



*Journal of Advances in
Science and Technology*

*Vol. V, Issue. IX, May-2013,
ISSN 2230-9659*

A STUDY ON CYCLIC GROUPS

A Study on Cyclic Groups

Rekha Rani

Research Scholar, Department of Mathematics, MDU, Rohtak, Haryana, India

Abstract :- A cyclic group is a group that is generated by a single element, in the sense that every element of the group can be written as a power of some particular element g in multiplicative notation, or as a multiple of g in additive notation. This element g is called a "generator" of the group. Any infinite cyclic group is isomorphic to \mathbb{Z} , the integers with addition as the group operation. Any finite cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n with addition as the group operation.

A group G is called cyclic if there exists an element g in G such that $G = \langle g \rangle = \{ g^n \mid n \text{ is an integer} \}$. Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group G that contains g is G itself suffices to show that G is cyclic.

For example, if $G = \{ g^0, g^1, g^2, g^3, g^4, g^5 \}$ is a group, then $g^6 = g^0$, and G is cyclic. In fact, G is essentially the same as that is, isomorphic to the set $\{ 0, 1, 2, 3, 4, 5 \}$ with addition modulo 6. For example, $1 + 2 \equiv 3 \pmod{6}$ corresponds to $g^1 \cdot g^2 = g^3$, and $2 + 5 \equiv 1 \pmod{6}$ corresponds to $g^2 \cdot g^5 = g^7 = g^1$, and so on. One can use the isomorphism χ defined by $\chi(g^i) = i$.

For every positive integer n there is exactly one cyclic group whose order is n , and there is exactly one infinite cyclic group. Hence, the cyclic groups are the simplest groups and they are completely classified.

The name "cyclic" may be misleading: it is possible to generate infinitely many elements and not form any literal cycles; that is, every g^n is distinct. It can be said that it has one infinitely long cycle. A group generated in this way is called an infinite cyclic group, and is isomorphic to the additive group of integers \mathbb{Z} .

Furthermore, the circle group (whose elements are uncountable) is not a cyclic group—a cyclic group always has countable elements.

Since the cyclic groups are abelian, they are often written additively and denoted \mathbb{Z}_n . However, this notation can be problematic for number theorists because it conflicts with the usual notation for p -adic number rings or localization at a prime ideal. The quotient notations $\mathbb{Z}/n\mathbb{Z}$, \mathbb{Z}/n , and $\mathbb{Z}/(n)$ are standard alternatives. One may write the group multiplicatively, and denote it by C_n , where n is the order (which can be ∞). For example, $g^2 g^4 = g^1$ in C_5 , whereas $2 + 4 = 1$ in $\mathbb{Z}/5\mathbb{Z}$.

INTRODUCTION

A cyclic group is a group that can be generated by a single element X (the group generator). Cyclic groups are Abelian.

A cyclic group of finite group order n is denoted C_n , \mathbb{Z}_n , or $\mathbb{Z}/n\mathbb{Z}$ and its generator X satisfies

$$X^n = I,$$

where I is the identity element.

The ring of integers \mathbb{Z} form an infinite cyclic group under addition, and the integers $0, 1, 2, \dots, n-1$ (\mathbb{Z}_n)

form a cyclic group of order n under addition (mod n). In both cases, 0 is the identity element.

There exists a unique cyclic group of every order $n \geq 2$, so cyclic groups of the same order are always isomorphic. Furthermore, subgroups of cyclic groups are cyclic, and all groups of prime group order are cyclic. In fact, the only simple Abelian groups are the cyclic groups of order $n = 1$ or n a prime.

The n th cyclic group is represented in Mathematics as Cyclic Group[n], and an inefficient permutation group representation is given by CyclicGroup[n] in the Mathematica package Combinatorica.

Examples of cyclic groups include C_2, C_3, C_4, \dots , and the modulo multiplication groups M_m such that $m = 2, 4, p^n$, or $2p^n$, for p an odd prime and $n \geq 1$.

More generally, if d is a divisor of n , then the number of elements in \mathbb{Z}/n which have order d is $\phi(d)$. The order of the residue class of m is $n / \gcd(n, m)$.

