Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 97-101
https://idjams.com/index.php/jms/index

Necessary and Sufficient Conditions for a Finite Cyclic Group to be a Cyclic Module

Arya Raditya Cahyadi[1], Sisilia Sylviani[2, *], Mary Gyenin[3]

[1, 2] *Universitas Padjadjaran, Jl. Soekarno Km 21 Jatinangor, Kab. Sumedang, West Java 45363, Indonesia*

[3] *Department of Mathematics Education, Akenten Appiah Menka University of Skills Training and Entrepreneurial Development, Kumasi, Ghana*

[*]*Corresponding author: sisilia.sylviani@unpad.ac.id*

Copyright: ©2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License-(CC-BY-SA) (https://creativecommons.org/licenses/by-sa/4.0/)

Article Info

Article history:
Received: May 7, 2025
Revised: September 22, 2025
Accepted: September 23, 2025
Available online: October 22, 2025

DOI:
https://doi.org/10.71385/idjams.v2i2.28

Abstract

The structures of cyclic groups and cyclic modules are fundamental topics in abstract algebra. While their individual structures are well-established, the precise conditions that link them over an arbitrary ring R are often not detailed in the literature. This paper aims to find the necessary and sufficient conditions for a finite cyclic group G of order n to be a cyclic R-module for an arbitrary ring R. The method used in this research is by utilizing the fundamental theorem stating a relationship between an abelian group viewed as a $\mathbb{Z}$-module and a ring homomorphism from R to the ring of endomorphism of its group, which is isomorphic to $\mathbb{Z}_n$. The result of this research is a theorem proving that a finite cyclic group G of order n can be endowed with the structure of a cyclic R-module if and only if there exists a surjective ring homomorphism from R to $\mathbb{Z}_n$ (the ring of integers modulo n). This finding establishes a clear connection between these algebraic structures.

Keywords: Cyclic Group; Cyclic Module; Ring Homomorphism; Endomorphism Ring; Module Theory.

I. Introduction

The origin of group theory is from the theory of equations. Évariste Galois worked on permutation groups, which Arthur Cayley then formulated into the abstract group so it could be applied more broadly [1-3]. Unlike group theory, which came from a single problem, ring theory originated from the theory of algebraic number fields, the theory of algebraic functions, the theory of polynomial forms, the theory of quaternions and hypercomplex numbers, and others. It was Emmy Noether who unified these different theories [4-5]. Modules, on the other hand, emerge as a generalization of vector spaces by using an arbitrary ring R with identity rather than a field [6-8]. Formally, R-modules are abelian groups endowed with an action of R [9-10].

A group is defined as cyclic if it is generated by a single element [11]. Each finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ (the additive group of integers modulo n) [12-14]. In module theory, a cyclic module is also generated by one element m such that $M = Rm = \{rm \mid r \in R\}$ [15]. It is also known that cyclic modules are isomorphic to a quotient module R/I for some left ideal I of the ring R [16].

It is well known that an abelian group is a module over the ring of integers $\mathbb{Z}$ [17-18]. Since a finite cyclic group is abelian, it is a $\mathbb{Z}$-module. However, the conditions for an arbitrary ring R are less commonly known. This paper examines this specific problem by asking a question: When does a finite cyclic group of order n become a cyclic module over an arbitrary ring R? To answer this question, we will utilize a theorem that states an abelian group M can be viewed as a module over a ring R if and only if there exists a ring homomorphism $\phi : R \to \mathrm{End}_{\mathbb{Z}}(M)$, where $\mathrm{End}_{\mathbb{Z}}(M)$ is the ring of endomorphisms

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 97-101
https://idjams.com/index.php/jms/index

of M [19]. Furthermore, to solve the problem, we will use the fact that the ring of endomorphisms $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$ is isomorphic to the ring $\mathbb{Z}_n$ for a finite cyclic group $G \cong \mathbb{Z}_n$ [20].

This paper's objective is to prove that a finite cyclic group G of order n can be endowed with the structure of a cyclic R-module if and only if there exists a surjective ring homomorphism from R to $\mathbb{Z}_n$ (the ring of integers modulo n). This theorem establishes the connection between finite cyclic groups, rings, and cyclic modules. Thus, it can be a foundation for advanced module theory.

