J. Indones. Math. Soc.
Vol. 29, No. 02 (2023), pp. 150–155.

A NOTE ON FREE MODULE DECOMPOSITION OVER A PRINCIPAL IDEAL DOMAIN

Ni Wayan Switrayni[a], I Gede Adhitya Wisnu Wardhana[b], Qurratul Aini[c]

Department of Mathematics, Universitas Mataram, Indonesia,
[a]niwayan.switrayni@unram.ac.id, [b]adhitya.wardhana@unram.ac.id,
[c]qurratulaini.aini@unram.ac.id

Abstract. Some methods have been used to express a finitely generated module over a principal ideal domain as a finite direct sum of its cyclic submodules. In this paper, we give an alternative technique to decompose a free module with finite rank over a principal ideal domain using eigen spaces of its endomorphism ring.

Endomorphism, Free Module, Principal Ideal Domain, Eigen Space.

1. INTRODUCTION

There are many decompositions of a module that are brought up to make it easy to analyze like the decomposition of a vector space by its basis [1]. Some research on the decomposition of a finitely generated module had been conducted such as by Hadjirezaei and Hedayat [3] who studied its decomposition using fitting ideals. A recent study gives a new way of proving the Main Fundamental Theorem for the finitely generated module over a principal ideal domain (PID) was carried out in 2020 in a favor of the module decomposition [4].

A study on matrices over a commutative ring investigated the properties of eigenspaces of a matrix. It was concluded that the eigenspace of a matrix over a commutative ring no need to have a basis. In this paper, we provide another technique to decompose a free module over a principal ideal domain with finite rank using its module endomorphism. First, we generalize the concept of the eigenspaces of a matrix into a general module endomorphism and then express this free module into a direct sum of these eigenspaces. Moreover, some particular matrices are also used in finding such endomorphism.

2020 Mathematics Subject Classification: 13C05, 13C12.
Received: 04-07-2022, accepted: 13-04-2023.

General properties, such as operations, determinants, etc on $M_n(R)$, the set of square matrices over a ring with unity R, have been defined as those in matrices over a field, see the details on [2]. In this paper, $U(R)$ will denote the set of all units in R. Some basic theories and notations are given as follows.

Definition 1.1. [2] *Let $A \in M_{m\times n}(R)$ and suppose $1 \leq t \leq min\{m, n\}$. The $t \times t$ minor of A is the determinant of a $t \times t$ submatrix of A.*

Theorem 1.2. [2] *If $A \in M_n(R)$, then A is invertible if and only if $det(A) \in U(R)$.*

Definition 1.3. [2] *Let $A \in M_{m\times n}(R)$. For each $t = 1, ..., r = min\{m, n\}$, $I_t(A)$ will denote the ideal in R generated by all $t \times t$ minors of A. Moreover, for any integer $t > min\{m, n\}$ and $t \leq 0$, $I_t(A) = \{0\}$ and $I_t(A) = R$ respectively.*

Definition 1.4. [2] *Let $A \in M_{m\times n}(R)$. The rank of A, denoted by $rk(A)$ is the following integer: $rk(A) =$max $\{t|Ann_R(I_t(A)) = 0\}$, where $Ann_R(I_t(A))$ denotes the annihilator of $I_t(A)$.*

Theorem 1.5. [2] *If $A \in M_n(R)$, then $rk(A) < n$ if and only if $det(A) \in Z(R)$.*

Theorem 1.6. [2] *Given $A \in M_{m\times n}(R)$. The homogenous linear system $Ax = 0$ has a non-trivial solution if and only if $rk(A) < n$.*

Now, the definition of eigen value and eigen vector of a square matrix over R is given as follows.

Definition 1.7. [2] *Given A be a matrix in $M_n(R)$.*

(1) An element $d \in R$ is called as eigen value of A if $A\xi = d\xi$ for some non-zero vector $\xi \in R^n$.
(2) A non-zero vector $\xi \in R^n$ is called an eigen vector of A if $A\xi = d\xi$ for some $d \in R$
(3) Let d be an eigen value of A. $E(d) = \{\xi \in R^n|A\xi = d\xi\}$ is called the eigen space associated to d.

In the definition, it is clear that $E(d) = NS(dI - A)$, where $NS(dI - A)$ denotes the null space of the matrix $dI - A$ [2]. Now we move to some basic definitions and theorems in module theory.

