Prime ideal on the endomorphism ring of $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$

Zakaria Bani Ikhtiyar*, Nikken Prima Puspita1, Titi Udjiani1

1 Departement of Mathematics, Universitas Diponegoro, Semarang, Indonesia.
✉ zakaria.bani45@gmail.com

Abstract
The set of all endomorphisms over $R$-module $M$ is a non-empty set denoted by $\text{End}_R(M)$. From $\text{End}_R(M)$, we can construct the ring of $\text{End}_R(M)$ over addition and composition function. The prime ideal is an ideal that satisfies the properties like prime numbers. In this paper, we take the ring of integer number $\mathbb{Z}$ and the module of $\mathbb{Z}^n$ over $\mathbb{Z}$ such that the $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ is a ring. Furthermore, we show the existence of the prime ideal on the $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$. We also applied a prime ideal property to prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$.

INTRODUCTION
A module over a ring is a generalization structure of a vector space over a field (Matlis, 1968; Nobusawa, 1964; Wahyuni et al., 2016). A vector space requires a commutative group and a field. In module theory, a field can be replaced with any ring with unity (Marks, 2002; Volodin, 1971; Jensen & Lenzing, 1989). Furthermore, the concept of a linear transformation is known in a vector space. This concept is also implemented in modules called module homomorphism.

Let $M$ and $N$ be modules over a ring $R$. If $f: M \to N$ is a module homomorphism in which $M = N$, then we call $f$ a module endomorphism (Nicholson, 1976). Here we collect all of the endomorphisms in a module $M$ over ring $R$ such that we have the set of endomorphisms $M$ over $R$ denoted by $\text{End}_R(M)$ (Lindo, 2017). The endomorphism set is non-empty because at least there is the identity function as an element of $\text{End}_R(M)$. Therefore, based on ring theory in Herstein (1975), by adding two binary operations, i.e., addition and composition function, we constructed a ring called an endomorphism ring, denoted by $(\text{End}_R(M), +, \circ)$.

In a ring $R$, a non-empty set $I \subseteq R$ that satisfies the axioms of the ring and $r, i \in I$ for all $r \in R$ and $i \in I$ is called ideal (Davvas, 2006; Jianming & Xueling, 2004). Furthermore, the special ideal was defined by Dedekind in 1871 based on the properties of prime numbers. The concept of the prime ideal is known (Kleiner, 1998). Moreover, the prime ideal was discussed by Khariani et al. (2014), Maulana et al. (2019), and Khairunnisa and Wardhana (2019). In this paper, we have a special ring, i.e., the endomorphism ring $(\text{End}_R(M), +, \circ)$ where $M = \mathbb{Z}^n$ and $R = \mathbb{Z}$. This research shows the existence of a prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$. We also applied a characteristic of prime ideal for the prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$. Here we start our discussion about the prime ideal by giving the fundamental theories of a module over a ring.

Definition 1. (Wahyuni et al., 2016) Let $(R, +, \cdot)$ be a ring with unity, $(M, +)$ a commutative group, and the scalar operation $\ast : R \times M \to M$. A group $M$ is a left $R$-module if satisfy the following conditions:

i. $r_1 \ast (m_1 + m_2) = r_1 \ast m_1 + r_1 \ast m_2$, 

How to cite

Published by
Mathematics Education Department, UIN Raden Intan Lampung.
ii. \((r_1 + r_2) \ast m_1 = r_1 \ast m_1 + r_2 \ast m_1\).

iii. \((r_1 \cdot r_2) \ast m_1 = r_1 \ast (r_2 \ast m_1)\),

iv. \(1_R \ast m_1 = m_1\).

