# CYCLIC GROUP

*A project submitted*

*by*

**LAXMI PRIYA MOHANTY**

*in partial fulfillment of the requirements*
*for the award of the degree of*

**BACHELOR OF SCIENCE**
**IN**
**MATHEMATICS**

**2022**

*DEPARTMENT OF MATHEMATICS*
*NILAMANI MAHAVIDYALAYA,RUPSA,*
*BALESORE, ODISHA-756028*

DEDICATED TO
MY
BELOVED PARENTS

# PROJECT CERTIFICATE

This is to certify that the project entitled **CYCLIC GROUP** submitted by **Laxmipriya Mohanty** to Nilamani mahavidyalaya, Rupsa for the partial fulfilment of the requirements of B.Sc degree in Mathematics is a bonafides record of review work carried out by him under my supervision and guidance.


Sambhunath Giri
Department of Mathematics
Nilamani Mahavidyalaya, Rupsa
Balasore, Odisha
India-756028


Sambhunath Giri
23.6.22.

Gopinath Swain (Retired)
23.06.22

93/100

# DECLARATION

I hereby declare that the work on the topic **CYCLIC GROUP** for my B.Sc. degree has been carried out by me in the Department of Mathematics, Nilamani Mahavidyalaya, Rupsa and further declare that it has not been submitted earlier wholly or in part to any other Institution or University for the award of any other degree or diploma.

Laxmipriya Mohanty
Roll No:- 5608B19007
Regd. No:- 02726/19

Place- Rupsa, Balasore
Date:- 23.06.2022

# ACKNOWLEDGEMENT

I respect and thank **Sambhunath Giri** for giving me an opportunity to do the project work and providing me all support and guidance which made me complete the project on time. The project would not have been possible without his help and the valuable time that he gave me in spite of his busy schedule.

I would also like to extend my gratitude and hearty thank to my teachers of the department for their able guidance, constant encouragement and co-operation during my studentship in the department. I shall remain indebted to them forever.

I am very much oblige to my loving parents and my family members for their continuous inspiration and sacrifice without which it would not have been possible to see these nice academic days.

Last but not least I would like to thank my friends, seniors and juniors who have been very cooperative with me and have helped me in completing my project.

Rupsa,756028
June,2022

Laxmipriya Mohanty

# CONTENTS

In algebra a cyclic group or homogenous group is a group that is generated by a single element that is

It consists of a set of element with a single invertible associative operation and it contains an element g such that every other element. of the group may be obtained by repeatedly applying the group operation or it invers to g. Each element can be written as a power of g in multiplicative notation, or as a multiple of g in additive notation. This element g is called a generator of the group.

Every infinite cycle group is isomorphic the additive group of z, the integers every finite cyclic group of order n is integers. Every finite cyclic group of order n is isomorphic to the additive group of Z/nZ, the integers modulo n.

Every cyclic group is an abelian group (meaning that it's group operation is commutative) and every finitely generator abelian group is a direct product of cyclic group.

# Preliminary

## Group

A group is a set, $G$, together with an operation $\bullet$ (called the *group law* of $G$) that combines any two elements $a$ and $b$ to form another element, denoted $a \bullet b$ or $ab$. To qualify as a group, the set and operation, $(G, \bullet)$, must satisfy four requirements known as the *group axioms*:

**Closure**

For all $a$, $b$ in $G$, the result of the operation, $a \bullet b$, is also in $G$.

**Associativity**

For all $a$, $b$ and $c$ in $G$, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

**Identity element**

There exists an element $e$ in $G$ such that, for every element $a$ in $G$, the equation $e \bullet a = a \bullet e = a$ holds. Such an element is unique (see below), and thus one speaks of *the* identity element.

**Inverse element**

For each $a$ in $G$, there exists an element $b$ in $G$, commonly denoted $a^{-1}$ (or $-a$, if the operation is denoted "+"), such that $a \bullet b = b \bullet a = e$, where $e$ is the identity element.

The result of an operation may depend on the order of the operands. In other words, the result of combining element $a$ with element $b$ need not yield the same result as combining element $b$ with element $a$; the equation

$$a \bullet b = b \bullet a$$

may not always be true. This equation always holds in the group of integers under addition, because $a + b = b + a$ for any two integers (commutativity of addition). Groups for which the

commutativity equation $a \bullet b = b \bullet a$ always holds are called abelian groups (in honor of Niels Henrik Abel). The symmetry group described in the following section is an example of a group that is not abelian.

The identity element of a group $G$ is often written as 1 or $1_G$, a notation inherited from the multiplicative_identity. If a group is abelian, then one may choose to denote the group operation by + and the identity element by 0; in that case, the group is called an additive group. The identity element can also be written as *id*.

The set $G$ is called the *underlying set* of the group $(G, \bullet)$. Often the group's underlying set $G$ is used as a short name for the group $(G, \bullet)$. Along the same lines, shorthand expressions such as "a subset of the group $G$" or "an element of group $G$" are used when what is actually meant is "a subset of the underlying set $G$ of the group $(G, \bullet)$" or "an element of the underlying set $G$ of the group $(G, \bullet)$". Usually, it is clear from the context whether a symbol like $G$ refers to a group or to an underlying set.

An alternate (but equivalent) definition is to expand the structure of a group to define a group as a set equipped with three operations satisfying the same axioms as above, with the "there exists" part removed in the two last axioms, these operations being the group law, as above, which is a binary operation, the *inverse operation*, which is a unary operation and maps $a$ to $a^{-1}$, and the identity element, which is viewed as a O-ary operation.

As this formulation of the definition avoids existential quantifiers, it is generally preferred for computing with groups and for computer-aided proofs. This formulation exhibits groups as a variety of universal algebra. It is also useful for talking of properties of the inverse operation, as needed for defining topological groups and group objects.

