ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec585

# Some Generalized Characteristics of Cyclic Group and Applications in Chemistry

B. I. Ita[1*]; P. C. Ukachukwa[2]; N. I. Ntoni[3]; Charity Amanyi[4]

[1;2;3;4]Group Theory Unit, Department of Pure and Industrial Chemistry, University of Calabar, Calabar, CRS, Nigeria

Corresponding Author: B. I. Ita[1*]

Publication Date: 2025/12/22

**Abstract: In group theory, the cyclic group is a fundamental and seriously studied and understood classes, and is a corner stone in the study of algebraic structures. This paper studies several generalized characteristics of cyclic group with the aim of extending fundamental results and their implications within a broader context and applications to chemistry. We looked at classical properties of cyclic groups, their generation, structure and subgroup behavior. We also explore generalizations such as the decomposition of finite abelian into cyclic subgroup and their behavior under direct product constructions, and the role of cyclicity in automorphism groups and homomorphic images. Using proof-based analysis, we show that these generalized properties reveal deeper structural insights and enable a quick understanding of algebraic systems. Applications to chemistry are also discussed to highlight the practical relevance of cyclic group theory. The paper concludes the directions to future research on cyclic groups in some complex algebraic systems.**

**How to Cite:** B. I. Ita; P. C. Ukachukwa; N. I. Ntoni; Charity Amanyi (2025) Some Generalized Characteristics of Cyclic Group and Applications in Chemistry. *International Journal of Innovative Science and Research Technology*, 10(12), 1264-1269. https://doi.org/10.38124/ijisrt/25dec585

## I. INTRODUCTION

Group theory is central to abstract algebra and studies groups which are algebraic structures. Groups discuss the notion of symmetry and structure-preserving transformations. It has very wide applications in chemistry and chemical physics etc. Studying the various classes of groups reveals that cyclic groups are very significant due to their simplicity and fundamental role in understanding the structure of chemistry and their related structures. A cyclic group is referred to one that can be generated by a single element such that every other element of the group can be expressed as a power or multiple of that generator. The group of integers under addition, Z and additive group of integers mod n, $Z_n$ are classic examples [1]. The motivation of this paper lies in the desire to revisit known properties of cyclic groups and use them to discuss more generalized texts such as products of cyclic groups, auto0morphism structures and cyclic behavior in non-cyclic environments. While classical texts have addressed the fundamental concepts of cyclic groups relatively few works focus on synthesizing and generalizing these properties across diverse algebraic constructions [2,3]. This paper explores both standard and generalized properties of cyclic groups and gives the core characteristics that broadens the theoretical concepts of cyclic groups. In particular we study the structural, homomorphic, and automorphic behavior in cyclic and related groups. Through rigorous proofs and examples we develop a more clearer understanding of how cyclicity imfluences broader theoretical concepts.

## II. MATHEMATICAL PRELIMINARIES

➢ *Definition of Cyclic Groups*

A cyclic group $C_n$ is defined as $C_n=\{e, g, g^2, \ldots, g^{n-1}\}\ with\ g^n = e.$ A 1-generator group $\langle C_n \rangle$ is termed cyclic and it consists of all the powers of $g$ [4]. The addition group of integers, (Z,+) is an infinite cyclic group generated by 1 or-1. The group $Z_n$ is the additive group of congruence classes modulo n and is a finite cyclic group of order n, generated by 1. The multiplicative group of units modulo n is denoted as $Z_n^*$ and is also cyclic for certain values of n such as when n is a prime. Thus if $C_n$ is a cyclic group then there exist $g \in C_{n,}, h \in C_n$ such that $g^n = h$ (in multiplicative form) or $h = ng$ (in additive form) for some integer n.

## III. NOTATION AND CONVENTION

- We shall use multiplication for a group operations unless stated otherwise
- We shall write $\langle C_n \rangle$ to denote cyclic group generated by $g$ .
- We shall use ≅ to denote isomorphism

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec585

- $Z_n$ will denote the addition group of integers modulo n
- We will discuss finite groups unless stated otherwise
- For $g \in C_n$, the smallest positive integer n which gives $g^n = e$, where $e$ is the identity element, is called the order of $g$.