II. Preliminaries

To prove our main theorem, we will utilize two fundamental theorem. First, an abelian group M can be viewed as a module over a ring R if and only if there exists a ring homomorphism $\phi : R \to \mathrm{End}_{\mathbb{Z}}(M)$, where $\mathrm{End}_{\mathbb{Z}}(M)$ is the ring of endomorphisms of M. Second, for a cyclic group $\mathbb{Z}_n$, a ring of endomorphisms $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$ is isomorphic to the ring $\mathbb{Z}_n$.
For clarity, we state the following key definitions.

Definition 1. [15] A group H is cyclic if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication). In additive notation H is cyclic if $H = \{nx \mid n \in \mathbb{Z}\}$.

In both cases we shall write $H = \langle x \rangle$ and say H is generated by x (x is a generator of H).

Example 1. $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ under addition mod 5 is a cyclic group generated by $[1]$, $\mathbb{Z}_5 = \langle [1] \rangle$.

Definition 2. [15] Let M be an R-module. A submodule N of M (possibly $N = M$) is cyclic if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element:

$$N = Ra = \{ra \mid r \in R\}$$

Example 2. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, then M is a cyclic $\mathbb{Z}$-module. We can see that $[1]$ generates M because $M = \mathbb{Z} \cdot [1] = \{n \cdot [1] \mid n \in \mathbb{Z}\} = \{[0], [1], [2], [3], [4]\}$.

Definition 3. [15] Let R and S be rings. A map $\varphi : R \to S$ is called ring homomorphism if:
(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$.
(2) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Definition 4. [15] Let M and N be R-modules. Define $\mathrm{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M into N. $\mathrm{Hom}_R(M, M)$ is called the endomorphism ring of M and will denoted by $\mathrm{End}_R(M)$.

Lemma 1. [20] The ring of endomorphisms of the group $\mathbb{Z}_n$, denoted $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$, is isomorphic as a ring to $\mathbb{Z}_n$.

Proof.

Let $f \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$. Because $\mathbb{Z}_n$ is a cyclic group generated by $[1]$, then every $[x] \in \mathbb{Z}_n$ can be written as the sum of $[1]$ with itself x times. It implies that $f([x]) = f\big([1] + [1] + \cdots + [1] \ \text{(x times)}\big) = f([1]) + f([1]) + \cdots + f([1])$ (x times) $= [x]f([1])$.

Consider the map $\gamma : \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n) \to \mathbb{Z}_n$ given by $\gamma(f) = f([1])$. This mapping is a ring isomorphism because:
i) $\gamma(f + g) = (f + g)([1]) = f([1]) + g([1]) = \gamma(f) + \gamma(g)$ for all $f, g \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$.
ii) $\gamma(fg) = (fg)([1]) = f([1])g([1]) = \gamma(f)\gamma(g)$ for all $f, g \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$.
iii) γ is injective because any endomorphism on $\mathbb{Z}_n$ is uniquely determined by its value at $[1]$.

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 97-101
https://idjams.com/index.php/jms/index

iv) γ is surjective because for all $[k] \in \mathbb{Z}_n$ there exists an $f([x]) = [k][x] \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$ such that $\gamma(f) = f([1]) = [k]$.

III. Results and Discussion

This paper will show us the condition that connect a finite cyclic group and cyclic modules by proving the theorem below:

Theorem 1 Let G be a finite cyclic group of order n, and let R be a ring with a multiplicative identity. The group G can be endowed with the structure of a cyclic R-module if and only if there exists a surjective ring homomorphism from R to $\mathbb{Z}_n$ (the ring of integers modulo n).

Proof.

($\Rightarrow$) Note that any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ (the additive group of integers modulo n). Since G is a finite cyclic group of order n, without loss of generality, we consider $G = \mathbb{Z}_n$. Assume that $\mathbb{Z}_n$ can be endowed with the structure of a cyclic R-module. This means that there exists an action of R on $\mathbb{Z}_n$, which we can write as $r * [g]$ for any $r \in R$ and $[g] \in \mathbb{Z}_n$.

