JOURNAL OF FUNDAMENTAL MATHEMATICS
AND APPLICATIONS (JFMA) VOL. 5 NO. 1 (JUN 2022)
Available online at www.jfma.math.fsm.undip.ac.id

ON CYCLIC DECOMPOSITION OF $\mathbb{Z}$-MODULE $M_{m\times r}(\mathbb{Z}_n)$

Ni Wayan Switrayni[1*], I Gede Adhitya Wisnu Wardhana[2], Qurratul Aini[3]

[1,2,3] *University of Mataram*
Email: [1*]niwayan.switrayni@unram.ac.id, [2]adhitya.wardhana@unram.ac.id, [3]qurratulaini.aini@unram.ac.id
*Corresponding author

Abstract. A torsion module over a principal ideal domain has special properties related to the way how it is decomposed either into primary or cyclic submodules. This paper carries out a special case of such module over the ring of integer, which consists of all matrices with entries from the set of integer modulo n. The results show that its decomposition depends on the prime factors of n.
Keywords: Torsion Modules, Primary Submodules, Cyclic Decomposition, Principal Ideal Domain, Integer Modulo n.

I. INTRODUCTION

Several investigations related to module decomposition have been conducted. One of those was primary and cyclic decomposition of a finitely generated module. Wardhana et al [7] wrote a cyclic decomposition of primary module $M_{2\times 2}(\mathbb{Z}_9)$ over the ring of integer $\mathbb{Z}$ in which each of the cyclic submodule has order 9. Also, in 2018, the decomposition of $M_{2\times 2}(\mathbb{Z}_n)$ with arbitrary $n \geq 2$ was given by Wardhana et al [8], in which each of the cyclic submodule is generated by a unit matrix. However, these results were still limited to 2×2 - matrices and each cyclic submodule in the internal direct sum can still be decomposed into some smaller submodules. See [1] [2] [3] [4] [5] [6] for others module decomposition.

Therefore, in this paper, we discuss a cyclic decomposition of module of matrices with entries over integer modulo n and arbitrary size (not only square matrices), $M_{m\times r}(\mathbb{Z}_n)$, which is considered as a module over ring $\mathbb{Z}$ using the primary decomposition theorem. This result will contribute to a study of torsion modules decomposition because some of those can be viewed as a module of matrices. Consequently, working on those complicated modules just can be substituted by working on matrices such that the properties of such modules will easily obtained from those of matrices.

Throughout this paper, R will denote a commutative ring with unity. Some basic definitions and theorems are given as follows.

Definition 1 [9] *Suppose that $\{M_\alpha\}_\Delta$ is a family of submodules of an R-module M such that $M_\beta \cap \sum_{\alpha\neq\beta} M_\beta = 0$ for each $\alpha, \beta \in \Delta$. Then the sum $\sum_\Delta M_\alpha$ is said to be the internal direct sum of the family $\{M_\alpha\}_\Delta$ and denoted by $\bigoplus_\Delta M_\alpha$. Moreover, if $M = \bigoplus_\Delta M_\alpha$, then M is said to be a direct decomposition of M.*

Notice that the condition $M_\beta \cap \sum_{\alpha\neq\beta} M_\beta = 0$ for each $\alpha, \beta \in \Delta$ is generally called the independence of the family $\{M_\alpha\}_\Delta$.

Definition 2 [10] *An R-module M is decomposable if it is the internal direct sum of two nonzero submodules. Otherwise, M is indecomposable.*

Now we move to another notion called as an external direct sum.

Definition 3 [11] *The external direct sum of R-modules $M_1, ..., M_n$, denoted by $M = M_1 \boxplus ... \boxplus M_n$ is the R-module whose elements are ordered n-tuples $M = \{(v_1, ..., v_n) | v_i \in M_i, i = 1, ..., n\}$ with componentwise operations $(u_1, ..., u_n) + (v_1, ..., v_n) = (u_1 + v_1, ..., u_n + v_n)$ and $r(v_1, ..., v_n) = (rv_1, ..., rv_n)$ for $r \in R$.*

Subsequently, in order to study the decomposition of the module $M_{m\times r}(\mathbb{Z}_n)$, we can see that it is a torsion module over $\mathbb{Z}$ since $\mathbb{Z}_n$ is a torsion module. The following definitions and theorems explain a torsion module and its decomposition.

