"CYCLIC GROUP"

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirement for the award of the degree of Master of Science in Mathematics

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

NAGAON,ASSAM

Submitted By:

Chayanika Kashyap

Roll No: MAT-04/23

Registration No: MSSV-0023-101-001353

Department of Mathematics MSSV, Nagaon

Under The Guidance:

Dr. Raju Bordoloi, HOD

Department of Mathematics, MSSV, Nagaon

Certificate

This is to certify that the dissertation entitled **" CYCLIC GROUP "**, submitted by **Chayanika Kashyap**, Roll No. **MAT-04/23**, Registration No. **MSSV-0023-101001353**, in partial fulfilment for the award of the degree of **Master of Science in Mathematics**, is a bonafide record of original work carried out under my supervision and guidance.

To the best of my knowledge, the work has not been submitted earlier to any other institution for the award of any degree or diploma.

Dr.Raju Bordoloi
HOD
Department of Mathematics
MAHAPURUSHA SRIMANTA SANKARADEVA VISWAVIDYALAYA

Date: Signature of Guide
Place:

Declaration

I, **CHAYANIKA KASHYAP**, hereby declare that the dissertation titled **"CYCLIC GROUP"**, submitted to the Department of Mathematics, **MAHAPURUSHA SRIMANTA SANKARADEVA VISWAVIDYALAYA**, is a record of original work carried out by me under the supervision of **Dr. Raju Bordoloi**, HOD,Department of Mathematics.

This work has not been submitted earlier to any other institution or university for the award of any degree or diploma.

Place: CHAYANIKA KASHYAP
Date: Roll No.: MAT-04/23

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my guide, **Dr. Raju Bordoloi**, HOD, Department of Mathematics, MAHAPURUSHA SRIMANTA SANKARADEVA VISWAVIDYALAYA for his valuable guidance, continuous support, and encouragement throughout the course of this dissertation.

I also extend my heartfelt thanks to the faculty members of the Department of Mathematics for their constant academic support and the friendly learning environment they provided.

I am deeply grateful to my family and friends for their unwavering moral support and motivation throughout my academic journey. Their encouragement gave me the strength to successfully complete this work.

Lastly, I thank all those who directly or indirectly helped me during this project.

Place: Chayanika Kashyap

Date: Roll No.: MAT-04/23

Table of Contents

Chapter 1

Introduction to Cyclic Groups

1.1 Introduction

Group theory is an elementary branch of abstract algebra that deals with algebraic structures referred to as groups. Of all the other types of groups, cyclic groups are significant since they are uncomplicated and possess a structured form. Not only are they easy to grasp, but they are also the building blocks of more complicated algebraic structures. In relation to this introduction, we will discuss the theoretical background of cyclic groups, their properties, and why we should care about them in mathematics.

1.2 Cyclic Groups

Cyclic group is a group that is formed by one element. What this implies is that each element of the group can be determined in terms of powers (or multiples, in the additive case) of the generator. For example, consider the set of integers with addition and denote it as (Z,+). The element 1 is a generator in this case since any integer can be obtained as an addition or a subtraction of 1 iterated (2 = 1 + 1, -3 = -1 -1 -1, etc.). Cyclic groups are finite or infinite depending on how many elements there are in the group. A finite cyclic group of order n exactly has n elements, while an infinite cyclic group such as (Z,+) is not bound by any finite number of elements. The form is completely determined by the order and therefore is one of the easiest groups to study.

1.3 Properties and Examples

One of the most important properties of cyclic groups is that cyclic groups are always abelian, i.e., the group operation is commutative. i.e., for any two elements a and b in any

cyclic group, $a * b$ and $b * a$ are equal. This is due to the reason that the group is constructed by one element and the rest are all just powers of the generator.

A very typical example of a finite cyclic group is the set of integers modulo n under addition, or $(Z_n,+)$. The group in this case is the set $\{0,1,2,...,n-1\}$, and addition is modulo n. 1 is also a generator since repeated additions of 1 yield all the other elements of the group. Another example is the family of rotational symmetries of a regular n-gon where each rotation is an integer number of elementary rotations by $360^\circ/n$.

1.4 Uses in Mathematics

Cyclic groups have uses in many branches of mathematics, such as number theory, cryptography, and geometry. They are easy to understand, and therefore mathematicians can use them to examine more complicated algebraic structures. Cyclic groups inevitably appear in many areas of mathematics, for instance, in the study of complex roots of unity or in the classification of finite abelian groups.

To a certain degree, cyclic groups are probably the simplest and most universally understandable of all abstract algebra groups. Their own simplicity and universality of application render them a vital study for anyone who wishes to learn group theory. As we move towards their properties and applications, you will be able to understand how these groups are the building block of much advanced mathematics.

Chapter 2 Cyclic

Group

2.1 Cyclic Group

Group G is *cyclic* if there exists $a \in G$ such that the cyclic subgroup generated by a, $\langle a \rangle$, equals all of G, i.e., $G = \{na \mid n \in Z\}$, in which case a is called a *generator* of G. The reader should note that additive notation is used for G. We have already defined a cyclic group $\langle a \rangle$ generated by an element a of a group G.