## Subgroup

In group theory, a branch of mathematics, given a group $G$ under a binary operation $*$, a subset $H$ of $G$ is called a **subgroup** of $G$ if $H$ also forms a group under the operation $*$. More precisely, $H$ is a subgroup of $G$ if the restriction of $*$ to $H \times H$ is a group operation on $H$. This is usually denoted $H \leq G$, read as "$H$ is a subgroup of $G$".

### Example Subgroups of $Z_8$

Let $G$ be the cyclic group $Z_8$ whose elements are

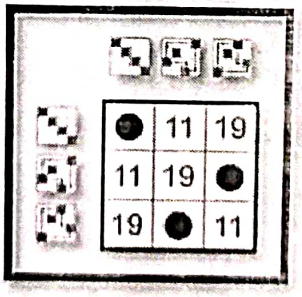
and whose group operation is addition modulo eight. Its Cayley table is

| + | 0 | 2 | 4 | 6 | 1 | 3 | 5 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 4 | 6 | 1 | 3 | 5 | 7 |

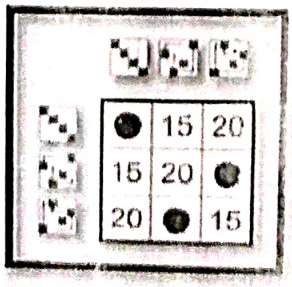
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **2** | 2 | 4 | 6 | 0 | 3 | 5 | 7 | 1 |
| **4** | 4 | 6 | 0 | 2 | 5 | 7 | 1 | 3 |
| **6** | 6 | 0 | 2 | 4 | 7 | 1 | 3 | 5 |
| **1** | 1 | 3 | 5 | 7 | 2 | 4 | 6 | 0 |
| **3** | 3 | 5 | 7 | 1 | 4 | 6 | 0 | 2 |
| **5** | 5 | 7 | 1 | 3 | 6 | 0 | 2 | 4 |
| **7** | 7 | 1 | 3 | 5 | 0 | 2 | 4 | 6 |

This group has two nontrivial subgroups: $J=\{0,4\}$ and $H=\{0,2,4,6\}$, where $J$ is also a subgroup of $H$. The Cayley table for $H$ is the top-left quadrant of the Cayley table for $G$. The group $G$ is cyclic, and so are its subgroups. In general, subgroups of cyclic groups are also cyclic.

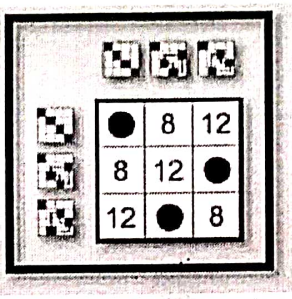
Cyclic group $Z_3$




Cyclic group $Z_3$




Cyclic group $Z_3$




## Subgroup and notation

All subgroups and quotient groups of cyclic groups are cyclic. Specifically, all subgroups of **Z** are of the form $m\mathbf{Z}$, with $m$ an integer ≥0. All of these subgroups are distinct from each other, and apart from the trivial group (for $m = 0$) all are isomorphic to **Z**. The lattice of subgroups of **Z** is isomorphic to the dual of the lattice of natural numbers ordered by divisibility. In particular, because the prime numbers are the numbers with no nontrivial divisors, a cyclic group is simple if and only if its order (the number of its elements) is prime.

Since the cyclic groups are abelian, they are often written additively and denoted $Z_n$ with the identity written 0. 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 $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}/(n)$, and $\mathbf{Z}/n$ are often-used alternatives.

One may instead write the group multiplicatively, and denote it by $C_n$, where $n$ is the order for finite groups and by C for the infinite cyclic group. For example, $g^2g^4 = g^1$ in $C_5$, whereas $2 + 4 = 1$ in $\mathbf{Z}/5\mathbf{Z}$.

All quotient groups of **Z** are finite, with the exception $\mathbf{Z}/0\mathbf{Z} = \mathbf{Z}/\{0\}$. For every positive divisor $d$ of $n$, the quotient group $\mathbf{Z}/n\mathbf{Z}$ has precisely one subgroup of order $d$, the one generated by the residue class of $n/d$. There are no other subgroups. Using the quotient group formalism, $\mathbf{Z}/n\mathbf{Z}$ is a standard notation for the additive cyclic group with $n$ elements. In ring terminology, the subgroup $n\mathbf{Z}$ is also the ideal $(n)$, so the quotient can also be written $\mathbf{Z}/(n)$ without abuse of notation. These alternatives do not conflict with the notation for the $p$-adic integers. The notation $\mathbf{Z}/n$ is common in informal calculations.

## Normal subgroup

A subgroup $N$ of a group $G$ is called a **normal subgroup** if it is invariant under conjugation; that is, the conjugation of an element of $N$ by an element of $G$ is always in $N$. The usual notation for this relation is **N**, and the definition may be written in symbols as

$$N \triangleleft G \Leftrightarrow \forall n \in N, \forall g \in G: gng^{-1} \in N.$$

For any subgroup, the following conditions are equivalent to normality. Therefore, any one of them may be taken as the definition:

- Any two elements commute regarding the normal subgroup membership relation: $\forall g, h \in G, gh \in N \Leftrightarrow hg \in N$.
- The image of conjugation of $N$ by any element of $G$ is a subset of $N$: $\forall g \in G, gNg^{-1} \subseteq N$.
- The image of conjugation of $N$ by any element of $G$ is $N$: $\forall g \in G, gNg^{-1} = N$.
- $\forall g \in G, gN = Ng$.
- The sets of left and right cosets of $N$ in $G$ coincide.
- The product of an element of the left coset of $N$ with respect to $g$ and an element of the left coset of $N$ with respect to $h$ is an element of the left coset of $N$ with respect to $gh$: $\forall x, y, g, h \in G, x \in gN$ and $y \in hN \Rightarrow xy \in (gh)N$.
- $N$ is a union of conjugacy classes of $G$: $N = \bigcup_{g \in N} \mathrm{Cl}(g)$.
- $N$ is preserved by inner automorphisms.
- There is some homomorphism on $G$ for which $N$ is the kernel: $\exists \phi \in \mathrm{Hom}(G) \mid \ker \phi = N$.