Definition 1.8. [5] *A module M over R is called the direct sum of a family $\mathcal{F} = \{S_i|i \in I\}$ of submodules of M, denoted by $M = \bigoplus \mathcal{F}$ or $M = \bigoplus_{i\in I} S_i$ if satisfying:*

(1) $M = \sum_{i\in I} S_i$
(2) For each $i \in I$, $S_i \cap (\sum_{j\neq i} S_j) = \{0\}$.

Subsequently, the definition of rank of a free module over a commutative ring with unity is given as follows.

Definition 1.9. [5] *Suppose R is a commutative ring with unity. The rank of a nonzero R-free module M, denoted by $rk(M)$, is the cardinality of any basis for M. Moreover, the trivial module $\{0\}$ has rank 0.*

Note that we used same symbol for the rank of a module and that of a matrix as those two definitions are analogous like in vector spaces. Moreover, when the base ring is a principal ideal domain, some significant properties apply.

Theorem 1.10. [5] *Let M be a free module over a principal ideal domain R. Any submodule S of M is also free and $rk(S) \leq rk(M)$.*

Theorem 1.11. [5] *A finitely generated module over a principal ideal domain is free if and only if it is torsion-free.*

2. MAIN RESULTS

We begin this section by defining the notion of eigen vector of a module endomorphism over a commutative ring with unity.

Definition 2.1. [2] *Given M be an R-module and $\theta : M \to M$ be an endomorphism. An eigen vector of θ is a non-zero vector v in M satisfying $\theta(v) = \lambda v$ for some $\lambda \in R$. The scalar λ is called the eigen value of θ associated with the eigen vector v.*

Now we have a properties that the characterization polynom value must be a zero or a zero divisor, and we give the notation $Z(R)$ is the collection of zero divisor of ring R with zero element.

Theorem 2.2. *Given M be a free R-module with rank n. Let $A = [\theta]_B$ be a representation matrix of an endomorphism $\theta : M \to M$, where B is a basis of M. A scalar $\lambda \in R$ is an eigen value of θ if and only if $C_A(\lambda) \in Z(R)$.*

Proof. Let $\lambda \in R$ be an eigen value of θ. Hence $\theta(v) = \lambda v$ for some $v \in M$ and $v \neq 0$. This implies $[\theta(v)]_B = \lambda[v]_B$ or we can write $\lambda I_n[v]_B - A[v]_B = (\lambda I_n - A)[v]_B = 0$. Since $v \neq 0$, we have $[v]_B \neq 0$, which means that the equation has a nonzero solution. By Theorem (1.6), we have $rk(\lambda I_n - A) < n$, and so by Theorem (1.5), $C_A(\lambda) = det(\lambda I_n - A) \in Z(R)$. Conversely, suppose that $C_A(\lambda) \in Z(R)$. By Theorem (1.5), we have $rk(\lambda I_n - A) < n$, and by Theorem (1.6) we have $(\lambda I_n - A)w = 0$ for some $w \in R^n, w \neq 0$. Now, set $v \in M$ that satisfies $[v]_B = w$, hence $\theta(v) = \lambda v$. □

In the rest of this paper, R will denote a principal ideal domain and M will be a free module with finite rank over R. Also, the set of all eigen values of an endomorphism θ will be denoted by $\mathcal{R}(\theta)$.

Theorem 2.3. *Given $rk(M) = n$ and $\theta : M \to M$ be an endomorphism on free module M. The set of eigen vectors from distinct eigen spaces is linearly independent.*

Proof. Let $S = \{v_1, v_2, ..., v_r\}$ be a set of eigen vectors with v_i is an eigen vector associated with eigen value λ_i where $\lambda_i \neq \lambda_j$ when $i \neq j$, $i, j = 1, 2, ..., r$. Suppose