Furthermore, the group \(M\) is the right \(R\)-module if satisfy the following conditions:

i. \((m_1 + m_2) \ast r_1 = m_1 \ast r_1 + m_2 \ast r_1\),

ii. \(m_1 \ast (r_1 + r_2) = m_1 \ast r_1 + m_1 \ast r_2\),

iii. \(m_1 \ast (r_1 \cdot r_2) = (m_1 \ast r_1) \ast r_2\),

iv. \(m_1 \ast 1_R = m_1\),

for all \(r_1, r_2 \in R\) and \(m_1, m_2 \in M\). Furthermore, group \(M\) is called an \(R\)-module if it is both a left and right \(R\)-module. A group \(M\), as a module over a ring \(R\), can be written by \(R\)-module \(M\).

Example 2. Let \(\mathbb{Z}\) be a ring with unity. \(\mathbb{Z}^n = \{(a_1, a_2, a_3, ..., a_n) | a_i \in \mathbb{Z}, i = 1, 2, 3, ..., n\}\) be a commutative group with a scalar operation \(\cdot : \mathbb{Z} \times \mathbb{Z}^n \rightarrow \mathbb{Z}^n\). Group \(\mathbb{Z}^n\) is a module over \(\mathbb{Z}\).

Let \(M, N\) be modules over \(R\). We can construct a relation between both of them, and we called it a module homomorphism as follows:

Definition 3. (Dummit and Foote, 2004) Let \((M, +_M), (N, +_N)\) be modules over ring \(R\) with scalar \(*_M\) and \(*_N\), respectively. Map \(f: M \rightarrow N\) is called \(R\)-module homomorphism if satisfy:

i. \(f(m_1 +_M m_2) = f(m_1) +_N f(m_2)\), and

ii. \(f(r \ast_M m_1) = r \ast_N f(m_1)\).

for all \(r \in R\) and \(m_1, m_2 \in M\).

Example 4. Let \((\mathbb{Z}, +)\) and \((\mathbb{Z}^n, +_1)\) be modules over \(\mathbb{Z}\) with the scalar operation \(\cdot\) and \(\cdot_1\), respectively, and \(+_1\) is an addition between two vectors in \(\mathbb{Z}^n\). Defined \(f: 2\mathbb{Z} \rightarrow \mathbb{Z}^n\) by \(f(2n) = [2n, 4n, 6n, ..., 2n^2]^T\) for any \(2n \in 2\mathbb{Z}\) and \([2n, 4n, 6n, ..., 2n^2]^T \in \mathbb{Z}^n\). Based on Definition 3, we have that for any \(2n, 2m \in 2\mathbb{Z}\), and \(k \in \mathbb{Z}\), this is satisfy:

i. \(f(2n + 2m) = f(2n) +_1 f(2m)\), and

ii. \(f(k \cdot 2n) = k \cdot_1 f(2n)\).

By this fact, we have that \(f\) is a homomorphism \(\mathbb{Z}\)-module.

In Definition 3, when \(M = N\), we can call \(f\) an \(R\)-module \(M\) endomorphism. We can collect all \(R\)-module \(M\) endomorphisms in a set denoted by \(\text{End}_R(M)\). This paper will have some properties of the set of all \(\mathbb{Z}\)-module \(\mathbb{Z}^n\) endomorphisms. According to the \(\text{End}_\mathbb{Z}(\mathbb{Z}^n)\), we have the trivial example when we define \(\vartheta: \mathbb{Z}^n \rightarrow \mathbb{Z}^n\), i.e., \(\vartheta([x_1, x_2, x_3, ..., x_n]^T) = [0, 0, 0, ..., 0]^T\) with \(\vartheta \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)\).

For studying this paper, we need to know about the definition of ideal and ideal, which is generated by an element as follows:

Definition 5. (Adkins & Weintraub, 1992) Let \(R\) be a ring and a non-empty set \(I \subseteq R\). The set \(I\) called a left ideal on \(R\) if it satisfies the following conditions:

i. \(i_1 - i_2 \in I\), and

ii. \(ri_1 \in I\).