If p is a prime number, then the only group (up to isomorphism) with p elements is the cyclic group C_p or $\mathbb{Z}/p\mathbb{Z}$. There are more numbers with the same property, see cyclic number.

The direct product of two cyclic groups $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ is cyclic if and only if n and m are coprime. Thus e.g. $\mathbb{Z}/12\mathbb{Z}$ is the direct product of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$, but not the direct product of $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

The definition immediately implies that cyclic groups have group presentation $C_\infty = \langle x \mid \rangle$ and $C_n = \langle x \mid x^n \rangle$ for finite n .

A primary cyclic group is a group of the form $\mathbb{Z}/p^k\mathbb{Z}$ where p is a prime number. The fundamental theorem of abelian groups states that every finitely generated abelian group is the direct product of finitely many finite primary cyclic and infinite cyclic groups.

$\mathbb{Z}/n\mathbb{Z}$ and \mathbb{Z} are also commutative rings. If p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field, also denoted by \mathbb{F}_p or $\mathbf{GF}(p)$. Every field with p elements is isomorphic to this one.

The units of the ring $\mathbb{Z}/n\mathbb{Z}$ are the numbers coprime to n . They form a group under multiplication modulo n with $\phi(n)$ elements (see above). It is written as $(\mathbb{Z}/n\mathbb{Z})^\times$. For example, when $n = 6$, we get $(\mathbb{Z}/n\mathbb{Z})^\times = \{1, 5\}$. When $n = 8$, we get $(\mathbb{Z}/n\mathbb{Z})^\times = \{1, 3, 5, 7\}$.

In fact, it is known that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if n is 1 or 2 or 4 or p^k or $2p^k$ for an odd prime number p and $k \geq 1$, in which case every generator of $(\mathbb{Z}/n\mathbb{Z})^\times$ is called a primitive root modulo n . Thus, $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic for $n = 6$, but not for $n = 8$, where it is instead isomorphic to the Klein four-group.

The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic with $p - 1$ elements for every prime p , and is also written $(\mathbb{Z}/p\mathbb{Z})^\times$ because it consists of the non-zero elements. More generally, every finite subgroup of the multiplicative group of any field is cyclic. For example, this follows from the characterization below.

Let G be a finite group. Then G is a cyclic group if, for each $n > 0$, G contains at most n elements of order dividing n .

EXAMPLES

In 2D and 3D the symmetry group for n -fold rotational symmetry is C_n , of abstract group type \mathbb{Z}_n . In 3D there are also other symmetry groups which are

algebraically the same, see Symmetry groups in 3D that are cyclic as abstract group.

Note that the group S^1 of all rotations of a circle (the circle group) is not cyclic, since it is not even countable.

The n th roots of unity form a cyclic group of order n under multiplication. e.g., $0 = z^3 - 1 = (z - s^0)(z - s^1)(z - s^2)$ where $s = e^{2\pi i/3}$ and a group of $\{s^0, s^1, s^2\}$ under multiplication is cyclic.

The Galois group of every finite field extension of a finite field is finite and cyclic; conversely, given a finite field F and a finite cyclic group G , there is a finite field extension of F whose Galois group is G .

PROPERTIES OF CYCLIC GROUP :

Given a cyclic group G of order n (n may be infinity) and for every g in G ,

- G is abelian; that is, their group operation is commutative: $gh = hg$ (for all g and h in G). This is so since $r + s \equiv s + r \pmod{n}$.
- If n is finite, then $g^n = g^0$ is the identity element of the group, since $kn \equiv 0 \pmod{n}$ for any integer k .
- If $n = \infty$, then there are exactly two elements that each generate the group: namely 1 and -1 for \mathbb{Z} .
- If n is finite, then it is isomorphic to the group $\{ [0], [1], [2], \dots, [n-1] \}$ of integers modulo n under addition and there are exactly $\phi(n)$ elements that generate the group on their own, where ϕ is the Euler quotient function.
- Every subgroup of G is cyclic. (see fundamental theorem of cyclic groups and see also a section below) Indeed, each finite subgroup of G is a group of $\{ 0, 1, 2, 3, \dots, m-1 \}$ with addition modulo m . And each infinite subgroup of G is $m\mathbb{Z}$ for some m , which is bijective to (so isomorphic to) \mathbb{Z} .
- Every quotient group of G is cyclic. In fact, under any group homomorphism, the image of a cyclic group is generated by the image of a generator of the cyclic group.