S is linearly dependent. Since M is free, we have every non zero singleton set in M is linearly independent. Now, let k be the greatest number where $1 \leq k < r$ (obtained by re-indexing if necessary) so that $\{v_1, v_2, ..., v_k\}$ is linearly independent. Hence $\{v_1, v_2, ..., v_k, v_{k+1}\}$ is linearly dependent. Hence the equation $r_1v_1 + r_2v_2 + ... + r_kv_k + r_{k+1}v_{k+1} = 0$ is not only satisfied by all scalars with zero values, which at least (without loss of generality) $\lambda_{k+1} \neq 0$. From this equation we obtain $r_1\theta(v_1) + r_2\theta(v_2) + ... + r_k\theta(v_k) + r_{k+1}\theta(v_{k+1}) = 0$ or i.e with $r_1\lambda_1v_1 + r_2\lambda_2v_2 + ... + r_k\lambda_kv_k + r_{k+1}\lambda_{k+1}v_{k+1} = 0$. By a multiplication of λ_{k+1} to the first equation and then subtract with the second equation, we have $r_1(\lambda_{k+1} - \lambda_1)v_1 + r_2(\lambda_{k+1} - \lambda_2)v_2 + ... + r_k(\lambda_{k+1} - \lambda_k)v_k = 0$. By the independence of $\{v_1, v_2, ..., v_k\}$, then we have $r_i(\lambda_{k+1} - \lambda_i) = 0$ for all $i = 1, 2, ..., k$. Since $\lambda_{k+1} \neq \lambda_i$ and R is an integral domain, $r_i = 0$ for all $i = 1, 2, ..., k$. So we have $r_{k+1}v_{k+1} = 0$ and implies $r_{k+1} = 0$, which is a contradiction. □

It is worth noting that the corollary below is a direct result of the independence condition on Theorem 2.3.

Corollary 2.4. *Let $\theta : M \to M$ be an endomorphism with $R(\theta)$ is all different eigen value of θ. Hence $\sum_{\lambda \in \mathcal{R}(\theta)} E_\lambda = \bigoplus_{\lambda \in \mathcal{R}(\theta)} E_\lambda$.*

In fact, we can consider R^n as an R-module. The following theorem will tell us not only about the existence of a decomposition of R^2 into some eigen spaces but it will also give a method to find such eigen spaces.

Theorem 2.5. *If $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in M_2(R)$ such that $a - c \neq 0$, then $R^2 = E(a) \oplus E(c)$ if and only if $(a - c) \mid b$.*

Proof. If $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in M_2(R)$ such that $a - c \neq 0$, then the set of all eigen values of A, $\mathcal{R}(A) = \{a, c\}$. For $\lambda = a$ we have $E(a) = NS \begin{bmatrix} 0 & -b \\ 0 & a-c \end{bmatrix} = R \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.
For $\lambda = c$, we have $E(c) = NS \begin{bmatrix} c-a & -b \\ 0 & 0 \end{bmatrix}$.
If $(a - c) \mid b$, then we have $E(c) = R \begin{bmatrix} -k \\ 1 \end{bmatrix}$ for $k \in R$ such that $b = k(a - c)$.
By Theorem (2.3), $S = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -k \\ 1 \end{bmatrix} \right\}$ is linearly independent. Moreover, R^2 is also spanned by S, since $\det \left(\begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} \right) = 1 \in U(R)$. This implies $R^2 = E(a) \oplus E(c)$.
Conversely, if $R^2 = E(a) \oplus E(c)$, then R^2 has a basis containing eigen vectors from $E(a)$ and $E(c)$. Since $E(a) = R \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, and $R^2 = E(a) \oplus E(c)$ then there exists $e, f \in R$ with $f \in U(R)$ such that $(c - a)e - bf = 0$. Noted that f must be a unit, otherwise it has no basis. This implies $b = (c - a)ef^{-1}$, and means that $(c - a) \mid b$. □

Now, let consider for a free module R^n with rank n for any $n \geq 2$.

Theorem 2.6. *Given* $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix} \in M_n(R)$ *with* $a_{ii} - a_{kk} \neq 0$ *for any* $i \neq k$. *If* $(a_{ii} - a_{kk}) \mid a_{ij}$ *for all* $i < j \leq n$, *then* $R^n = \bigoplus_{i=1}^n E(a_{ii})$.