Furthermore, \(I\) is called a right ideal on \(R\) if it satisfies the following conditions:
i. \( i_1 - i_2 \in I \)

ii. \( i_1 r \in I \)

for all \( r \in R \) and \( i_1, i_2 \in M \). The set \( I \) is called an ideal on \( R \) if it is both a left and a right ideal on \( R \). For all \( I \neq R \), then \( I \) is called a proper ideal on \( R \). Furthermore, for an ideal whose elements are only zero elements, it is called a zero ideal, denoted by \( 0 \).

**Definition 6.** *(Gallian, 2017)* Let \( R \) be a ring and \( a \in R \). A denoted by \( aL = ra \mid r \in R \) generates the left ideal on \( \langle a \rangle \) \( \{ R \} \), and the right one on \( R \) is generated by \( a \langle a \rangle_R = \{ ar \mid r \in R \} \). If \( \langle a \rangle_L = \langle a \rangle_R \), then \( \langle a \rangle \) is a notation for the ideal on \( R \) generated by \( a \).

Based on Definition 6, we have the following example.

**Example 7.** Let \( \mathbb{Z} \) be a ring and \( 2 \in \mathbb{Z} \). We have \( 2\mathbb{Z} = \{ 2n \mid n \in \mathbb{Z} \} \) as an ideal on \( \mathbb{Z} \) generated by \( 2 \), denoted by \( \langle 2 \rangle \).

The property of prime number can be applied for ideal such that we have the following definition.

**Definition 8.** *(McCoy, 1949)* Let \( R \) be a ring and \( P \) proper ideal on \( R \). Ideal \( P \) is called prime ideal on \( R \), if for all \( a, b \in R \), with \( aRb \subseteq P \), then \( a \in P \) or \( b \in P \).

**Example 9.** Let \( \mathbb{Z} \) be a ring, and \( 2\mathbb{Z} \) proper ideal on \( \mathbb{Z} \). Ideal \( 2\mathbb{Z} \) is prime ideal on \( \mathbb{Z} \) since, for all \( a, b \in \mathbb{Z} \) with \( a\mathbb{Z}b \subseteq 2\mathbb{Z} \) always results in \( a \in 2\mathbb{Z} \) or \( b \in 2\mathbb{Z} \).

In addition to defining the prime ideal, McCoy (1949), in his article, gave the following lemma relating to the prime ideal.

**Lemma 10.** *(McCoy, 1949)* If \( I \) an ideal on \( R \) and \( P \) is a prime ideal on \( R \), then \( I \cap P \) is the prime ideal on \( I \).

**METHODS**

To investigate this project, we need to survey relevant topics. The initial step is studying the concept of the prime ideal in the work of McCoy (1975) and Wahyuni et al. (2016). Next, we study the application of the prime ideal in particular rings of previous research by Khariani et al. (2014), Maulana et al. (2019), and Khairunnisa and Wardhana (2019). Then we analyze the module structure, module homomorphism, module endomorphism, and the endomorphism of ring \( \text{End}_R(M) \). This paper determined and chose \( R = \mathbb{Z} \) and \( M = \mathbb{Z}^n \). The last step is giving an example of a prime ideal in \( \text{End}_\mathbb{Z}(\mathbb{Z}^n) \) and a prime ideal property that apply to it.