Considering that we have an R-module $\mathbb{Z}_n$, we know that there exists a ring homomorphism from R to the ring of endomorphisms of $\mathbb{Z}_n$, denoted $\psi : R \to \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$. Since the composition of two ring homomorphisms is also a ring homomorphism, we need to show there is a ring homomorphism (or isomorphism) from $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$ to $\mathbb{Z}_n$ to construct a ring homomorphism from R to $\mathbb{Z}_n$. By Lemma 1, we know that the ring of endomorphisms of $\mathbb{Z}_n$ is isomorphic to te ring $\mathbb{Z}_n$. Let this isomorphism be $\gamma : \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n) \to \mathbb{Z}_n$ given by $\gamma(f) = f([1])$. Since we already have $\psi : R \to \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n)$, then $\phi = \gamma \circ \psi : R \to \mathbb{Z}_n$ is a ring homomorphism from R to $\mathbb{Z}_n$. The action of R on $\mathbb{Z}_n$ now can be written as $r * [g] = \phi(r)[g]$ where $\phi(r) \in \mathbb{Z}_n$ and $\phi(r)[g]$ is a multiplication in $\mathbb{Z}_n$.

After we obtained the ring homomorphism from R to $\mathbb{Z}_n$ (which is ϕ), we need to prove that ϕ is surjective ($\mathrm{Im}(\phi) = \mathbb{Z}_n$). From the hypothesis we know that $\mathbb{Z}_n$ is a cyclic R-module. This means there is a generator $[g_0] \in \mathbb{Z}_n$ such that $\mathbb{Z}_n = R * [g_0] = \{r * [g_0] \mid r \in R\}$. By applying the previously defined action to the generator $[g_0]$, we have $\mathbb{Z}_n = \{\phi(r)[g_0] \mid r \in R\}$. This set must contain the element $[1]$, thus, there exists $s \in R$ such that $s * [g_0] = \phi(s)[g_0] = [1]$. This means $[g_0]$ must be a multiplicative unit and $\phi(s)$ must be its multiplicative inverse. Then, for an arbitrary element $[y] \in \mathbb{Z}_n$, there exists $r_{[y]} \in R$ such that $[y] = \phi(r_{[y]})[g_0]$. Since $[g_0]$ is a unit, there exists $[g_0]^{-1} \in \mathbb{Z}_n$ and we can multiply $[y]$ by $[g_0]^{-1}$ to get $[y][g_0]^{-1} = \phi(r_{[y]})$. Since multiplication by $[g_0]^{-1}$ is a permutation of the group $\mathbb{Z}_n$ (a bijective function from $\mathbb{Z}_n$ to itself), the set $\{[y][g_0]^{-1} \mid [y] \in \mathbb{Z}_n\} = \{\phi(r_{[y]}) \mid r_{[y]} \in R\}$ is equal to $\mathbb{Z}_n$. This implies $\mathrm{Im}(\phi) = \mathbb{Z}_n$.Thus, the ring homomorphism $\phi : R \to \mathbb{Z}_n$ is surjective.

($\Leftarrow$) As before, to prove this theorem we will treat G as $\mathbb{Z}_n$. Assume there exists a surjective ring homomorphism $\phi : R \to \mathbb{Z}_n$. We can define the action from R to $\mathbb{Z}_n$ as:

$$r * [g] = \phi(r)[g] \tag{1}$$

for any $r \in R$ and $[g] \in \mathbb{Z}_n$, where $\phi(r) \in \mathbb{Z}_n$ and $\phi(r)[g]$ is a multiplication in $\mathbb{Z}_n$. Then we need to prove that the action defined in equation (1) satisfies the R-module axioms.

Let $r, s \in R$ and $[x], [y] \in \mathbb{Z}_n$.

i) $r * ([x] + [y]) = r * [x] + r * [y]$

$$\begin{aligned} r * ([x] + [y]) &= \phi(r)([x] + [y]) \\ &= \phi(r)[x] + \phi(r)[y] \\ &= r * [x] + r * [y] \end{aligned}$$

ii) $(r + s) * [x] = r * [x] + s * [x]$

$(r + s) * [x] = \phi(r + s)[x]$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 97-101
https://idjams.com/index.php/jms/index

$$= \big(\phi(r) + \phi(s)\big)[x]$$
$$= \phi(r)[x] + \phi(s)[x]$$
$$= r * [x] + s * [x]$$

iii) $(rs) * [x] = r * (s * [x])$

$$(rs) * [x] = \phi(rs)[x]$$
$$= \big(\phi(r)\phi(s)\big)[x]$$
$$= \phi(r)(\phi(s)[x])$$
$$= r * (s * [x])$$

iv) $1_R * [x] = [x]$

$$1_R * [x] = \phi(1_R)[x]$$
$$= [1][x]$$
$$= [x]$$

Since all axioms are satisfied, $\mathbb{Z}_n$ is an R-module under this action.