We have already mentioned that a cyclic group may have more than one generator. For instance, if we choose the additive group $Z_8 = \{0,1,2,3,4,5,6,7\}$, then it can be seen that $Z_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$. However, one should not conclude that all groups are cyclic. For instance, the group $U(8) = \{1,3,5,7\}$ under multiplication (mod 8) is not a cyclic group. One can verify that $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1,3\}$, $\langle 5 \rangle = \{1,5\}$, $\langle 7 \rangle = \{1,7\}$. At this point, we would like to mention that the order of a cyclic group $G = \langle a \rangle$ will always equal the order of the generator, i.e., $|G| = |a|$.

Theorem 1

Suppose G is a group and $a \in G$. Then:

(i) If $|a|$ is infinite, then $a^i = a^j \Leftrightarrow i = j$.

(ii) If $|a|$ is finite, then $a^i = a^j \Leftrightarrow n \mid (i - j)$.

Proof

(i) Since $|a|$ is infinite, for any nonzero integer n, we have $a^n \neq e$. Now,

$$a^i = a^j \Leftrightarrow a^{i-j} = e \Leftrightarrow i - j = 0 \Leftrightarrow i = j$$

This completes the proof of the first part.

(ii) Suppose $|a| = n$, then by the closure property:

$$\{e, a, a^2, \ldots, a^{n-1}\} \subseteq \langle a \rangle$$

For any a, if $k \in \langle a \rangle$, by the division algorithm we have,

$$k = nq + r \qquad \text{where } 0 \leq r < n.$$

Then,

$$a_k = (a_n)_q a_r = a_r.$$

It follows that,

$$\langle a \rangle \subseteq \{e, a, a^2, \ldots, a^{n-1}\} \tag{2.2}$$

From (2.2), it follows that:

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

Since $|a| = n$, therefore n is the least positive integer such that $a^n = e$. Now, by the division algorithm we have:

$$i - j = nq + r \qquad \text{where } 0 \leq r < n.$$

It follows that,

$e = a^{i-j} = (a^n)^q a^r = a^r \Rightarrow r = 0$ [since $0 \leq r < n$ and n is the smallest positive integer such that a^n

It follows that,

$$i - j = nq \Rightarrow n \mid (i - j)$$

Conversely, suppose that $n \mid (i - j)$ so that $i - j = ns$ for some positive integer s. It follows that,

$$a_{i-j} = (a_n)_s = e \Rightarrow a_i = a_j$$

This completes the proof.

Remark 1. As we have seen that $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ whenever $|a| = n$, therefore we can conclude that:

$$|a| = |\langle a \rangle|$$

Remark 2. In a cyclic group $\langle a \rangle$, for any positive integer k, whenever we get $a^k = e = a^0$, we can conclude that:

$$|a| = n \mid k$$

Remark 3. If a,b are elements of a finite group G and $ab = ba$, then:

$$|ab| \mid |a||b|$$

Proof. Since $a,b \in G$ and the group G is finite, therefore $|a|$ and $|b|$ must be finite. Suppose that $|a| = m$ and $|b| = n$. We now have,

$$(ab)^{mn} = (a^m)^n(b^n)^m = e \qquad [\because ab = ba \text{ and } a^m = e, b^n = e]$$

Thus by Remark (2), $|ab|$ will divide $mn = |a||b|$.
This completes the proof.

Theorem 2. Let a be an element of order n in a group G. Then for any positive integer k,

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle \quad \text{and} \quad |a^k| = \frac{n}{\gcd(n,k)}.$$

Proof. Let us assume that $d = \gcd(n,k)$ and we consider the cyclic group $\langle a^d \rangle$. Thus, the first part of the result will be established if we can prove that $\langle a^k \rangle = \langle a^d \rangle$. Since $d = \gcd(n,k)$, therefore there exist integers s,t such that

$$d = ns + kt.$$

It follows that

$$a^d = (a^n)^s(a^k)^t = (a^k)^t \in \langle a^k \rangle \qquad [\because a^n = e]$$

$$\Rightarrow \langle a^d \rangle \subseteq \langle a^k \rangle.$$

On the other hand, since $d \mid k$, therefore for some integer s we have $k = ds$. It follows that

$$a^k = (a^d)^s \in \langle a^d \rangle \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle.$$

It follows that

$$\langle a^k \rangle = \langle a^d \rangle.$$

For the second part of the result, we notice that

$$(a^d)^{\frac{n}{d}} = e,$$

from which we can conclude that

$$|a^d| \leq \frac{n}{d}.$$

If possible, let us assume that there exists a positive integer t such that $t < \frac{n}{d}$ and $a^{dt} = e$. Thus we arrive at a contradiction because $dt < n$ and $|a| = n$.

This contradiction leads us to the conclusion that

$$|a^d| = \frac{n}{d}.$$

This completes the proof.