Definition 4 [11] *Given an R-module M. A non-zero element $v \in M$ is called as a torsion element if there exists a non-zero element $r \in R$ such that $rv = 0$. If all elements of M are torsion elements, then M is called as torsion module.*

Definition 5 [11] *Let M be an R-module and $v \in M$. The annihilator of v is defined as $ann(v) = \{r \in R | rv = 0\}$ and the annihilator of submodule N of M is $ann(N) = \{r \in R | rN = \{0\}\}$.*

Definition 6 [11] *Given M be a module over a principal ideal domain R and N be its submodule. An order of N is defined as any generator of $ann(N)$ and denoted by $o(N)$. Moreover, the order of an element $v \in M$ is an order of submodule $\langle v \rangle$ and written as $o(v)$.*

Theorem 1 [11] *Let R be a principal ideal domain and M is a module over R. If $v \in M$ and $ann(\langle v \rangle) = \langle \alpha \rangle$, then $\langle v \rangle \approx R/\langle \alpha \rangle$.*

In Definition 6, an order of a submodule is an element of the ring that generates the annihilator of the submodule. If the order is a prime power, then the module is called as primary module. The formal definition is given as follows.

Definition 7 [11] *Given p be a prime in R. A primary module is a module whose order is a power of p.*

Theorem 2 *(The Primary Decomposition Theorem)*[11] *Given a torsion module M over a PID R with order $\mu = p_1^{e_1} ... p_n^{e_n}$, where the $p_i's$ are distinct nonassociate primes in R. Then $M = M_{p_1} \oplus ... \oplus M_{p_n}$, where $M_{p_i} = \{v \in M | p_i^{e_i} v = 0\}$ is a primary submodule of order $p_i^{e_i}$. This decomposition of M into primary submodules is called the primary decomposition of M.*

II. RESULTS

This section will be initiated by defining primary submodules of $\mathbb{Z}_n$ over $\mathbb{Z}$ and showing the submodules are indecomposable.

Definition 1 *Given $\mathbb{Z}_n$ be $\mathbb{Z}$-module where $n = p_1^{k_1} p_2^{k_2} ... p_l^{k_l}$. A primary submodule of $\mathbb{Z}_n$ is defined as $S_{p_i} = \{v \in \mathbb{Z}_n | p_i^{k_i} v = 0\}$ for $i = 1, .., l$.*

Now, we will find a generator of every primary submodule of $\mathbb{Z}_n$.

Theorem 1 *Given $\mathbb{Z}_n$ be $\mathbb{Z}$-module where $n = p_1^{k_1}p_2^{k_2}...p_l^{k_l}$. Then for $i = 1, ..., l$, the primary submodule $S_{p_i} = \langle\overline{\prod_{j\neq i} p_j^{k_j}}\rangle$.*

Proof. Let $v_i = \prod_{j\neq i} p_j^{k_j}$ where $i, j = 1, ..., l$. For any $\overline{w} \in S_{p_i}$ with $o(\overline{w}) = p_i^t$ for $t \leq k_i$, we have $p_i^t\overline{w} = \overline{0} = kn = kp_i^tp_i^{k_i-t}\prod_{j\neq i} p_j^{k_j}$ for some $k \in \mathbb{Z}$. Thus $p_i^t(w - kp_i^{k_i-t}v_i) = 0$ which implies $w = kp_i^{k_i-t}v_i$. Therefore $\overline{w} \in \langle\overline{v}_i\rangle$. □

Before finding the decomposition of $\mathbb{Z}_n$, we will show that each of its primary submodule cannot be written as internal direct sum of smaller submodules. This is stated on the following theorem.

Theorem 2 *For any $i = 1, ..., l$, S_{p_i} is indecomposable.*

Proof. For any $i = 1, ..., n$, let N_1 and N_2 be two non zero submodules of S_{p_i} with order $p_i^{e_1}$ and $p_i^{e_2}$, respectively. Suppose $e_1 < e_2 < k_i$, then $N_1 = \langle\overline{\prod_{j\neq i} p_j^{k_j}p_i^{k_i-e_1}}\rangle$ and $N_2 = \langle\overline{\prod_{j\neq i} p_j^{k_j}p_i^{k_i-e_2}}\rangle$. Notice that $k_i-e_1 > k_i-e_2$ or $e_2-e_1 > 0$. Hence, we can write $\overline{\prod_{j\neq i} p_j^{k_j}p_i^{k_i-e_1}} = \overline{\prod_{j\neq i} p_j^{k_j}p_i^{k_i-e_2}p_i^{e_2-e_1}}$. Consequently, if $v \in N_1$ then $v \in N_2$. Thus, $N_1 \subseteq N_2$. This implies that $N_1 \cap N_2 = N_1 \neq \{\overline{0}\}$. Therefore, S_{p_i} is indecomposable. □

Theorem 2 tells us that each primary submodule of $\mathbb{Z}_n$ can not be expressed as a sum of cyclic submodules. As a result, the least cyclic decomposition of $\mathbb{Z}_n$ can be written as follows.