To prove that $\mathbb{Z}_n$ is a cyclic R-module, we must find an element in $\mathbb{Z}_n$ that acts as a generator. It means we want to show there exists an element $[g_0] \in \mathbb{Z}_n$ such that $R * [g_0] = \{\phi(r)[g_0] \mid r \in R\} = \mathbb{Z}_n$. Considering the element $[1] \in \mathbb{Z}_n$, we have $R * [1] = \{\phi(r)[1] \mid r \in R\} = \{\phi(r) \mid r \in R\} = \mathrm{Im}(\phi)$. Given that ϕ is surjective, $\mathrm{Im}(\phi) = \mathbb{Z}_n$. Therefore $R * [1] = \mathbb{Z}_n$. This means $\mathbb{Z}_n$ is a cyclic R-module with $[1]$ as its generator.

■

This proof has shown that the necessary and sufficient condition for a finite cyclic group of order n to be a cyclic R-module for an arbitrary ring R is the existence of a surjective ring homomorphism from R to $\mathbb{Z}_n$. Since the theorem contains an "if and only if" statement, we work in both directions to prove it. The argument applied the fundamental theorem stating that an abelian group can be viewed as an R-module if and only if there exists a ring homomorphism from R to its endomorphism ring. It also utilized the fact that the ring of endomorphisms of $\mathbb{Z}_n$ is isomorphic to the ring $\mathbb{Z}_n$.

While the individual structures of cyclic groups and cyclic modules are well known, the exact conditions that connect them over an arbitrary ring R are not always explicitly detailed in the literature. This paper fills this gap by proving a theorem that shows us these conditions.

However, this theorem only applies to finite cyclic groups. It does not show the conditions for an infinite cyclic group, such as $\mathbb{Z}$. This naturally raises a question: Can we construct similar conditions for an infinite cyclic group? The answer to this question would generalize the theorem that is presented here.

To see how the theorem works, we now consider two examples. First, let $G = \mathbb{Z}_7$ and $R = \mathbb{Z}_{14}$. We will show there exists a surjective ring homomorphism $\phi : \mathbb{Z}_{14} \to \mathbb{Z}_7$. Define $\phi([x]_{14}) = [x]_7$. ϕ is a homomorphism because it satisfies $\phi([a]_{14} + [b]_{14}) = \phi([a+b]_{14}) = [a+b]_7 = [a]_7 + [b]_7 = \phi([a]_{14}) + \phi([b]_{14})$ and $\phi([a]_{14}[b]_{14}) = \phi([ab]_{14}) = [ab]_7 = [a]_7[b]_7 = \phi([a]_{14})\phi([b]_{14})$ for all $[a]_{14}, [b]_{14} \in \mathbb{Z}_{14}$. Then ϕ is surjective because $\forall [y]_7 \in \mathbb{Z}_7 \exists [x]_{14} = [y]_{14} \in \mathbb{Z}_{14} \ni \phi([x]_{14}) = \phi([y]_{14}) = [y]_7$. Since we found a surjective ring homomorphism from $\mathbb{Z}_{14} \to \mathbb{Z}_7$, it is guaranteed that $\mathbb{Z}_7$ can be a cyclic $\mathbb{Z}_{14}$-module. By the action $r * [g] = \phi(r)[g]$, we can see how an element of $\mathbb{Z}_{14}$ acts on an element of $\mathbb{Z}_7$. For instance $[13]_{14}$ acts on $[4]_7$ as $[13]_{14} * [4]_7 = \phi([13]_{14})[4]_7 = 13 \cdot 4 = 52 \equiv [3]_7$.

For the second example, let $G = \mathbb{Z}_5$ and $R = \mathbb{Z}_8$. Assume there exists a ring homomorphism $\phi : \mathbb{Z}_8 \to \mathbb{Z}_5$. In the ring $\mathbb{Z}_8$, we can write $[0]_8$ as $[8]_8$ such that $\phi([8]_8) = \phi([0]_8) = [0]_5$. We can also write $[8]_8$ as the sum of $[1]_8$ with itself eight times. $\phi([8]_8) = \phi([1]_8 + \cdots + [1]_8) = \phi([1]_8) + \cdots + \phi([1]_8) = 8 \cdot \phi([1]_8)$. Since ϕ is a homomorphism, we know that $\phi([1]_8) = [1]_5$, so $\phi([8]_8) = 8 \cdot [1]_5 = [8]_5 = [3]_5$. But we also know that $\phi([8]_8) = [0]_5$. It means $\phi([8]_8)$ must be equals to $[0]_5$ and $[3]_5$. This implies that $[0]_5 = [3]_5$ which is false. Therefore, our assumption is false and there is no such ring homomorphism exists and $\mathbb{Z}_5$ can't be a cyclic $\mathbb{Z}_8$-module.