## IV. FUNDAMENTAL PROPERTIES OF CYCLIC GROUPS

There are basic properties of cyclic groups that make them different from the other types of groups. We shall prove some theorems of cyclic groups here:

➢ *Theorem: Every subgroup of a cyclic group is cyclic. Mathematically:*

Let $C_n = \langle g \rangle$ be a cyclic group. Then every subgroup $H \leq C_n$ is also cyclic.

- Proof: Let $C_n = \langle g \rangle$ and let also $H \leq C_n$. Since $C_n$ is cyclic, we shall write every element of $C_n$ to be of the form $g^n$ for some $n \in Z$. Let $p$ be smallest positive integer such that $g^p \in H$. Then we can write $H = \langle g^p \rangle$. Let $v \in H$, so $v = g^w$ for some $w = Z$. Using the division algorithm, we write $w = ap + b$, with $0 \leq b < p$.
- Then:

$$v = g^w = g^{ap+b} = g^{ap}g^b = (g^p)^a g^b$$

Since $v \in H$ and $g^p \in H$, it follows that $g^b \in H$. But $0 \leq b < p$, and $p$ is the minimal positive integer such that $g^b \in H$. Hence, $b = 0$.

Therefore,

$v \in \langle g^p \rangle$. Thus, $H = \langle g^p \rangle$, and $H$ is cyclic.

➢ *Number of Generators of a Cyclic Group*

Let $C_n = Z_n$. The number of generators of $C_n$ is given by the Euler's totient function [5] $\omega(n)$, which counts the number of integers less than $n$ that are relatively prime to $n$. Example: In $Z_8$, the elements 1, 3, 5, and 7 are relatively prime to 8. Hence, there are $\omega(8) = 4$ generators.

➢ *Structure of Finite versus Infinite Cyclic Groups*

- *If $C_n$ is a Cyclic Group Generated by g Such that all Powers of g are Not Different then*

$C_n = \{g\}$ is a finite cyclic group. $g^n = e$ if $n > 0$, the order of $g$. Thus a finite cyclic group of order $n$ is isomorphic to $Z_n$, the group of integers modulo n. We can write that $C_n = \{g^1, g^2, \ldots, g^{n-1}, g^n\}$

➢ *If $C_n$ be a cyclic group generated by $g$ such that all the powers of $g$ are distinct, then we can say that $C_n = \{g\}$ is an infinite cyclic group. It is isomorphic with $Z$, the group of integers with addition. Each subgroup of $Z$ is of the form of $vZ$, which is itself cyclic. Thus, both finite and infinite cyclic groups have cyclic subgroups [6].*

- *Isomorphism Between $Z_n$ and Finite Cyclic Groups of Order $n$*

✓ Theorem: Every finite cyclic group of order $n$ is isomorphic to $Z_n$.

✓ Proof: Let $|C| = n$. Define a map: $\gamma: Z_n \to C$. $\gamma(p) = g^p$. This map is a homomorphism since: $\gamma(\alpha + \beta) = g^{\alpha+\beta} = g^\alpha g^\beta = \gamma(\alpha)\gamma(\beta)$. It is also bijective, since $|C| = |Z_n| = n$ and the orders match. Thus, $C \cong Z_n$.

➢ *Generalizations and Extended Characteristics*

While cyclic groups are well studied and understood by mathematicians, their structural influence cover more broader classes of algebra. We here discuss other generalizations and a more complex behavior of cyclic groups:

- *Generalizations to Direct Products of Cyclic Groups:*

The fundamental theorem of finite abelian groups indicate that any abelian finite group can be linked up to the direct product of cyclic groups.

✓ Example: The group $Z_6 \cong Z_2 \times Z_3$ since 2 and 3 are coprime.

- *Characteristics of Finite Abelian Groups Using Cyclic Groups.*

✓ Theorem: Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.

✓ Proof: The proof has two main steps:

- *Reduce to P-Groups (Primary Decomposition)*

Let $|C| = n$ and a factor $n = \prod_{i=1}^{r} p_i^{a_i}$ into distinct primes $p_i$. For each prime $p$ dividing $|C|$ define the $p$-primary component

$$C_{\langle p \rangle} = \{g \in C : p^r g = e \text{ } for \text{ } some \text{ } r \geq 0\}$$

✓ *Direct Primary Components Intersect Trivially:*

If $g \in C_{\langle p \rangle} \cap C_{\langle q \rangle}$ with $p \neq q$ then $q$ has order a divisor of a power of $p$ and of a power of $q$, hence order is 1, so $g = e$.