IMPORTANCE OF CYCLIC GROUP :

Cyclic groups are groups in which every element is a power of some fixed element. (If the group is abelian and I'm using $+$ as the operation, then I should say instead that every element is a {it multiple} of some fixed element.) Here are the relevant definitions.

Definition. Let G be a group, $g \in G$. The order of g is the smallest positive integer n such that $g^n = 1$. If

there is no positive integer n such that $g^n = 1$, then g has infinite order.

In the case of an abelian group with $+$ as the operation and 0 as the identity, the order of g is the smallest positive integer n such that $ng = 0$.

Definition. If G is a group and $g \in G$, then the subgroup generated by g is

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

If the group is abelian and I'm using $+$ as the operation, then

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}.$$

Definition. A group G is cyclic if $G = \langle g \rangle$ for some $g \in G$. g is a generator of $\langle g \rangle$.

If a generator g has order n , $G = \langle g \rangle$ is cyclic of order n . If a generator g has infinite order, $G = \langle g \rangle$ is infinite cyclic.

Example. (The integers and the integers mod n are cyclic) \mathbb{Z} is an infinite cyclic group. (In fact, it is the only infinite cyclic group up to isomorphism.) Notice that \mathbb{Z} is generated by 1 and by -1 --- a cyclic group can have more than one generator.

If n is a positive integer, \mathbb{Z}_n is a cyclic group of order n generated by 1 .

Theorem. Subgroups of cyclic groups are cyclic.

Proof. Let $G = \langle g \rangle$ be a cyclic group, where $g \in G$. Let $H < G$. If $H = \{1\}$, then H is cyclic with generator 1 . So assume $H \neq \{1\}$.

On the other hand, if H contains a negative power of g --- say g^{-k} , where $k > 0$ --- then $g^k \in H$, since H is closed under inverses. Hence, H again contains positive powers of g , so it contains a *smallest* positive power, by Well Ordering.

So We have g^m , the smallest positive power of g in H . I claim that g^m generates H . I must show that every $h \in H$ is a power of g^k . Well, $h \in H < G$, so at least I can write $h = g^n$ for some n . But by the Division Algorithm, there are unique integers q and r such that $n = mq + r$, where $0 \leq r < m$.

It follows that

$$g^n = g^{mq+r} = (g^m)^q \cdot g^r, \text{ so } h = (g^m)^q \cdot g^r, \text{ or } g^r = (g^m)^{-q} \cdot h.$$

Now $g^m \in H$, so $(g^m)^{-q} \in H$. Hence, $(g^m)^{-q} \cdot h \in H$, so $g^r \in H$. However, g^m was the *smallest positive power of g lying in H* . Since $g^r \in H$ and $r < m$, the only way out is if $r = 0$. Therefore, $n = qm$, and $h = g^n = (g^m)^q \in \langle g^m \rangle$.

This proves that g^m generates H , so H is cyclic.

Theorem. A finite cyclic group of order n contains a subgroup of order m for each positive integer m which divides n .

Proof. Suppose G is a finite cyclic group of order n with generator g , and suppose $m \mid n$. Thus, $mp = n$ for some p .

I claim that g^p generates a subgroup of order m . The preceding proposition says that the order of g^p is $\frac{n}{(p, n)}$. However, $p \mid n$, so $(p, n) = p$. Therefore, g^p has order

$$\frac{n}{(p, n)} = \frac{n}{p} = m.$$

In other words, g^p generates a subgroup of order m .

In fact, it's possible to prove that there is a unique a subgroup of order m for each m dividing n .