Corollary 1 *Given $\mathbb{Z}_n$ be $\mathbb{Z}$-module where $n = p_1^{k_1}p_2^{k_2}...p_l^{k_l}$. Then $\mathbb{Z}_n = \bigoplus_{i=1}^{l}\langle\overline{\prod_{j\neq i} p_j^{k_j}}\rangle$ is the least cyclic decomposition of $\mathbb{Z}_n$.*

Now, consider $M_{m\times r}(\mathbb{Z}_n)$ as a module over $\mathbb{Z}$ (the scalar multiplication is defined by scalar multiplication with matrix). Then the following definition and theorem give the decomposition of $M_{m\times r}(\mathbb{Z}_n)$ using the decomposition of $\mathbb{Z}_n$.

Definition 2 *Given $M_{m\times r}(\mathbb{Z}_n)$ be a module over $\mathbb{Z}$ where $n = p_1^{k_1}p_2^{k_2}...p_l^{k_l}$. An $m \times r$ matrix $N_{tu}^i \in M_{m\times r}(\mathbb{Z}_n)$ is defined as $N_{tu}^i = (a_{rs})$ where $a_{rs} = \overline{\prod_{j\neq i}^{l} p_j^{k_j}}$ if $r = t, s = u$ where $i = 1, ..., l$, $t = 1, 2, ..., m$, $u = 1, ..., r$, and 0 otherwise.*

Theorem 3 *Let $n = p_1^{k_1}p_2^{k_2}...p_l^{k_l}$. Then a module $M_{m\times r}(\mathbb{Z}_n)$ over $\mathbb{Z}$ can be written as $M_{m\times r}(\mathbb{Z}_n) = \bigoplus_{t\in A,u\in B}\bigoplus_{i=1}^{l} N_{tu}^i\mathbb{Z}$ where $A = \{1, 2, ..., m\}$ and $B = \{1, 2, ..., r\}$.*

Proof. Let $C = (c_{tu}) = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1_r} \\ c_{21} & c_{22} & \cdots & c_{2_r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mr} \end{bmatrix} \in M_{m\times r}(\mathbb{Z}_n)$. Let for $t = 1, ..., m, u = 1, ..., r$, C_{tu} be a matrix obtained from C with the tu-th entry is c_{tu} and 0 otherwise. Then $C = \sum_{t\in A,u\in B} C_{tu}$. However, every $c_{tu} = \sum_{i=1}^{l}\alpha_{tui}(\overline{\prod_{j\neq i} p_j^{k_j}})$ which implies $C_{tu} = \sum_{i=1}^{l}\alpha_{tui}N_{tu}^i$.

Hence, we have $C = \sum_{t\in A,u\in B}(\sum_{i=1}^{l} \alpha_{tui}N_{tu}^{i}) \in \sum_{t\in A,u\in B}\sum_{i=1}^{l} N_{tu}^{i}\mathbb{Z}$ where $A = \{1,2,...,m\}$ and $B = \{1,2,...,r\}$. Thus, we have $M_{m\times r}(\mathbb{Z}_n) = \sum_{t\in A,u\in B}\sum_{i=1}^{l} N_{tu}^{i}\mathbb{Z}$. The independence is guaranteed by Corollary 1, so we obtain $M_{m\times r}(\mathbb{Z}_n) = \bigoplus_{t\in A,u\in B}\bigoplus_{i=1}^{l} N_{tu}^{i}\mathbb{Z}$. □

The result of Theorem 3 gives us an important tool to view the external direct sum of modules of integer modulo (modulo of each prime power) such that we can study the module properties through the module $M_{m\times r}(\mathbb{Z}_n)$ over $\mathbb{Z}$. This fact is stated as the following.