The last condition accounts for some of the importance of normal subgroups; they are a way to internally classify all homomorphisms defined on a group. For example, a non-identity finite group is simple if and only if it is isomorphic to all of its non-identity homomorphic images, a finite group is perfect if and only if it has no normal subgroups of prime index, and a group is imperfect if and only if the derived subgroupis not supplemented by any proper normal subgroup.

## Example

- The subgroup $\{e\}$ consisting of just the identity element of $G$ and $G$ itself are always normal subgroups of $G$. The former is called the trivial subgroup, and if these are the only normal subgroups, then $G$ is said to be simple.
- The center of a group is a normal subgroup.
- The commutator subgroup is a normal subgroup.
- More generally, any characteristic subgroup is normal, since conjugation is always an automorphism.
- Every subgroup $N$ of an abelian group $G$ is normal, because $gN = Ng$. A group that is not abelian but for which every subgroup is normal is called a Hamiltonian group.
- The translation group is a normal subgroup of the Euclidean group in any dimension.
- In the Rubik's Cube group, the subgroups consisting of operations which only affect the orientations of either the corner pieces or the edge pieces are normal.

## Definition

A group G is called cyclic if there exists an element g in G such that

$G = \langle g \rangle = \{ g^n \mid n \text{ is an integer} \}$

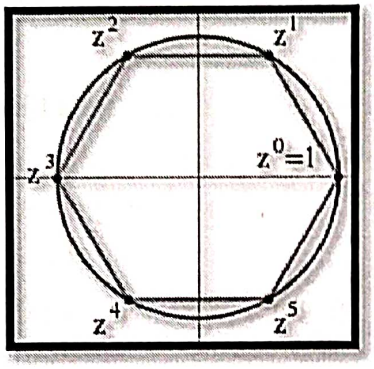
Or $G=\{a^n/n \in z\}$

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 of order 6, 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 $\chi$ defined by $\chi(g^i) = i$.

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 thought of as having one infinitely long cycle.) A group generated in this way (for example, the first frieze group, p1) is called an **infinite cyclic group**, and is isomorphic to the additive group of the integers, $(\mathbf{Z}, +)$.

The collection of French mathematicians publishing under the name Nicolas Bourbaki introduced the term **monogenous group** for a group admitting a system of generators consisting of a single element and restricted the term "cyclic group" to mean only finite monogenous groups, avoiding the term "infinite cyclic group".




The six 6th complex roots of unity form a cyclic group under multiplication. $Z$ is a primitive element, but $z^2$is not, because the odd powers of $z$ are not a power of $z^2$.

# Example

## Integer and modular addition

The set of integers, with the operation of addition, forms a group. It is an **infinite cyclic group**, because all integers can be written as a finite sum or difference of copies of the number 1. In this group, 1 and −1 are the only generators. Every infinite cyclic group is isomorphic to this group.

For every positive integer $n$, the set of integers modulo $n$, again with the operation of addition, forms a finite cyclic group, the group $\mathbf{Z}/(n)$. An element $g$ is a generator of this group if $g$ is relatively prime to $n$ (because these elements can generate all other elements of the group through integer multiplication). Thus, the number of different generators is $\varphi(n)$, where $\varphi$ is the Euler totient function, the function that counts the number of numbers modulo $n$ that are relatively prime to $n$. Every finite cyclic group is isomorphic to a group $\mathbf{Z}/(n)$, where $n$ is the order of the group.

The integer and modular addition operations, used to define the cyclic groups, are both the addition operations of commutative rings, also denoted $\mathbf{Z}$ and $\mathbf{Z}/(n)$. If $p$ is a prime, then $\mathbf{Z}/(p)$ is a finite field, and is usually instead written as $\mathbf{F}_p$ or $\mathrm{GF}(p)$. Every field with $p$ elements is isomorphic to this one.

## Modular multiplication

For every positive integer $n$, the subset of the integers modulo $n$ that are relatively prime to $n$, with the operation of multiplication, forms a finite group that for many values of $n$ is again cyclic. It is the group under multiplication modulo $n$, and it is cyclic whenever $n$ is 1, 2, 4, a power of an odd prime, or twice a power of an odd prime. Its elements are the units of the ring $\mathbf{Z}/n\mathbf{Z}$; there are $\varphi(n)$ of them, where again $\varphi$ is the totient function. This group is written as $(\mathbf{Z}/n\mathbf{Z})^\times$. For example, $(\mathbf{Z}/6\mathbf{Z})^\times$ has as its elements $\{1,5\}$; 6 is twice a prime, so this is a cyclic group. In contrast, $(\mathbf{Z}/8\mathbf{Z})^\times$ (with elements $\{1,3,5,7\}$) is the Klein group and is not cyclic. When $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic, every generator (through exponentiation) of $(\mathbf{Z}/n\mathbf{Z})^\times$ is called a primitive root modulo $n$.

The cyclic group $(\mathbf{Z}/p\mathbf{Z})^\times$ for a prime number $p$, is also written $(\mathbf{Z}/p\mathbf{Z})^*$ because it consists of the non-zero elements of the finite field of order $p$. More generally, every finite subgroup of the multiplicative group of any field is cyclic.

