means that circulant matrix satisfies the distributive property of multiplication with addition. ■

Furthermore, in field formation over a set of matrix it will also show the inverse properties of the circulant matrix. Let multiplication identity matrix:

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

which can be written as a circulant matrix $CIRC_n(1,0,0,\cdots 0)$, so that the matrix $I_n = CIRC_n(1,0,0,\cdots 0) \in \mathbb{CIRN}_n(a), a \in \mathbb{R}$ is unity of ring $[\mathbb{CIRN}_n(a), +, \times]$. In this section, will be shown that the inverse multiplication of the circulant matrix is also a circulant matrix.

Theorem 2. *The inverse of an invertible element of* $\mathbb{CIRN}_n(a)$ *also belongs to* $\mathbb{CIRN}_n(a)$
Proof. Based on Equation (8) if V is a non-singular circulant matrix, then:

$$V = F_n\,\Lambda_v {F_n}^{-1} \tag{11}$$

so that:

$$V^{-1} = F_n\,(\Lambda_v)^{-1} {F_n}^{-1} \tag{12}$$

Furthermore, to prove this theorem it will be shown that the diagonal matrix $(\Lambda_v)^{-1} = \Lambda_{V^{-1}}$. Based on Equation (12) it appears that the inverse of the circulant matrix can be diagonalized by the matrix F_n, based on equation (11), the equation (12) can be written in the form:

$$V^{-1} = F_n \, \Lambda_{V^{-1}} {F_n}^{-1} \tag{13}$$

so it is proven $(\Lambda_v)^{-1} = \Lambda_{V^{-1}}$ ■

Theorem 2 states that not all circulant matrix have an inverse, this can happen because there are circulant matrix that have zero determinants, for example a circulant matrix has zero determinants is the matrix $CIRC_n(a, a, a, \cdots a), a \in \mathbb{R}$. Then another example is a circulant matrix whose elements have a pattern on the first row, such that $\boldsymbol{a} = (\boldsymbol{a_0}, \boldsymbol{a_1}, \cdots, \boldsymbol{a_{n-1}})$ then the elements in even order are always the same $\boldsymbol{a_0} = \boldsymbol{a_2} = \boldsymbol{a_4} = \cdots$ and the odd order always the same $\boldsymbol{a_1} = \boldsymbol{a_3} = \boldsymbol{a_5} = \cdots$.

Furtheremore, field formation. Based on Theorem 2 states that each circulant matrix will have an inverse if and only if the matrix have a determinant value which is not zero. In this paper, will be defined a set $\mathbb{CIRN}_n^*(a)$ is a set of circulant matrix where the determinant of each circulant matrix is not zero with zero matrix. Based on the properties of the circulant matrix described in Theorem 1 and Theorem 2, the set $\mathbb{CIRN}_n^*(a)$ for the binary operations addition and multiplication is a field if and only if the set is $\mathbb{CIRN}_n^*(a)$ satisfies the commutative property of multiplication.

Distinguishing matrix generally with a circulant matrix is on the results of a commutative and well-defined multiplication. The following proposition is proven:

Proposition 2. Multiplication in $\mathbb{CIRN}_n(a)$ is commutative.
Proof. Let matrix circulant:

$$A = CIRC_n(a) \text{ dan } B = CIRC_n(b)$$

to prove that the circulant matrix set satisfies the distributive properties, it will be shown that $AB = BA$. Matrix A and B can be expressed in the following form:

$$A = F \, \Lambda_A \, F^{-1} \quad ; \quad B = F \, \Lambda_B \, F^{-1}$$

then:

$AB = (F \, \Lambda_A \, F^{-1})(F \, \Lambda_B \, F^{-1})$

$AB = F \, \Lambda_A \, F^{-1} F \, \Lambda_B \, F^{-1}$

$AB = F \, \Lambda_A \; I \, \Lambda_B \, F^{-1}$

$AB = F \, \Lambda_A \, \Lambda_B \, F^{-1}$

with the diagonal matrix properties then:

$AB = F \, \Lambda_B \; \Lambda_A \, F^{-1}$

$AB = F \, \Lambda_B \; \mathrm{I} \, \Lambda_A \, F^{-1}$

$AB = (F\Lambda_B \, F^{-1})(F\Lambda_A \, F^{-1})$

$AB = BA$

Since $AB = BA$, thus $\mathbb{CIRN}_n(a)$ is commutative. ■

3. CONCLUSION

Matrix set $\mathbb{CIRN}_n(a)$ is a set of circulant matrix that can statisfies the commutative ring properties of addition and multiplication operations. In order for the matrix set satisfy the field axioms, it is necessary to impose restrictions on the matrix $\mathbb{CIRN}_n(a)$. $\mathbb{CIRN}_n^*(a)$ is a set of non-singular circulant matrix with zero matrix, such that each element of the matrix set $\mathbb{CIRN}_n^*(a)$ has a multiplicative inverse and statify the commutative properties.

$\mathbb{CIRN}_n^*(a)$ is a set of matrix that satisfies the axioms of a field for binary operations of addition and multiplication, with the addition identity is a zero matrix $\big(CIRC_n(0, 0, \cdots, 0)\big)$ and the multiplication identity (unit) is the matrix $I_n = \big(CIRC_n(1, 0, \cdots, 0)\big)$.

REFERENCE

[1] Anton H. and Rorres C., *Elementary Linear Algebra 9th Edition*, USA. John Wiley & Sons, 2005
[2] Brown J. W. and Churchill R. V., *Complex Variables and Aplication, New York. McGraw Hill*, 2009.
[3] Cleghorn C. S., "*Application of Generalized Inverses and Circulant Matrix to Iterated Functions on Integers*". Journal of Rose-Hulman Undergraduate Mathematics Vol. 2, Iss. 2, Article 3. USA: Texas. 2001
[4] Davis P. J., *Ciculant Matrix*, Canada. John Wiley & Sons, 1979.
[5] Jitman S., "*Vector-Circulant Matrix over Finite Fields and Related Codes*". Journal of Rings and Algebras Vol I, New York. Cornell University, 2014.
[6] Pop V. and Furdui O., *Square Matrix of Order 2 Theory Applications and Problems*, New York. Springer, 2017.
[7] Gilbert L. and Gilbert J., *Elements of Modern Algebra*, Stamford USA. Cengage Learning, 2015.
[8] Goldberg J. L., *Matrix Theory with Aplication*, USA. McGraw-Hill.1991.
[9] Jones A. W., *Circulant*s, Pennsylvania. Carlisle, 2008.
[10] Kra I. and Simanca S. R., "*On Circulant Matrix*". Siam Rev., 59: 368-377. DOI: 10.1090/noti804, 2012.
[11] Poole D., *Linear Algebra A Modern Introduction Second Edition*, USA. Thomson, 2006.
[12] Zhang F. *Matrix Theory Basic Result and Techiques*, New York. Springer, 2010.