IV. Conclusion

This paper's objective was to determine the necessary and sufficient condition for a finite cyclic group of order n to be endowed with the structure of a cyclic R-module for an arbitrary ring R. This work has shown that such a structure exists if and only if there exists a surjective ring homomorphism from R to $\mathbb{Z}_n$, where n is the order of the group. It implies that the conditions to view a finite cyclic group as a cyclic R-module depend entirely on the structure of the ring R, not the structure of its group. This result emphasizes the relationship between finite cyclic groups, rings, and cyclic modules, a topic that is often not explained in detail in the literature, thereby providing valuable theoretical clarity.

References

[1] W. K. Nicholson, "*Introduction to Abstract Algebra."* John Wiley & Sons, Inc., 2012.
[2] T. Hausberger, "*Abstract Algebra Teaching and Learning*," in Encyclopedia of Mathematics Education, S. Lerman, Ed. Cham, Springer, 2018.
[3] A. Chernousov, A. Merkurjev, J. Mináč, and Z. Reichstein, "*Algebraic Groups, Quadratic Forms and Related Topics.*" Workshop report, 2009.
[4] L. Corry, "The origins of the definition of abstract rings," *Modern Logic*, vol. 8, no. 1–2, pp. 5–27, 1998.
[5] D. S. Malik, J. M. Mordeson, and M. K. Sen, "*Fundamentals of Abstract Algebra*." McGraw-Hill, 1997.
[6] G. Sardanashvily, "Lectures on Differential Geometry of Modules and Rings," *arXiv Preprint*, arXiv:0910.1515, 2009. [Online]. Available: https://arxiv.org/abs/0910.1515
[7] R. E. Parsons, "Alternate Definitions of Vector Space Dimension and Module Rank Using Isomorphisms," *arXiv Preprint*, arXiv:2211.05577, 2022. DOI: 10.48550/arxiv.2211.05577
[8] W. A. Adkins and S. H. Weintraub, "*Algebra: An Approach via Module Theory*, *ser. Graduate Texts in Mathematics."* Springer-Verlag, 1992.
[9] P. Aluffi, "*Algebra: Chapter 0*," ser. Graduate Texts in Mathematics. Mathematical Society, 2009.
[10] T. W. Hungerford, "*Algebra*," ser. Graduate Texts in Mathematics, vol. 73. Springer-Verlag, 1980.
[11] J. S. Milne, *Group Theory*, v4.00, 2021. [Online]. Available: https://www.jmilne.org/math/
[12] C. C. Pinter, "*A Book of Abstract Algebra*," 2nd ed. Mineola. Dover Publications, Inc., 2010.
[13] A. W. Knapp, "*Basic Algebra*," Digital 2nd ed. Birkhäuser, 2016.
[14] H. Kurzweil and B. Stellmacher, "*The Theory of Finite Groups: An Introduction*." Springer-Verlag, 2004.
[15] D. S. Dummit and R. M. Foote, "*Abstract Algebra*," 3rd ed. Hoboken. Wiley, 2004.
[16] R. B. Ash, "*A Course in Commutative Algebra*, 2003. [Online]. Available: https://faculty.math.illinois.edu/~r-ash/ComAlg.pdf
[17] S. Lang, "*Algebra*," 3rd ed., ser. Graduate Texts in Mathematics, vol. 211. New York, NY, USA: Springer-Verlag, 2002.
[18] P. A. Grillet, "*Abstract Algebra*," 2nd ed. Springer, 2007.
[19] Y. Watase, "Ring of Endomorphisms and Modules over a Ring," *Formalized Math.*, vol. 30, no. 3, pp. 211–221, 2022.
[20] N. Jacobson, "*Basic Algebra I*," 2nd ed.: W. H. Freeman and Company, 1985.