## Rotational symmetries

The set of rotational symmetries of a polygon forms a finite cyclic group.[7] If there are $n$ different ways of mapping the polygon to itself by a rotation (including the null rotation) then this group is isomorphic to $Z_n$. In three or higher dimensions there can exist other finite symmetry groups that are cyclic, but that do not form the set of rotations around a single axis.

The group $S^1$ of all rotations of a circle (the circle group) is *not* cyclic. Unlike the infinite cyclic group, it is not even countable. There also exist other infinite rotation groups (such as the set of rotations by rational angles) that are countable but not cyclic.

## Galois theory

An $n$th root of unity may be thought of as a complex number whose $n$th power is 1. That is, it is a root of the polynomial $x^n - 1$. The $n$th roots of unity form a cyclic group of order $n$ under multiplication. For example, the polynomial $0 = z^3 - 1$ factors as $(z - s^0)(z - s^1)(z - s^2)$, where $s = e^{2\pi i/3}$; the set $\{s^0, s^1, s^2\}$ forms a cyclic group under multiplication. The Galois group of the field extension of the rational numbers generated by the $n$th roots of unity forms a different group. It is isomorphic to the multiplicative group modulo $n$, which has order $\phi(n)$ and is cyclic for some but not all $n$.

A field extension is called a cyclic extension if its Galois group is a cyclic group. The Galois group of every finite extension of a finite field is finite and cyclic, with an iterate of the Frobenius endomorphism as its generator. Conversely, given a finite field $F$ and a finite cyclic group $G$, there is a finite field extension of $F$ whose Galois group is $G$.

# Subgroups of cyclic groups

In abstract algebra, every subgroup of a cyclic group is cyclic. Moreover, for a finite cyclic group of order $n$, every subgroup's order is a divisor of $n$, and there is exactly one subgroup for each divisor. This result has been called the fundamental theorem of cyclic groups.

## Finite cyclic groups

For every finite group $G$ of order $n$, the following statements are equivalent:

- $G$ is cyclic.
- For every divisor $d$ of $n$, $G$ has exactly one subgroup of order $d$.
- For every divisor $d$ of $n$, $G$ has at most one subgroup of order $d$.

This statement is known by various names such as **characterization by subgroups**. (See also cyclic group for some characterization.)

There exist finite groups other than cyclic groups with the property that all proper subgroups are cyclic; the Klein group is an example. However, the Klein group has more than one subgroup of order 2, so it does not meet the conditions of the characterization.

## The infinite cyclic group

The infinite cyclic group is isomorphic to the additive subgroup $\mathbf{Z}$ of the integers. There is one subgroup $d\mathbf{Z}$ for each integer $d$ (consisting of the multiples of $d$), and with the exception of the trivial group (generated by $d = 0$) every such subgroup is itself an infinite cyclic group. Because the infinite cyclic group is a free group on one generator (and the trivial group is a free group on no generators), this result can be seen as a special case of the Nielsen–Schreier theorem that every subgroup of a free group is itself free.

The fundamental theorem for finite cyclic groups can be established from the same theorem for the infinite cyclic groups, by viewing each finite cyclic group as a quotient group of the infinite cyclic group.

## Lattice of subgroups

In both the finite and the infinite case, the lattice of subgroups of a cyclic group is isomorphic to the dual of a divisibility lattice. In the finite case, the lattice of subgroups of a cyclic group of order $n$ is isomorphic to the dual of the lattice of divisors of $n$, with a subgroup of order $n/d$ for each divisor $d$. The subgroup of order $n/d$ is a subgroup of the subgroup of order $n/e$ if and only if $e$ is a divisor of $d$. The lattice of subgroups of the infinite cyclic group can be described in the same way, as the dual of the divisibility lattice of all positive integers. If the infinite cyclic group is represented as the additive group on the integers, then the subgroup generated by $d$ is a subgroup of the subgroup generated by $e$ if and only if $e$ is a divisor of $d$.

Divisibility lattices are distributive lattices, and therefore so are the lattices of subgroups of cyclic groups. This provides another alternative characterization of the finite cyclic groups: they are exactly the finite groups whose lattices of subgroups are distributive. More

generally, a finitely generated group is cyclic if and only if its lattice of subgroups is distributive and an arbitrary group is locally cyclic if and only its lattice of subgroups is distributive. The additive group of the rational numbers provides an example of a group that is locally cyclic, and that has a distributive lattice of subgroups, but that is not itself cyclic.

# Additional properties

Every cyclic group is abelian. That is, its group operation is commutative: $gh = hg$ (for all $g$ and $h$ in $G$). This is clear for the groups of integer and modular addition since $r + s \equiv s + r \pmod{n}$, and it follows for all cyclic groups since they are all isomorphic to a group generated by an addition operation. For a finite cyclic group of order $n$, and every element $e$ of the group, $e^n$ is the identity element of the group. This again follows by using the isomorphism to modular addition, since $kn \equiv 0 \pmod{n}$ for every integer $k$.

If $d$ is a divisor of $n$, then the number of elements in $\mathbf{Z}/n$ which have order $d$ is $\varphi(d)$, and the number of elements whose order divides $d$ is exactly $d$. If $G$ is a finite group in which, for each $n > 0$, $G$ contains at most $n$ elements of order dividing $n$, then $G$ must be cyclic. The order of an element $m$ of the group is $n/\gcd(n,m)$.