The product of the primary components equals $C$: every element of $g \in C$ has a finite order dividing $n$, so $g$ can be uniquely written as product of elements each of prime-power order. The map $\prod C_{\langle p \rangle} \to C$ is an isomorphism. Thus, $C \cong \prod_{p \langle |C| \rangle} C_{\langle p \rangle}$

- *Decompose a Finite Abelian p-Group into Cyclic p-Power Factors*

Let $C$ be a finite abelian $p$-group. Define $pC = \{pg : g \in C\}$. $k = dim_{F_p}(C/pC)$

We claim

$$C = \langle y_1 \rangle \oplus \langle y_2 \rangle \oplus \ldots \oplus \langle y_i \rangle$$

- *The Subgroups $\langle y_i \rangle$ Generate $C$*

Let $g \in C$. Its coset $\bar{g} \in C/pC$ can be written as an $F_p$-linear combination of basis.

$$\bar{g}=a_1\overline{y_1}+\cdots+a_r\overline{y_r} \qquad (a_i \in \{0,\dots,p-1\})$$

$$g-(a_1y_1+\cdots+a_ry_r) \in pC$$

$$g=(a_1y_1+\cdots+a_ry_r)+p(b_1y_1+\cdots+b_ry_r)+p^2(\dots)+\cdots$$

- *The Sum is Direct*

Suppose

$$x_1+x_2+\cdots+x_r=e$$

Then $p(\gamma_1+\gamma_2+\cdots+\gamma_r)=e$

Therefore $C$ is (isomorphic to) a direct product of the cyclic groups $\langle y_i \rangle$ of orders $p^{n_i}$

- *Combine Primary Components*

- ✓ Putting steps (i) and (ii) together,
- ✓ For each prime $p/|C|$ we have

$$C_{\langle p \rangle} \cong Z/p^{n_{p,i}}Z$$

This proves the desired statement.

- *Cyclicity in Permutation Groups, Matrix Groups and Modular Arithmetics*

- ✓ In permutation groups, some subgroups especially those generated by a single cycle are cyclic.

- Proof: Let $S_n$ be the symmetric group on 1,…,$n$. Fix an $\mu-$ cycle, $\beta=(c_1c_2 \dots c_\mu)$

- ✓ All powers of $\beta$ are in $H$ and $\beta^\mu=e$. Applying $\beta, \mu$ times returns every $C_i$ to itself, so $\beta^\mu$ is the identity permutation $e$. Hence, every $\beta^\propto$ (for integer $\propto$ ) lies in $H$, and $\beta^\mu=e$.
- ✓ The powers $e, \beta, \beta^2, \dots, \beta^{\mu-1}$ are distinct.

If $\beta^i=\beta^j$ with $0 \le i < j < \mu$, then $\beta^{j-i}=e$ with $0 < j-i < \mu$, contradicting that $\mu$ is the length of the circle (the least positive integer $r$ with $\beta^i=e$ is $r=\mu$). Therefeore, the $\mu$ elements $e, \beta, \beta^2, \dots, \beta^{\mu-1}$ are pairwise distinct.

- ✓ These Powers Exhaust $H$

By definition $H$ consists of all integer powers $\beta^\mu$. But any integer $\omega$ can be written $\omega=q\mu+v$ with $0 \le \omega < v$, then $\beta^\mu=(\beta^\mu)^\omega\beta^v=e^\omega\beta^v=\beta^v$. So every power equals one of the $\mu$ listed elements.

From (ii) and (iii) we conclude $|H|=\mu$ and $H=e, \beta, \dots, \beta^{\mu-1}$. Thus, $H$ is generated by a single element $\beta$ and is therefore a cyclic group of order $\mu$. Infact $H \cong Z_n$ via the map $r \mapsto \beta^\mu$. If $\beta=(C_1 \dots C_\mu)$ and $\tau=(d_1 \dots d_v)$ are disjoint cycles, then $\beta$ and $\tau$ commute and the other of the product $\beta\tau$ is 1cm $(\mu, v)$. Consequently, the subgroup $\langle \beta, \tau \rangle=\langle \beta\tau \rangle$ is cyclic iff $\mu$ and $v$ are coprime $(so\ 1cm\ (\mu, v)=\mu v)$; more generally, a product of disjoint cycles generates a cyclic subgroup exactly when the cycle lengths are pairwise coprime.