**RESULTS AND DISCUSSION**

The set \( \text{End}_\mathbb{Z}(\mathbb{Z}^n) = \{ f: \mathbb{Z}^n \to \mathbb{Z}^n \mid f \text{ is a } \mathbb{Z} - \text{ module homomorphism} \} \). For every \( [a_1 a_2 a_3 ... a_n]^T, [b_1 b_2 b_3 ... b_n]^T \in \mathbb{Z}^n, f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n) \) can be written as \( f([a_1 a_2 a_3 ... a_n]^T) = [b_1 b_2 b_3 ... b_n]^T \). Because the codomain entries are integers, the Greatest Common Divisor (GCD) can be found. For example, if the GCD of each entry in the codomain is \( k \), that is \( (b_1, b_2, b_3, ..., b_n) = k \), then the function \( f \) can be written as \( f([a_1 a_2 a_3 ... a_n]^T) = k[c_1 c_2 c_3 ... c_n]^T \) with \( c_i = \frac{b_i}{k}, i = 1, 2, 3, ..., n \) and \( [c_1 c_2 c_3 ... c_n]^T \in \mathbb{Z}^n \). With this fact, we have the following proposition.
Proposition 11. Given set $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ and $f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$ with $f([a_1 a_2 a_3 \ldots a_n]^T) = [b_1 b_2 b_3 \ldots b_n]^T$. Element $f$ can be written as $f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 c_2 c_3 \ldots c_n]^T$ with $c_i = \frac{b_i}{k}$, $i = 1, 2, 3, \ldots, n$ and $k = (b_1 b_2 b_3 \ldots b_n)$.

For $f, g \in \text{End}_\mathbb{Z}(\mathbb{Z})$ with $f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 c_2 c_3 \ldots c_n]^T$ and $g([a_1 a_2 a_3 \ldots a_n]^T) = l[d_1 d_2 d_3 \ldots d_n]^T$, we define that $(f \circ g)([a_1 a_2 a_3 \ldots a_n]^T) = kl[m_1 m_2 m_3 \ldots m_n]^T$.

It was known that $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ is a non-empty set. Based on ring theory by Gallian (2017) an Koh (1971), the set $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ with the binary operation addition $"+"$ and composition $"\circ"$ function can generate a ring called the endomorphism ring of $\mathbb{Z}$-module $\mathbb{Z}^n$, denoted by the endomorphism ring of $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$. Therefore based on Definition 6., an ideal in the ring $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$, which is generated by $f$, can be formed as follows.

Example 12. Given ring $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ and $f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$, with $f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 c_2 c_3 \ldots c_n]^T$. The right ideal generated by $f$, i.e.

$\langle f \rangle_R = \{f \circ g | g \in \text{End}_\mathbb{Z}(\mathbb{Z}^n), g([a_1 a_2 a_3 \ldots a_n]^T) = l[x_1 x_2 x_3 \ldots x_n]^T\}$

$= \{h | h([a_1 a_2 a_3 \ldots a_n]^T) = kl[d_1 d_2 d_3 \ldots d_n]^T\}.$

Based on Example 12., the prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ is explained in the following proposition.

Proposition 13. Given the ring $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$, $f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$, with $f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 c_2 c_3 \ldots c_n]^T$. If $k$ is a prime number, then

$\langle f \rangle_R = \{f \circ g | g \in \text{End}_\mathbb{Z}(\mathbb{Z}^n), g([a_1 a_2 a_3 \ldots a_n]^T) = l[x_1 x_2 x_3 \ldots x_n]^T\}$

$= \{h | h([a_1 a_2 a_3 \ldots a_n]^T) = kl[d_1 d_2 d_3 \ldots d_n]^T\}.$

Is prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$.

Proof:
We have $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$, $f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$, with $f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 c_2 c_3 \ldots c_n]^T$. It will be shown that if $k$ is the prime number, then $\langle f \rangle_R$ is the prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$.

Taken $\theta, \gamma \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$ with $\theta([a_1 a_2 a_3 \ldots a_n]^T) = r[x_1 x_2 x_3 \ldots x_n]^T$, $\gamma([a_1 a_2 a_3 \ldots a_n]^T) = s[y_1 y_2 y_3 \ldots y_n]^T$, and $\theta \circ \text{End}_\mathbb{Z}(\mathbb{Z}^n) \circ \gamma \subseteq \langle f \rangle_R$. Since $\circ \circ$ it is a competition function, we get