The direct product of two cyclic groups $\mathbf{Z}/n$ and $\mathbf{Z}/m$ is cyclic if and only if $n$ and $m$ are coprime. Thus e.g. $\mathbf{Z}/12$ is the direct product of $\mathbf{Z}/3$ and $\mathbf{Z}/4$, but not the direct product of $\mathbf{Z}/6$ and $\mathbf{Z}/2$. If $p$ is a prime number, then the only group (up to isomorphism) with $p$ elements is $\mathbf{Z}/p$. it is called a primary cyclic group. 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. A number $n$ is called a cyclic number if it has the property that $\mathbf{Z}/n$ is the only group of order $n$, which is true exactly when $\gcd(n,\varphi(n)) = 1$. The cyclic numbers include all prime numbers, but also include some composite numbers such as 15. However, except 2, all cyclic numbers are odd. The cyclic numbers are:

1, 2, 3, 5, 7, 11, 13, 15, 17, 19, 23, 29, 31, 33, 35, 37, 41, 43, 47, 51, 53, 59, 61, 65, 67, 69, 71, 73, 77, 79, 83, 85, 87, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 123, 127, 131, 133, 137, 139, 141, 143, ...

In fact, a number $n$ is a cyclic number if and only if $\gcd(n, \varphi(n)) = 1$, where $\varphi$ is the Euler's totient function.

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 $n$.

# Associated objects

## Representation

The representation theory of the cyclic group is a critical base case for the representation theory of more general finite groups. In the complex case, a representation of a cyclic group decomposes into a direct sum of linear characters, making the connection between character theory and representation theory transparent. In the positive

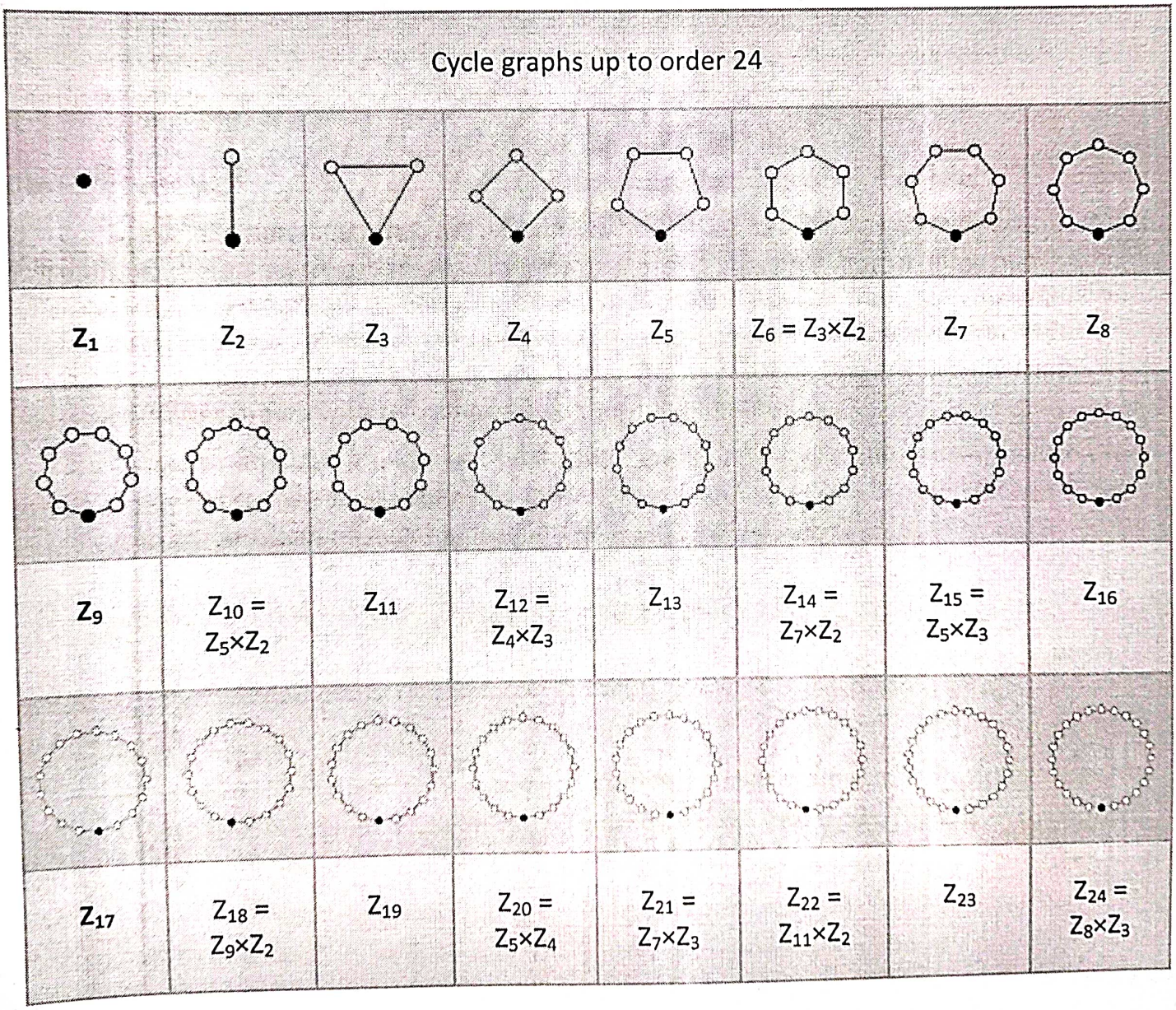
characteristic case, the indecomposable representations of the cyclic group form a model and inductive basis for the representation theory of groups with cyclic Sylow subgroups and more generally the representation theory of blocks of cyclic defect.

## Cycle graph

A **cycle graph** illustrates the various cycles of a group and is particularly useful in visualizing the structure of small finite groups. A cycle graph for a cyclic group is simply a circular graph, where the group order is equal to the number of nodes. A single generator defines the group as a directional path on the graph, and the inverse generator defines a backwards path. Trivial paths (identity) can be drawn as a loop but are usually suppressed. $Z_2$ is sometimes drawn with two curved edges as a multigraph.

Cyclic groups $Z_n$, order $n$, is a single cycle graphed simply as an $n$-sided polygon with the elements at the vertices. When $n = ab$ with $a$ and $b$ being relatively prime (i.e., $\gcd(a, b) = 1$), a cyclic group $Z_n$ can be decomposed into a direct product $Z_a \times Z_b$.