- ✓ Detailed Proof of Disjoint-Cycle Extension Statement

Let $\beta$ and $\tau$ be disjoint cycles in $S_n$ of lengths $\omega=ord(\beta)$ and $v=ord(\tau)$. Then

- $\beta$ and $\tau$ commute: $\beta\tau=\tau\beta$.
- $ord(\beta\tau)$ $=1cm(\omega, v)$.
- The Subgroup $\langle \beta, \tau \rangle$ consists exactly of the same element $\beta^i\tau^j: 0 \le i < \omega; 0 \le j < v$ and $|\langle \beta, \tau \rangle|=\omega v$. Consequently $\langle \beta, \tau \rangle \cong Z_{\omega;} \times Z_v$ and is cyclic iff $gcd(\omega, v)$=1; in that case : $\beta\tau$ has the order $\omega v$ and generates the whole subgroup.

Proof

- ➢ *They Commute*

Let M be the support of $\beta$ (the set of points moved by $\beta$) and N the support of $\tau$. Disjoint cycle mean $M \cap N=\emptyset$. For any $x \in 1, \dots, n$ there are three cases:

- $y \in M$; then $\tau(y)=y$, so $\beta\tau(y)=\beta(y)$. Also $\tau\beta(y)=\tau(\beta(y))=\beta(y)$ because $\beta(y) \in M$ and $\tau$ fixes $M$. Thus $\beta\tau(y)=\tau\beta(y)$.
- $y \in N$: Symmetric argument
- $y \notin M \cup N$: both fix $y$, so equally holds. Therefore so $\beta\tau=\tau\beta$.

- ➢ *Order of $\beta\tau$.*

Since $\beta$ and $\tau$ commute, $(\beta\tau)^v=\tau^v\beta^v$ for all integers $v$. Suppose$(\beta\tau)^v=e$. Then $\beta^v=\tau^{-v}$. Apply both sides to any $a\epsilon M$. The right side $\tau^{-v}$ fixes $a$ (since $a \notin N$), so $\beta^v(a)=a$. Hence $\beta^v$ is the identity on $M$, so $\omega$ / $v$. Similarly by applying to points of $N$ we get $\mu/v$. Thus any $v$ with $(\beta\tau)^v=e$ is a common multiple of $\omega$ and $\mu$; equivalently the order of $\beta\tau$ is a multiple of 1cm $(\beta, \mu)$. On the other hand $(\beta\tau)^{1cm(\omega,\mu)}=\beta^{1cm((\omega,\mu))}\tau^{1cm((\omega,\mu))}=e.e=e$. So the least positive $v$ with $(\beta\tau)^v=e$ is exactly 1cm $(\beta, \mu)$. Therefore ord$(\beta\tau)=$ 1cm $(\beta, \mu)$.

- ➢ *Structure of $\langle \beta, \tau \rangle$*

Since $\beta$ and $\tau$ commute, any word in $\beta, \tau$ can be rearranged to form $\beta^i\tau^j$. So $\langle \beta, \tau \rangle \subseteq \beta^i\tau^j; i, j \in Z$. Reducing exponents modulo $\omega$ and $\mu$ shows every element of the subgroup can be written with $0 \le i < \omega; 0 \le j < \mu$. Uniqueness: Suppose $\beta^i\tau^j=\beta^{i'}\tau^{j'}$. Then $\beta^{i-i'}=\tau^{j'-j}$. Therefore $|\langle \beta, \tau \rangle|=\omega \cdot \mu$, and the map $Z_\omega \times Z_\mu \to \langle \beta, \tau \rangle, (i(mod\ \omega), j(mod\ \mu)) \mapsto \beta^i\tau^j$ .

Now a finite direct product $Z_\omega \times Z_\mu$ is a cycle iff $gcd(\omega, \mu)=1$ [7] Translating back: $\langle \beta, \tau \rangle$ is cyclic iff $gcd(\omega, \mu)=1$. If $gcd(\omega, \mu)=1$. then ord$(\beta\tau)=1cm$ $(\omega, \mu)=\omega r=|\langle \beta, \tau \rangle|$ .