Corollary 2 *Given a module $M_{m\times r}(\mathbb{Z}_n)$ over $\mathbb{Z}$ where $n = p_1^{k_1}p_2^{k_2}...p_l^{k_l}$. Then $M_{m\times r}(\mathbb{Z}_n) \approx \mathbb{Z}_{p_1^{k_1}}^{mr} \boxplus ... \boxplus \mathbb{Z}_{p_l^{k_l}}^{mr}$.*

Proof. It is clear that for each $i = 1,...,l$, $o(N_{tu}^{i}) = p_i^{k_i}$ for all $t \in A = \{1,...,m\}$ and $u \in B = \{1,...,r\}$. Hence, for each $i = 1,...,l$, $N_{tu}^{i} \approx \mathbb{Z}_{p_i^{k_i}}$ for all $t \in A$ and $u \in B$. Therefore, by Theorem 3 we have $M_{m\times r}(\mathbb{Z}_n) = \bigoplus_{t\in A,u\in B}\bigoplus_{i=1}^{l} N_{tu}^{i}\mathbb{Z} \approx \mathbb{Z}_{p_1^{k_1}}^{mr} \boxplus ... \boxplus \mathbb{Z}_{p_l^{k_l}}^{mr}$. □

III. CONCLUSIONS AND FUTURE RESEARCH DIRECTION

Based on the result, it can be concluded that a cyclic decomposition of module $M_{m\times r}(\mathbb{Z}_n)$ over $\mathbb{Z}$ can be obtained from that of $\mathbb{Z}$-module $\mathbb{Z}_n$ in which each of the summand is generated by the product of several primes appearing in the factorization of n. For future research, we will study the form of prime submodules, weakly prime submodules, and almost prime submodules of $\mathbb{Z}_{p_1^{k_1}}^{mr} \boxplus ... \boxplus \mathbb{Z}_{p_l^{k_l}}^{mr}$ through the module $M_{m\times r}(\mathbb{Z}_n)$ over $\mathbb{Z}$.

REFERENCES

[1] I. G. A. W. Wardhana, "The Decomposition of a Finitely Generated Module over Some Special Ring," *Jurnal Teori dan Aplikasi Matematika*, vol. 6, no. 2, pp. 261—267, 2022.

[2] I. G. A. W. Wardhana, F. Maulana, "Sebuah Karakteristik dari Modul Uniserial dan Gelanggang Uniserial," *Unisda Journal of Mathematics and Computer Science (UJMC)*, vol. 7, no. 2, pp. 9—18, 2021.

[3] I. G. A. W. Wardhana, N.D.H. Ngiem, N.W. Switrayni, Q. Aini, "A Note on Almost Prime Submodule of CSM Module over Principal Ideal Domain," *In Journal of Physics: Conference Series*, vol. 2106, no. 1, pp. 012011, 2021.

[4] I. G. A. W. Wardhana, P. Astuti, I. M. Alamsyah, "On Almost Prime Submodules of a Module over a Principal Ideal Domain," *JP Journal of Algebra, Number Theory and Applications*, vol. 38, no. 2, pp. 121—128, 2016.

[5] W. U. Misuki, I. G. A. W. Wardhana, N. W. Switrayni, " Some Characteristics of Prime Cyclic Ideal On Gaussian Integer Ring Modulo," *In IOP Conference Series: Materials Science and Engineering*, vol. 1115, no. 1, pp. 012084, 2021.

[6] R. Juliana, I. G. A.W. Wardhana, Irwansyah, "Some Characteristics of Cyclic Prime, Weakly Prime and Almost Prime Submodule of Gaussian Integer Modulo over Integer," *In AIP Conference Proceedings*, vol. 2329, no. 1, pp. 020004, 2021.

[7] I. G. A. W. Wardhana, N. W. Switrayni, Q. Aini, "Submodul Prima Lemah dan Submodul Hampir Prima Pada $\mathbb{Z}$-Modul $M_{2\times 2}(\mathbb{Z}_9)$," *Eigen Mathematics Journal*, vol. 1, no. 1, pp. 28—30, 2018.

[8] I. G. A. W. Wardhana, N. W. Switrayni, Q. Aini, "Submodul Prima, Submodul Prima Lemah dan Submodul Hampir Prima Pada $\mathbb{Z}$-Modul $M_{2\times 2}(\mathbb{Z}_n)$," *Proceeding of Konferensi Nasional Matematika XIX, Indonesian Mathematical Society*, ISBN: 978-623-94020-0-6, pp. 85—89, 2018.

[9] P. E. Bland, *Rings and Their Modules*. Berlin: De Gruyter, 2011.

[10] D. S. Passman, *A Course in Ring Theory*. USA: AMS Chelsea Publishing, 2004.

[11] S. Roman, *Advanced Linear Algebra, Third Edition*. New York: Springer, 2008.