Cycle graphs up to order 24



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $Z_1$ | $Z_2$ | $Z_3$ | $Z_4$ | $Z_5$ | $Z_6 = Z_3 \times Z_2$ | $Z_7$ | $Z_8$ |
| $Z_9$ | $Z_{10} = Z_5 \times Z_2$ | $Z_{11}$ | $Z_{12} = Z_4 \times Z_3$ | $Z_{13}$ | $Z_{14} = Z_7 \times Z_2$ | $Z_{15} = Z_5 \times Z_3$ | $Z_{16}$ |
| $Z_{17}$ | $Z_{18} = Z_9 \times Z_2$ | $Z_{19}$ | $Z_{20} = Z_5 \times Z_4$ | $Z_{21} = Z_7 \times Z_3$ | $Z_{22} = Z_{11} \times Z_2$ | $Z_{23}$ | $Z_{24} = Z_8 \times Z_3$ |

## Cayley graph

A Cayley graph is a graph defined from a pair $(G,S)$ where $G$ is a group and $S$ is a set of generators for the group; it has a vertex for each group element, and an edge for each

product of an element with a generator. In the case of a finite cyclic group, with its single generator, the Cayley graph is a cycle graph, and for an infinite cyclic group with its generator the Cayley graph is a doubly infinite path graph. However, Cayley graphs can be defined from other sets of generators as well. The Cayley graphs of cyclic groups with arbitrary generator sets are called circulant graphs. These graphs may be represented geometrically as a set of equally spaced points on a circle or on a line, with each point connected to neighbors with the same set of distances as each other point. They are exactly the vertex- transitive graphs whose symmetry group includes a transitive cyclic group.

## Endomorphisms

The endomorphism ring of the abelian group $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ itself as a ring. Under this isomorphism, the number $r$ corresponds to the endomorphism of $\mathbf{Z}/n\mathbf{Z}$ that maps each element to the sum of $r$ copies of it. This is a bijection if and only if $r$ is coprime with $n$, so the automorphism group of $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to the unit group $(\mathbf{Z}/n\mathbf{Z})^{\times}$.

Similarly, the endomorphism ring of the additive group of $\mathbf{Z}$ is isomorphic to the ring $\mathbf{Z}$. Its automorphism group is isomorphic to the group of units of the ring $\mathbf{Z}$, i.e. to $(\{-1, +1\}, \times) \cong C_2$.

## Tensor product and hom of cyclic groups

The tensor product Z/mZ  Z/nZ and the group of homeomorphisms hom(Z/mZ, Z/nZ) can be show to both be isomorphic to Z/gcd (m,n)Z.

For the tender product, this is a consequence of the general fact.

R/I  R/J . for the Hom group, recall that it is isomorphic to the subgroup of Z/nZ consisting of the element of orders dividing of M. that subgroup is cyclic subgroup is cyclic order gcd(m,n) which completes the proof.

# Related classes of subgroups

Several other classes of groups have been defined by their relation to the cyclic groups:

## Virtually cyclic groups

A group is called **virtually cyclic** if it contains a cyclic subgroup of finite index (the number of cosets that the subgroup has). In other words, any element in a virtually cyclic group can be arrived at by applying a member of the cyclic subgroup to a member in a certain finite set. Every cyclic group is virtually cyclic, as is every finite group. An infinite group is virtually cyclic if and only if it is finitely generated and has exactly two ends; an example of such a group is the product of $\mathbf{Z}/(n)$ and $\mathbf{Z}$, in which the factor $\mathbf{Z}$ has finite index $n$. Every abelian subgroup of a Gromov hyperbolic group is virtually cyclic.

## Locally cyclic groups

A cyclically ordered group is a group together with a cyclic order preserved by the group structure. Every cyclic group can be given a structure as a cyclically ordered group, consistent with the ordering of the integers (or the integers modulo the order of the group). Every finite subgroup of a cyclically ordered group is cyclic.

## Metacyclic and polycyclic groups

A metacyclic group is a group containing a cyclic normal subgroup whose quotient is also cyclic. These groups include the cyclic groups, the dicyclic groups, and the direct products of two cyclic groups. The polycyclic groups generalize metacyclic groups by allowing more than one level of group extension. A group is polycyclic if it has a finite descending sequence of subgroups, each of which is normal in the previous subgroup with a cyclic quotient, ending in the trivial group. Every finitely generated Abelian group or nilpotent group is polycyclic.

# Application

## Theorem 4.1

Let g be a group, and let a belong to G. if a has infinite order, then all distinct powders of a are distinct group element. if a has finite order, say, n, then $\langle a\rangle=\{e, a, a^2, \ldots\ldots, a^{n-1}\}$ and $a^i=a^j$ if and only if n divides i – j.

## proof

If has infinite order, there is no nonzero n such that $a^n$ is the identity. Since $a^i = a^j$ implies $a^{i-j} = e$, we must have i – j = 0, and the statement of the theorem is proved.

Now assume that |a| = n. we will proved that $\langle a\rangle = \{e, a, \ldots\ldots, a^{n-1}\}$. Certainly, the elements $e, a, \ldots\ldots, a^{n-1}$ distinct. For if $a^i = a^j$ with $0 < i < j < n-1$, then $a^{i-j} = e$. but this contradicts the fact that least positive integer such that an is the identity.

Now suppose that $a^k$ is an arbitrary member of $\langle a\rangle$. by the division algorithm, there exist integers q and r such that

$$K=qn + r \text{ with } 0< r <n.$$

Then $a^n = a^{qn+r} = a^{qn} \cdot a^r = e \cdot a^r = a^r$, show that $ak \in \{e, a, a^2, \ldots\ldots\ldots, a^{n-1}\}$. This proves that $\langle a\rangle = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$.