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec585

- *Generalization:*

If $\beta_1, \ldots, \beta_v$ are pairwise disjoint cycles with lengths $\omega_1, \ldots, \omega_v$, then they pairwise commute and every element of $(\beta_1, \ldots, \beta_\omega)$ can be written uniquely as $\beta_1^{i_1} \ldots \beta_\omega^{i_\omega}$ with $0 \le i_x < \omega_x$. Thus the subgroup is isomorphic to $Z_{\omega v}$; has order $\prod_{x=1}^{v} \omega_x$, and the product $\beta_1, \ldots, \beta_\omega$ has order 1cm $(\omega_1, \ldots, \omega_v)$. Consequently the subgroup is cyclic exactly when the cycle lengths $\omega_1, \ldots, \omega_v$ are pairwise coprime.

- *Some Sub Groups of General Linear Groups Over Finite Fields (e.g., $GL(n, F_p)$) Contain Cyclic Elements.*

Proof:

We view the finite field $F_p$ as an n-dimensional vector space over the subfield $F_\alpha$ ( with $\alpha = p^r$). Multiplication by any nonzero element $\beta \in F_{\alpha^n}^x$ is an $F_\alpha$-linear map of that vector space with respect to a basis and it is an invertible $n \times n$ matrix over $F_\alpha$. The multiplicative group $F_{\alpha^n}^x$ is a cyclic of order $\alpha^n - 1$, so taking a generator ( a primitive element) gives an element of $GL(n, F_\alpha)$ of order $\alpha^n - 1$. Thus $GL(n, F_\alpha)$ contains a cyclic subgroup of order $\alpha^n - 1$. We consider the following:

✓ *Field and Vector Field Structure*

Let $\alpha = p^r$ (we take r=1, so $q = \alpha$) $\exists$ a degree n extension field $F_{\alpha^n}$. As an $F_\alpha$-vector space, $F_{\alpha^n}$ has dimension n.

✓ *Multiplication by $\beta$ Linear*

For any field $\beta \in F_{\alpha^n}$, define $K_\beta: F_{\alpha^n} \to F_{\alpha^n}$ by $K_\beta(x) = \beta x$. For $a \in F_\alpha$ and $x, y \in F_{\alpha^n}$, $K_\beta(x + ay) = \beta(x + ay) = \beta x + a(\beta y) = K_\beta(x) + aK_\beta(y)$

✓ *Homomorphism from $F_{\alpha^n}^x$ to $GL(n, F_\alpha)$*

The map $\gamma: F_{\alpha^n}^x \to GL(n, F_\alpha), \beta \mapsto K_\beta$, is a group homomorphism because $K_{\beta\delta} = K_\beta \circ K_\delta$. It is injective: if $K_\beta$ is the identity map then $\beta x = x \forall x$, so $\beta = 1$. More generally $K_\beta = K_\delta$ implies $K_{\beta\delta} - 1 = I$ so $\beta\delta^{-1} = 1$, hence $\beta = \delta$. Therefore $F_{\alpha^n}^x$ embeds as a subgroup of $GL(n, F_\alpha)$.

✓ *Cyclicity and the Singer Cycle*

The multiplicative group $F_{\alpha^n}^x$ is cycle of order $\alpha^n - 1$. Let $\theta$ be a generator (a primitive element) of $F_{\alpha^n}^x$. Then $K_\theta \in GL(n, F_\alpha)$ has order $\alpha^n - 1$ and generates an ambedded cyclic subgroup isomotphic to $Z_{\alpha^n - 1}$. Such a $K_\theta$ is called a singer cycle.

✓ *Alternative Concrete Matrix Realization ( Companion Matrix)*

Choose an irreducible monic polynomial $j(x) \in F_\alpha[x]$ of degree n whose root $\theta$ generates $F_{\alpha^n}$ over $K_\alpha$. With respect to the basis $(1, \theta, \theta^2, \ldots, \theta^{n-1})$ the linear map $K_\theta$ has the companion matrix of $j(x)$. That companion matrix is an explicit $n \times n$ matrix in $GL(n, F_\alpha)$ of order dividing $\alpha^n - 1$; if $\theta$ is primitive its order is exactly $\alpha^n - 1$.