Proof. To prove this, we necessary show that the eigen vectors of λ_i has the form $(k_{i1}t, k_{i2}t, ..., t, 0, ..., 0) = t(k_{i1}, k_{i2}, ..., 1, 0, ..., 0)$ where $t \in R$ and for some $k_{i1}, k_{i2}, ..., k_{i(i-1)} \in R$ i.e with having an eigen vector with 1 at the i-th component and 0 for all j-components when $j > i$. We will prove this by induction on n. For $n = 2$, it has been proved by Theorem (2.5). Suppose this is true for $n = k - 1$. Now, let $n = k$ and consider the characteristic equation of A, that is:

$$|\lambda I - A| = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1k} \\ 0 & \lambda - a_{22} & \cdots & -a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda - a_{kk} \end{vmatrix} = 0, \text{ hence } \lambda_i = a_{ii} \text{ for all } i = 1, ..., k.$$

It is clear that for every $i = 1, ..., k-1$, we have x_k, the k-th component of the eigen vector associated to λ_i must be 0 since $a_{ii} - a_{kk} \neq 0$. Hence the remaining equations are including $k - 1$ equations and $k - 1$ indeterminates. By the induction hypothesis which is the remaining sub-matrix having $(k - 1) \times (k - 1)$ size and together with the fact that $x_k = 0$, then the eigen vectors for λ_i for every $i = 1, ..., k - 1$ when $n = k$ are have the form $t(k_{i1}, k_{i2}, ..., 1, 0, ..., 0)$ where $t \in R$ and for some $k_{i1}, k_{i2}, ..., k_{i(i-1)} \in R$. Moreover, when $\lambda = a_{kk}$, we have the i-th equation for each $1 \leq i \leq (k - 1)$ on the linear system obtained from the characteristic equation is $(a_{kk} - a_{ii})x_i - \sum_{j=i+1}^{k} a_{ij}x_j = 0$. Since $(a_{kk} - a_{ii}) \mid a_{ij}, \forall j = i + 1, ..., k$ and $(a_{kk} - a_{ii}) \neq 0$, we have $x_i = \sum_{j=i+1}^{k} l_{ij}x_j$ for some $l_{ij} \in R$ satisfying $l_{ij}(a_{kk} - a_{ii}) = a_{ij}$. Moreover we can see that every x_j for $j = i + 1, ..., k - 1$ can be expressed in the x_k form which implies that $x_i = d_i x_k$ for some $d_i \in R$. Hence, if $x_k = s$ for $s \in R$, then the eigen vector $(x_1, x_2, ..., x_k)^T$ associated to λ_k has the form $s(d_1, d_2, ..., 1)$. This implies that for any $n \geq 2$, we have obtained n eigenvectors that span R^n. The independence of the vectors is guaranteed by Theorem (2.3). Therefore, we can write $R^n = \bigoplus_{i=1}^n E(a_{ii})$. □

One can easily conclude that the Theorem 2.5 and Theorem 2.6 deal for a lower triangular matrix with a similar way of construction.

Now we will use Theorem (2.6) to express any module with finite rank into a direct sum of its eigenspaces. This is stated in the following theorem.

Theorem 2.7. *Given* M *be a free* R*-module with rank* n *and* B *be any basis of* M *and with* $\theta : M \to M$ *be an endomorphism with representation matrix* $[\theta]_B$ *as on Theorem* (2.6). *Hence* $M = \bigoplus_{\lambda \in \mathcal{R}(\theta)} E(\lambda)$.

Proof. By Theorem (2.6), choose any basis $S = \{v_1, v_2, ..., v_n\}$ of R^n where $\{v_i\}$ is a basis for the i-th eigen space of $[\theta]_B$ with $i = 1, 2, ..., n$. By setting $m_i \in M$ such that $[m_i]_B = v_i$ for all $i = 1, ..., n$, hence $\{m_i\}$ is a basis for $E(\lambda_i)$. Thus, $M = \bigoplus_{\lambda_i \in \mathcal{R}(\theta)} E(\lambda_i)$. □

Acknowledgement. The authors would like to thank to the University of Mataram that has supported this research through the PNBP Research Funding 2021.

REFERENCES

[1] Wardhana, I. G. A. W., The Decomposition of a Finitely Generated Module over Some Special Ring, *Jurnal Teori dan Aplikasi Matematika*, **6(2)** (2022), 261-267.
[2] Brown, W. C., *Matrices Over Commutative Rings*, Marcel Dekker Inc., New York, 1993.
[3] Hadjirezaei, S., and Hedayat, S., Decomposition of Finitely Generated Modues Using Fitting Ideals, *Czechoslovak Mathematical Journal*, **70(4)** (2020), 1179-1190.
[4] Ma,X. R., Liu, H. G., and Zhang, H. L., A Note on Finitely Generated Modules over a PID, *Advances in Pure Mathematics*, **10(12)** (2020), 699-705.
[5] Roman, S., *Advanced Linear Algebra*, Third Edition, Springer, New York, 2008.