Next we assume that $a^i = a^j$ and prove that n divides i – j. we begin by observing that $a^i = a^j$ implies $a^{i-j} = e$. again, by the division algorithm, there are integers q and r such that

$i - j = qn + r$ with $0 < r < n$.

then $a^{i-j} = a^{qn+r}$ and, therefore, $e = ea^r = a^r$. since n is the least positive integer such that $a^n$ is the identity, we must have $r = 0$ so that n divides $i - j$.

conversely, if n divides $i - j$, then $a^{i-j} = a^{nq} = e^q = e$ so that $a^i = a^j$.

one special case of theorem 4.1 occurs so often it deserves singling out.

## Theorem 4.1.1

Let G be a group and let a bed an element of order n in G. If $a^k = e$, then n divides k.

## Proof

Since $a^k = e = a^0$, we know by theorem 4.1 that n divides $k - 0$.

Theorem 4.1and its corollary for the case $|a| = 6$ are illustrated in figure 4.1.

What is important about theorem 4.1 in the finite case is that it say that multiplication in <a> is essentially done by addition modulo n. that is, or how the element a is chosen , multiplication in <a> works the same as addition in Zn whenever $|a| = n$. similarly, if a has infinite order, then multiplication in <a> work the same as addition in Z,since $a^i.a^j = a^{i+}a^j$and no modular arithmetic is done.

For these reason, the cyclic group Zn and Z serve as prototypes for all cyclic groups, and algebraists say that there is essentially only one cyclic group of each order. What is meant by this is that, although there may be many different sets of the from $\{a^n | n \in Z\}$, there is essentially only one way to operate on these sets, depending on the order of a. Algebraists do not really care what the elements of a set are; they care only about the algebraic properties of the set-that is, the ways the elements of a set can be combined. We will return to this theme in the chapter on isomorphism.

In Example 3, we saw that 3 was a generator for $Z_8$ whereas 2 was not. Similarly, 3 and 7 are generators for U(10) whereas 9 is not. It would be nice to be able to "eyeball" the generators for $Z_n$ and for cyclic groups in general. Theorem 4.2 and its corollary give us a simple arithmetic method for identifying generators.

## Theorem 4.2 generator of cyclic groups

Let G= <a> be a cyclic group of order n. then $G=\langle a^k \rangle$ if and only if gcd (k, n)= 1.

## Proof

If gcd(k,n)=1, we may write 1 = ku + nv for some integers u and v. Then $a= a^{ku+nv}= a^{ku} . a^{nv} = a^{ku}$. Thus, a belongs to $<a^k>$ and therefor all power of a belongs to $<a^k>$. So, $G= <a^k>$ and $a^k$ is a generator of G.

Now suppose that gcd(k,n) = d>1. Write k =td and n = sd. Then $(a^k)^s = (a^{td})^s =(a^{sd})^t =(a^n)^t = e$, so that $|a^k|< s < n$. this is shows that $a^k$ is not generator of G.

Taking $G =Z_n$ and a = 1 in theorem 4.2, we have the following useful result.

## Theorem 4.3 fundamental theorem of cyclic group

Every subgroup of a cyclic group is cyclic. Moreover, if $|<a>| = n$, then the order of any subgroup of $<a>$ is a divisor k of n; and, for each positive divisor k of n, the group $<a>$ has exactly one subgroup of order k- namely, $<a^{n/k}>$.

## Proof

Let $G = <a>$ and suppose that H is subgroup of G. we must show that H is cyclic. If it consist of the identity alone, then clearly H is cyclic. So we may assume that $H \neq \{e\}$. we now claim that H contains an element of the form $a^t$, where t is positive. Since $= <a>$, every element of H has the form $a^t$; and when $a^t$ belongs to H with $t < 0$, then $a^{-t}$ belongs to H also and –t is positive. Thus, our claim is verified. Now let m be the least positive integer such that $a^m \in H$. By closer, $<a^m> \leq H$. we next claim that $H = <a^m>$. to prove this claim, it suffices to let b be an arbitrary member of H and show that b is in $<a^m>$. since $b \in G = <a>$, we have $b = a^k$ for some k. now, apply the division algorithm to k and m to obtain integers q and r such that = mq + r where $o \leq r < m$. then $a^k =a^{mq+r} = a^{mq} . a^r$ so that $a^r = a^{-mq}a^k$. since $a^k = b \in H$, and $a^{-mq} = (a^m)^{-q}$ is in H also, $a^r \in H$. but, m is the least positive integer such that $a^m \in H$, and $0 \leq r <m$, so r must be 0. Thus, $a^{-mq}a^k = e$, and therefore $b = a^k = a^{mq} = (a^m)^q \in <a^m>$. this proves the assertion of the theorem that every subgroup of a cyclic group is cyclic.

To prove the next portion of the theorem, suppose that $|<a>| =n$ and H is any subgroup of $<a>$. we have already show that $H = <a^m>$ for some m. and, since $(a^m)^n = e^m = e$, we know from corollary to theorem 4.1 that $|a^m|$ is divisor of n. thus, $|H|=|a^m|$ is a divider of n.

Finally let k be any divisor of n. clearly, $(a^{n/k})^k = a^n = e$ and $(a^{n/k})^t \neq e$ for any positive $t < k$, so $<a^{n/k}>$ has order k. we next show that $<a^{n/k}>$ is only the subgroup of order k. to this end, let H be any subgroup of order k. we have previously show that $H = <a^m>$, where m is the least positive integer such that $a^m$ is in H. now, writing n = mq+r, where $0 \leq r < m$, we have $e = a^n = a^{mq+r} = a^{mq} . a^r$ so that $a^r = a^{-mq} = (a^m)^{-q} \in H$. thus, r = 0 and n = mq. So, $k = |H| =|<a^m>| = n/m$. it follows that m = n/k and $H = <a^m> = <a^{n/k}>$.