➢ *Remarks and Small Examples*

For $\alpha = p$ (primitive field), this shows $GL(n, F_p)$ contains a cyclic subgroup of order $\alpha^n - 1$. So already for $GL(2, F_3)$, there is an element of order $3^2 - 1 = 8$.

More elementary cyclic elements also exist, any scalar matrix $\lambda I$ with $\lambda \epsilon F_\alpha^x$ is in $GL(n, F_\alpha)$ and generates a cyclic subgroup of order $\alpha - 1$. Diagonal matrices with entries in $F_\alpha^x$ give other cyclic subgroups (products of cyclic groups from diagonal entries). The singer cycle is important in finite geometry (ie. Acts regularly on the 1-dimensional subspaces of $F_{\alpha^n}$, i.e. on the point of projective spaces $PG(n - 1, \alpha)$) [8].

- *In Modular Arithmetic , $Z_n \times Z_n^*$ is cyclic iff $n = 1,2,4, \alpha^\beta, or 2\alpha^\beta$ for odd prime $\alpha\alpha$.*

✓ *Proof: Theorem: (Primitive-Root Theorem/ Classification)*

The group $U(n) = (Z/nZ)^x$ is cyclic iff $n \in \{1,2,4\}$ or $n = p^k or\, n = 2p^k$. Proof splits into two parts: reduction by Chinese Remainder Theorem (CRT) and impossibility for most 2-power factors, and existence of primitive roots for odd prime powers.

✓ *Reduction by the Chinese Remainder Theorem (CRT):*

We write the prime-power factorization $= \prod_{i=1}^{\alpha} P_i^{\beta_i}$. Therefore $U(n) \cong \prod_{i=1}^{\alpha} U(P_i^{\beta_i})$. Each factor $U(P_i^{\beta_i})$. Must be cyclic, mand the integers $\left|U(P_i^{\beta_i})\right| = K(P_i^{\beta_i})$. Must be pairwise coprime. So we reduce to understanding the groups $U(P_i^{\beta_i})$ and their orders $K(P_i^{\beta_i})$.

✓ *Structure of $(2^p)$*

$|U(2)| = 1$ (trivial)

$|U(2)| = 1$ for $\beta \ge 3, \left|U(2^\beta) = 2^{\beta - 1}\right|$. But important structural fact is that for $\beta \ge 3, (2^\beta) \cong C_2 \times C_{2^{\beta-2}}$.

Thus only 2-power moduli that give a cyclic unit group are 2 and 4. For $2^\beta$ with $\beta \ge 3, U(2^\beta)$ is not cyclic.

✓ *Structure of $U(p^\beta)$ for Odd Prime $p$*

For a finite field $F_\alpha$, the multiplicative group $F_\alpha^x$ is cyclic of order $\alpha - 1$. This gives a primitive root modulo $p(i.e. U(p) is\ cyclic)$. One then shows a lifting lemma: if $a$ is a primitive not modulo $p(odd\ p)$, then there exists a lift of $a$ to a primitive root modulo $p^\beta$ for every $\beta \ge 1$. A standard statement: if $a$ is primitive modulo $p$ then either $a$ or $a + p$ is primitive modulo $p^2$; once you have a primitive root modulo $p^2$ you can lift inductively to all higher powers $p^\beta$. Hence for every odd prime $p$ and every $\beta \ge 1$, the group $U(p^\beta)$ is cyclic of order $\gamma(p^\beta) = p^{\beta - 1}(p - 1)$.

✓ *Putting Pieces Together (Necessity and Sufficiency)*

- Sufficiency: If $n = 1,2,4$ then $U(n)$ is trivially cyclic. If $n = p^\beta$ with $p$ odd, $U(p^\beta)$ is cyclic. If $n = 2p^\beta$ with $p$

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec585

odd, then by CRT $U(2p^{\beta}) \cong U(2) \times U(p^{\beta}) \cong [1] \times U(p^{\beta}) \cong U(p^{\beta})$.