$\text{End}_\mathbb{Z}(\mathbb{Z}^n) \circ \gamma = \{g \circ \gamma | g \in \text{End}_\mathbb{Z}(\mathbb{Z}^n), g([a_1 a_2 a_3 \ldots a_n]^T) = l[m_1 m_2 m_3 \ldots m_n]^T\}$

$= \{\omega | \omega([a_1 a_2 a_3 \ldots a_n]^T) = ls[d_1 d_2 d_3 \ldots d_n]^T\}.$

Next, we have

$\theta \circ \text{End}_\mathbb{Z}(\mathbb{Z}^n) \circ \gamma = \{\theta \circ g \circ \gamma | g \in \text{End}_\mathbb{Z}(\mathbb{Z}^n), g([a_1 a_2 a_3 \ldots a_n]^T) \}$

$= \{l[m_1 m_2 m_3 \ldots m_n]^T\}$

$= \{l[m_1 m_2 m_3 \ldots m_n]^T\}.$

Since $\theta \circ \text{End}_\mathbb{Z}(\mathbb{Z}^n) \circ \gamma \subseteq \langle f \rangle_R$, then $rls$ is a multiple of $k$, in other words, $rls = km$, with $m \in \mathbb{N}$. Since $s$ is the $\text{GCD}$ of the codomain entries of any function $f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$, then $s$ is not always a prime number, so it is not always a multiple of $k$. Since $k$ is prime, this results in
$r = vk$ or $s = vk$ for some $v \in N$. This means $\theta \in \langle f \rangle_R$ or $\gamma \in \langle f \rangle_R$. Based on Definition 8, $\langle f \rangle_R$ is a prime ideal in $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$.

Before being given prime ideal property on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$, additional conditions will be given to Lemma 10. In Lemma 10, no special conditions are given for ideal $I$ and prime ideal $P$. This condition has the possibility that $I \cap P = I$. Consequently, there is the possibility that the ideal $I \cap P$ is not a proper ideal in $I$. This means that the condition of a prime ideal based on Definition 8, which must be a proper ideal, is not satisfied. Therefore, given the following lemma to complete Lemma 10.

**Proposition 14.** If $I$ ideal on $R$, $P$ prime ideal on $R$, and $I \nsubseteq P$, then $I \cap P$ prime ideal on $I$.

**Proof:**
We have the $I$ ideal on $R$, $P$ prime ideal on $R$, and $I \nsubseteq P$. It will be shown that the $I \cap P$ prime ideal on $I$.

First, it is necessary to show that $I \cap P$ is ideal in $I$. Take any $a, b \in I \cap P$, and $r \in I$. This means $a, b \in I$, and $a, b \in P$. Since $I$ and $P$ are ideal in $R$, then $-b \in I$ and $-b \in P$, so $a - b \in I$ and $a - b \in P$. This shows that $a - b \in I \cap P$. Furthermore, because $I$ is ideal, then $ra \in I$ or $ar \in I$. So it is proven that $I \cap P$ is left and right ideal in $I$. Since $I \nsubseteq P$, then $I \cap P$ is a proper ideal in $I$. To show that $I \cap P$ prime ideal in $I$, take any $a, b \in I$ with $a \neq b \subseteq I \cap P$. It will be shown that $a \in I \cap P$ or $b \in I \cap P$.

Therefore $a \neq b \subseteq I \cap P$, then $a \neq b \subseteq P$. Therefore $a \neq b \subseteq P$. Since $P$ is a prime ideal, then $aR \subseteq P$ or $bR \subseteq P$. If $aR \subseteq P$, then $aR \subseteq P$, since $P$ is a prime ideal, then $a \in P$. This also applies if $bR \subseteq P$, then $b \in P$. Therefore it means $a \in I \cap P$ or $b \in I \cap P$. So that $I \cap P$ is the prime ideal of $I$.

Furthermore, based on Proposition 14, we claim the following proposition as the prime ideal property on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$.