## Theorem 4.4 number of elements of each order in a cyclic group

If d is a positive divider of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

## Proof

By theorem 4.3, there is exactly one subgroup of order d call it <a>. then every element of order d also generates the subgroup <a> and by theorem 4.2, an element $a^k$ generates <a> if and only if gcd(k,d) = 1. The number of such elements is precisely $\phi(d)$.

# The cycle notation for permutation

The cycle notation has theoretical advantage in that certain important properties of the permutation can be readily defined when cycle notation is used.

## Example

1. A cycle notation for the permutation is

$$\alpha = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{matrix}$$

This notation can also be written as $\alpha = (1,2)\ (3,4,6)\ (5)$

Note

We can multiply cycles by thinking of them as permutation given in array form.

Note

One many not prefor to write cycles that have only one entry. In this case it is understood that any missing element is mode to itself.

Properties of permutation

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycle.

## Proof

Let $\alpha$ be a permutation on.

$A = \{1,2,3,4,.....,n\}$

Let $\alpha$ is written in the disjoint cycle form. So we shall start by choosing any member of A as $a_1$.

So

$a_2 = \alpha(a_1)$

$a_3 = \alpha(a_2) = \alpha(\alpha(a_1)) = \alpha^2(a_1)$

$a_4 = \alpha(a_3) = \alpha(\alpha^2(a_1)) = \alpha^3(a_1)$

And so on

The process will continue until we arrived at $a_1 = \alpha^m(a_1)$ for some integer m. here m will exist because the sequence $a_1$, $\alpha(a_1)$, $\alpha^2(a_1)$, ..... Must be finite. So there are finitely many term with infinite number of repetition so there exist two positive integer i & j with i<j s.t $\alpha^i(a_1)=\alpha^j(a_1)$

$\alpha^m(a_1) = a_1$

That is there exist a cycle which end at $a_m$.

The three dotes at the end indicate the possibility that we may not have exhausted the set a in this proses. Similarly we can chose another element $B_1(a)$ not appearing in first cycle and by similar proses we proceed and obtained another cycle of $\alpha$ that is $(B_1,B_2,B_3,.....,B_k)$ containing this proses until we run out the element of A. hence our permutation can be expression as the product of disjoint cycle such as $\alpha = (a_1,a_2,.....,a_m)(b_1,b_2,.....,b_k).....(c_1,c_2,.....,c_n)$.

# Group action

In the above example of the symmetry group of a square, the permutations "describe" the movement of the vertices of the square induced by the group of symmetries. It is common to say that these group elements are "acting" on the set of vertices of the square. This idea can be made precise by formally defining a **group action**.

Let *G* be a group and *M* a nonempty set. An **action** of *G* on *M* is a function $f: G \times M \to M$ such that

$f(1, x) = x$, for all *x* in *M* (1 is the identity (neutral) element of the group *G*), and

$f(g, f(h, x)) = f(gh, x)$, for all *g*,*h* in *G* and all *x* in *M*.

This last condition can also be expressed as saying that the action induces a group homomorphism from *G* into *Sym*(*M*). Any such homomorphism is called a *(permutation) representation* of *G* on *M*.

For any permutation group, the action that sends $(g, x) \to g(x)$ is called the **natural action** of *G* on *M*. This is the action that is assumed unless otherwise indicated. In the example of the symmetry group of the square, the group's action on the set of vertices is the natural action. However, this group also induces an action on the set of four triangles in the square, which are: $t_1 = 234$, $t_2 = 134$, $t_3 = 124$ and $t_4 = 123$. It also acts on the two diagonals: $d_1 = 13$ and $d_2 = 24$.

| Group element | Action on triangles | Action on diagonals |
|---|---|---|

| | | |
|---|---|---|
| (1) | (1) | (1) |
| (1234) | $(t_1\ t_2\ t_3\ t_4)$ | $(d_1\ d_2)$ |
| (13)(24) | $(t_1\ t_3)(t_2\ t_4)$ | (1) |
| (1432) | $(t_1\ t_4\ t_3\ t_2)$ | $(d_1\ d_2)$ |
| (12)(34) | $(t_1\ t_2)(t_3\ t_4)$ | $(d_1\ d_2)$ |
| (14)(23) | $(t_1\ t_4)(t_2\ t_3)$ | $(d_1\ d_2)$ |
| (13) | $(t_1\ t_3)$ | (1) |
| (24) | $(t_2\ t_4)$ | (1) |

# Permutation isomorphic group

If $G$ and $H$ are two permutation groups on sets $X$ and $Y$ with actions $f_1$ and $f_2$ respectively, then we say that $G$ and $H$ are *permutation isomorphic* (isomorphic *as permutation groups*) if there exists a bijective map $\lambda : X \to Y$ and a group isomorphism $\psi : G \to H$ such that:

$\lambda(f_1(g, x)) = f_2(\psi(g), \lambda(x))$ for all $g$ in $G$ and $x$ in $X$.

If $X = Y$ this is equivalent to $G$ and $H$ being conjugate as subgroups of Sym($X$). The special case where $G = H$ and $\psi$ is the identity map gives rise to the concept of *equivalent actions* of a group.

In the example of the symmetries of a square given above, the natural action on the set {1,2,3,4} is equivalent to the action on the triangles. The bijection $\lambda$ between the sets is given by $i \mapsto t_i$. The natural action of group $G_1$ above and its action on itself (via left multiplication) are not equivalent as the natural action has fixed points and the second action does not.

# Bibliography


- *Gallian,* Joseph, *Contemporary* Abstract Algebra *(7th ed.), Cengage Learning,* 2010.