- Necessity: Suppose $U(n)$ is cyclic. By CRT, each factor $U\left(p_i^{\beta_i}\right)$ must be cyclic. Only the 2-power factor allowed are 2 or 4 (or absent). All odd-prime power factor $U(p^{\beta})$ are cyclic, but now the orders $K(p^{\beta}) = p^{\beta-1}(p-1)$ must be pairwise coprime. If there were two distinct odd powers $p$ and $\theta$ dividing $n$, then both $K(p^{\beta_p})$ and $K(\theta^{\beta_\theta})$ are even (since each contains a factor $p-1$ or $\theta - 1$ which is even), so they have gcd atleast 2; thus the product cannot be cyclic (orders not coprime). Hence there can be at most one odd prime dividing $n$. So $n$ is of the form $2^e \; or \; 2^e p^{\beta}$ with a single odd prime p. As noted, $e$ can only be 0,1,2 (giving 1,2,4) because for $e \geq 3$ the 2-part group is noncyclic. If $e = 2$ and $p$ occurs ( so $n = 4p^{\beta}$), then $|U(4)| = 2$ and $|U(p^{\beta}) = p^{\beta-1}|(p-1)$ is even, so the orders are not coprime and the product is not cyclic. Thus $e$ cannot be 2 when an odd prime factor is present. The only allowed combinations are therefore $n = 1,2,4, n = p^{\beta}$ (one odd prime power), $n = 2p^{\beta}$ (single odd prime power times a single factor 2). That completes the proof.

## V. RELATION TO GROUP HOMOMORPHISM AND AUTOMORPHISM

If $G \cong Z_n$, then the automorphism group $Aut(G) \cong Z_n^*$. The number of automorphisms of a cyclic group of order $n$ is $\phi(n)$.

Proof

Let $C_n = \langle v \rangle$ be a cyclic group of order $n$. An automorphism of $C_n$ is a bijective homomorphism $\phi: C_n \to C_n$. A homomorphism of a cyclic group is completely determined by the image of a generator.

- *Image of a Generator Must be a Generator*

If $\phi$ is an automorphism and $v$ is a generator of $C_n$, then $\varphi(v)$ must generate $C_n$ (because $\phi$ is surjective). Conversely, if $g \in C_n$ is a generator, then the map defined by $v \longmapsto g$ extends to a homomorphism $C_n \longrightarrow C_n$ which is necessarily surjective (hence bijective), so it is an automorphism.

- *Generators of $C_n$*

The elements of $C_n$ can be written$v^0, v^1, \dots, v^{n-1}$. An element $v^k$ is a generator iif gcd (k,n) = 1. The number of integers $k$ with $0 \leq k \leq n-1 \; and \; \gcd(k,n) = 1$ is $\phi(n)$(Euler's totient function).

- *Counting Automorphism*

Each automorphism is determined uniquely by the image of $v$, and the possible images are exactly the $\phi(n)$ generator $v^k$ with $\gcd(k,n) = 1$. Therefore there are exactly $\phi(n)$ automorphisms: $|Aut(C_n)| = \phi(n)$.

Examples:

- $C_6$ (cyclic group of order 6)

$C_6 = \langle v \rangle = v^0, v^1, v^2, v^3, v^4, v^5$. The generators are $v^k$ with $\gcd(k,6) = 1$.

Check each exponent $k$:

$\gcd(1,6) = 1 \Longrightarrow v^1$ is a generator

$\gcd(2,6) = 2 \Longrightarrow v^2$ is not a generator

$\gcd(3,6) = 3 \Longrightarrow v^3$ is not a generator

$\gcd(4,6) = 2 \Longrightarrow v^4$ is not a generator

$\gcd(5,6) = 1 \Longrightarrow v^5$ is a generator

So the generators are $v^1, v^5$. Thus $\phi(6) = 2$, and indeed $|Aut(C_6)|$=2. The automorphisms are

$\phi_1: v \longmapsto v^1$ (identity automorphism)

$\phi_2: v \longmapsto v^5$ (inversion automorphism)

- For $Z_7$, since $\varphi(7) = 6$, there are 6 automorphisms. Homomorphic images of cyclic groups are also cyclic. Let $\varphi: G \longrightarrow H$ be a group homomorphism where $G$ is cyclic. Then $\varphi(G)$ is also cyclic.