**Proposition 15.** Given ring $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$, $f_1, f_2 \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$ with $f_1([a_1 a_2 a_3 \ldots a_n]^T) = k_1[c_1 \ c_2 \ c_3 \ldots c_n]^T$, $f_2([a_1 a_2 a_3 \ldots a_n]^T) = k_2[c_1 \ c_2 \ c_3 \ldots c_n]^T$,

\[
I = \langle f_1 \rangle_{R_1} = \{ f \circ g | g \in \text{End}_\mathbb{Z}(\mathbb{Z}^n), g([a_1 a_2 a_3 \ldots a_n]^T) = r[x_1 x_2 x_3 \ldots x_n]^T \}
\]

\[
= \{ h \circ h([a_1 a_2 a_3 \ldots a_n]^T) = k_1r[b_1 b_2 b_3 \ldots b_n]^T \}, \text{ and }
\]

\[
P = \langle f_2 \rangle_{R_2} = \{ f \circ g | g \in \text{End}_\mathbb{Z}(\mathbb{Z}^n), g([a_1 a_2 a_3 \ldots a_n]^T) = s[x_1 x_2 x_3 \ldots x_n]^T \}
\]

\[
= \{ h \circ h([a_1 a_2 a_3 \ldots a_n]^T) = k_2s[b_1 b_2 b_3 \ldots b_n]^T \}.
\]

For all $k_1$ composite numbers, $k_2$ prime numbers, and $k$ not multiples of $k_2$, then $I \cap P$ is prime ideal on $I$.

**Proof:**
Based on Proposition 13., we have that $I$ is ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$, but not prime ideal since $k_1$ is a composite number, and $P$ is prime ideal on $\text{End}_\mathbb{Z}(\mathbb{Z}^n)$ since $k_2$ is a prime number. Furthermore, since $r \neq ms$ for $m \in \mathbb{N}$, then $I \nsubseteq P$. So, based on Lemma 13., $I \cap P$ is a prime ideal in $I$.

**CONCLUSIONS**
The right ideal constructed by any $f \in \text{End}_\mathbb{Z}(\mathbb{Z}^n)$ where $f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 \ c_2 \ c_3 \ldots c_n]^T$, i.e., $\langle f \rangle_R$, is a prime ideal if $k$ prime. If $k$ is a composite number, then $\langle f \rangle_R$
is not a prime ideal. Furthermore, the condition for an intersection between an ideal and a prime ideal in a ring holds that the intersection is a prime ideal in an ideal. It must be an ideal constituent set, not a subset of a prime ideal forming set. The last result is that the intersection between the ideals formed by \( f_1([a_1 a_2 a_3 \ldots a_n]^T) = k_1[c_1 c_2 c_3 \ldots c_n]^T \) and \( f_2([a_1 a_2 a_3 \ldots a_n]^T) = k_2[c_1 c_2 c_3 \ldots c_n]^T \) with \( k_1 \) composite numbers and \( k_2 \) prime, is a prime ideal on the constructed ideal \( f_1([a_1 a_2 a_3 \ldots a_n]^T) = k_1[c_1 c_2 c_3 \ldots c_n]^T \).

For extension of our research, we can change \( f([a_1 a_2 a_3 \ldots a_n]^T) = k[c_1 c_2 c_3 \ldots c_n]^T \) by \( f \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} k & 0 & 0 & \cdots & 0 \\ 0 & k & 0 & \cdots & 0 \\ 0 & 0 & k & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & k \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{pmatrix} \). Then the properties of the diagonal matrix can be used to examine other properties of the ring \( \text{End}_n(\mathbb{Z}) \) and the prime ideal in that ring.

**AUTHOR CONTRIBUTIONS STATEMENT**

ZBI designs research and writing script. NPP conducts project investigations and contribute to interpretation results. TU designed the study and reviewed it script. All authors read and approve the final manuscript.

**REFERENCES**