Note that for an arbitrary finite group G , it isn't true that if $n \mid |G|$, then G contains a cyclic subgroup of order n .

Example. (Subgroups of a cyclic group) \mathbb{Z}_{15} contains subgroups of order 1 , 3 , 5 , and 15 , since these are the divisors of 15 . The subgroup of order 1 is the identity, and the subgroup of order 15 is the entire group.

The last result says:

- If n divides 15 , then there is a subgroup of order n --- in fact, a unique subgroup of order n .

Since \mathbb{Z}_{15} is cyclic, these subgroups must be cyclic. They are generated by 0 and the nonzero elements in \mathbb{Z}_{15} which divide 15 : 1 , 3 , and 5 .

Example. (A product of cyclic groups) Consider the group

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(m, n) \mid m \in \mathbb{Z}_2, n \in \mathbb{Z}_3\}.$$

The operation is componentwise addition:

$$(m, n) + (m', n') = (m + m', n + n').$$

It is routine to verify that this is a group, the *direct product* of \mathbb{Z}_2 and \mathbb{Z}_3 .

The element $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ has order 6:

$$(1, 1) + (1, 1) = (0, 2),$$

$$(1, 1) + (0, 2) = (1, 0),$$

$$(1, 1) + (1, 0) = (0, 1),$$

$$(1, 1) + (0, 1) = (1, 2),$$

$$(1, 1) + (1, 2) = (0, 0).$$

Hence, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic of order 6. More generally, if $(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn . Be careful! --- $\mathbb{Z}_2 \times \mathbb{Z}_2$ is *not* the same as \mathbb{Z}_4

A cyclic group is a group in which there is an element x such that each element of the group may be written as x^k for some integer k . In additive notation, this translates to $k \cdot x$. We say that x is a generator of the cyclic group or that the group is generated by x .

As an example, the integers under addition is a cyclic group. The number 1 is a generator. This is because for any n in the integers we have $n = n \cdot 1$. Note that -1 is also a generator.

Another example is provided by the set of complex numbers $\{1, -1, i, -i\}$ under multiplication of complex numbers. A generator is i since $i^1 = i$, $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$. Note that $-i$ is also a generator.

For a finite cyclic group G having n elements, any element of order n is a generator. If x is a generator having order n then the order of x^k is $n / \gcd(n, k)$.

It follows that a cyclic group is an abelian group although not every abelian group is a cyclic group. For example, the rational numbers under addition is not cyclic but is abelian.

REFERENCES :

- Patterson, J.D, (2001) Performance Appraisal: Managing the Process and Perceptions of Supervisor Efficiency in the Test Department at Lock head Martin
- Astronautics-Denver. Unpublished Dissertation Abstracts International, 61(7), January, p.2805-A.

- Petter, D. (1977) Peoples and Performance: The Best of Petter Durcker on Management. Mumbai: Allied Publishers Pvt. Ltd.

- Pettersen, C.A (1999) Higher Education and Teacher Induction: The Role of Higher Education and the Residency Programme in Oklahoma. Unpublished

- Dissertation Abstracts International, 60 (4), October, pp. 964-A, 965-A.

- Phillips, P.J. (2002) A Case Study of the Efficacy of Human Resource Managers Serving as Change Agents. Unpublished Dissertation Abstracts International, 62(12), June, p.4352-A.

- Porter M.E. (1990) The Competitive Advantage of Nations Macmillan Press Ltd. London

- Prokopenko, J. (1987). Productivity management: A practical handbook. Geneva: International Labor Organization.261

- Rai U.K. (1996) Teacher and Human Resource Development. University News, October. Pp.6, 7.

- Raja, M. (2005). Globalization and Education : Need for Curriculum for Lifelong Learning Programs. The Indian Scene. Pp. 1-8. www.boloji.com. Retrieved on October 26, 2005.

- Rajaram, M. (2000) Towards Quality in Education Administration. New Delhi: Nobel Publishers.

- Rao P.S & Rao V.S.P (1990) Personal / Human Resource Management. Text, Cases and Games. New Delhi: National HRD Network Office.