Proof: Let $G$ be a cyclic group and $\varphi: G \longrightarrow H$ a group homomorphism. Write $G = \langle v \rangle$ (so every element of $G$ is $v^k$ for some integer $k$).

$$\varphi(v^k) = (\varphi(v))^k$$

$$\varphi(G) = \{(\varphi(v))^k : k \in Z\} = \langle \varphi(v) \rangle$$

- *Remarks:*

If $\varphi(v)$ is the identity in $H$, then $\varphi(G)$ is the trivial (cyclic) subgroup. If $|v| = n < \infty$, then $|\varphi(v)|$ divides $n$. For $G \cong Z$ (infinite cyclic), the same argument shows any image in $Z$ is cyclic.

## VI. APPLICATIONS AND IMPLICATIONS

- *Cyclic Groups are Very Important in Chemistry with Significant Applications Across Multiple Disciplines.*

- Cyclic groups describe: (a) Planar ring systems such as benzene ($C_6$), cyclobutadiene ($C_4$) where the symmetry operation available is rotation. We therefore model this by $C_n$ where $n$ is a single rotation order representing rotation by $\frac{2\pi}{n}$. The group $C_n$ does not include reflections or inversion but captures only all the rotational operations. Therefore, the symmetry group of a planar ring molecule is often isomorphic to $C_n$ . Benzene is a planar hexagonal ring and its rotation is by $\frac{2\pi}{n} = 60^o$ about its central axix

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec585

and maps the molecule onto itself. The set of operations are $\{E, C_6, C_6^2, C_6^3, C_6^4, C_6^5\}$ [9]

$C_6$ represents a $60^o$ rotation. Thus, benzene's rotation has a subgroup of $C_6$. Also cyclobutadiene $(C_4H_4)$ is a square planar ring with symmetry of $90^o$ rotation $\left(\frac{2\pi}{4}\right)$ having elements $E, C_4, C_4^2, C_4^3 \equiv C_4^-$.So its rotational symmetry is $C_4$. Cyclopropane $(C_3H_6)$ is an equilateral triangular ring with $120^o$ symmetry rotation of $C_3$having symmetry elemetns $E, C_3, C_3^2 \equiv C_3^-$. Cyclooctatetraene (COT,$C_8H_8, planar\ form$) has octagonal symmetry with $45^o$ rotations. Its symmetry elements are $E, C_8, C_8^2, \dots, C_8^7 \equiv C_8^-$.

- Cyclic groups are also useful in spectroscopy. Using group theory we can predict allowed IR and Raman vibrational modes by classifying them into irreducible representations of $C_n$. Benzene's six $\pi$ −orbitals also transform under $C_6$. Cyclic groups also model rotational symmetry of 2D crystal lattices (e.g. grapheme sheets). All planar ring molecules have rotational symmetry groups isomorphic to cyclic $C_n$ groups.
- Non-linear molecules like ammonia $(NH_3)$ are modeled by $C_3$ [10]. The elements are $E, C_3, C_3^2 \equiv C_3^-$.

## VII. CONCLUSION

Cyclic groups are known to analyze chemical systems like planar molecules, spectroscopy and crystallography. Therefore cyclic groups bridge the gap between mathematics and chemistry.

## REFERENCES


[1]. F. A. Cotton, and G. Wilkinson. (2021). Advanced Inorganic Chemistry, Wiley.

[2]. D. M. Bishop. (2020). Group Theory and Chemistry. Dover publications.

[3]. P. W. Atkins and R. Friedman. (2023). Molecular Quantum Mechanics. Oxford University Press.

[4]. M. Hargittai and I. Hargittai. (2021). Symmetry through eyes of a Chemist. Springer.

[5]. M. Ziolkowski. (2022). Applications of symmetry and group theory in Computational Chemistry. Journal of molecular modelling, 28 *5), 141-148.

[6]. K. Balasubramanian. (2021). Group Theory and Molecular symmetry in Modern Quantum Chemistry. International Reviews in Physical Chemistry. 40 (1), 1-53.

[7]. M. Tinkham. (2020). Group Theory and quantum Mechanics. Dover Publications.

[8]. T. Solymosi and L. Nemes (2022). Group-Theoretical Analysis of Vibrational Spectra of Cyclic molecules. Spectrochimica Acta Part A: molecular and Biomolecular Spectroscopy. 273, 121026-121054.

[9]. M. Senechal. (2021). Crystalline Symmetries: An Informal Mathematical Introduction. Dover.

[10]. C. Liu. (2023). Cyclic Group Symmetry in Supramolecular Self-Assembly. Chemical Society Reviews. 52(12), 4931-4954.