Remark 4. The order of any element of a finite cyclic group divides the order of the group.

Proof. Suppose that ⟨*a*⟩ is a finite cyclic group and |*a*| = |⟨*a*⟩| = *n*. Suppose that a^k ∈ ⟨*a*⟩ and $|a^k| = m$.

By the above result,

$$m = \frac{n}{\gcd(n,k)} \Rightarrow \frac{n}{m} = \gcd(n,k).$$

This completes the proof.

Remark 5. In a cyclic group *G* = ⟨*a*⟩ of order *n*, for any two positive integers *i,j* the following results hold:

(i) ⟨a^i⟩ = ⟨a^j⟩ ⟺ gcd(*n,i*) = gcd(*n,j*)

(ii) $|a^i| = |a^j|$ ⟺ gcd(*n,i*) = gcd(*n,j*)

Proof. Suppose that gcd(*n,i*) = *d* and gcd(*n,j*) = *d*′. By the known result, we have

⟨a^i⟩ = ⟨a^d⟩ and ⟨a^j⟩ = ⟨$a^{d'}$⟩.

It follows that

⟨a^i⟩ = ⟨a^j⟩ ⟺ ⟨a^d⟩ = ⟨$a^{d'}$⟩ ⟺ *d* = *d*′.

This completes the proof of the first part.

On the other hand,

$$|a^i| = |a^j| \iff \frac{n}{d} = \frac{n}{d'} \iff d = d'.$$

This completes the proof of the second part. □

Remark 6. In a cyclic group *G* = ⟨*a*⟩ of order *n*, for any positive integer *k*, we always have ⟨*a*⟩ = ⟨a^k⟩ if and only if gcd(*n,k*) = 1.

Proof. Suppose that gcd(*n,k*) = *d*.

Let ⟨*a*⟩ = ⟨a^k⟩ so that |*a*| = $|a^k|$. It follows that

$$n = \frac{n}{d} \Rightarrow d = 1.$$

Conversely, suppose that *d* = 1. But then

$$|a^k| = n = |a|,$$

and consequently

$$\langle a \rangle = \langle a^k \rangle.$$

This completes the proof. □

Example 1. Suppose that $G = \langle a \rangle$ is a cyclic group of order 30. Determine the subgroups $\langle a^{26} \rangle$, $\langle a^{18} \rangle$, and $\langle a^{17} \rangle$. Also determine $|a^{26}|$, $|a^{18}|$, and $|a^{17}|$.

Solution: Since $G = \langle a \rangle$ is a cyclic group of order 30, we have:

$$G = \{e, a, a^2, \ldots, a^{29}\}$$

Since gcd(30,26) = 2, therefore

$$|a^{26}| = \frac{30}{2} = 15, \quad \langle a^{26} \rangle = \langle a^2 \rangle = \{a^2, a^4, \ldots, a^{28}, a^{30} = e\}$$

Since gcd(30,18) = 6, therefore

$$|a^{18}| = \frac{30}{6} = 5, \quad \langle a^{18} \rangle = \langle a^6 \rangle = \{a^6, a^{12}, a^{18}, a^{24}, a^{30} = e\}$$

Since gcd(30,17) = 1, therefore

$$|a^{17}| = \frac{30}{1} = 30, \quad \langle a^{17} \rangle = \langle a \rangle = \{a, a^2, a^3, \ldots, a^{29}, a^{30} = e\}$$

Example 2

Suppose that $G = \langle a \rangle$ is a cyclic group of order 1000. Determine the subgroups $\langle a^{400} \rangle$, $\langle a^{62} \rangle$, and $\langle a^{185} \rangle$. Also determine $|a^{400}|$, $|a^{62}|$, and $|a^{185}|$.

Solution:

Since $G = \langle a \rangle$ is a cyclic group of order 1000, we have:

$$G = \{e, a, a^2, \ldots, a^{999}\}$$

Since gcd(1000,400) = gcd($2^3 \cdot 5^3, 2^4 \cdot 5^2$) = $2^3 \cdot 5^2$ = 200, therefore:

$$|a^{400}| = \frac{1000}{\gcd(1000, 400)} = \frac{1000}{200} = 5$$

and

$$\langle a^{400} \rangle = \langle a^{200} \rangle = \{a^{200}, a^{400}, a^{600}, a^{800}, a^{1000} = e\}$$

Since gcd(1000,62) = gcd($2^3 \cdot 5^3, 2 \cdot 31$) = 2, therefore:

$$|a^{62}| = \frac{1000}{\gcd(1000, 62)} = \frac{1000}{2} = 500$$

and

$\langle a_{62} \rangle = \langle a_2 \rangle = \{a_2, a_4, a_6, a_8, \ldots, a_{998}, a_{1000} = e\}$ Since

$\gcd(1000,185) = \gcd(2^3 \cdot 5^3, 2^2 \cdot 5 \cdot 37) = 2^2 \cdot 5 = 20$, therefore:

$$|a^{185}| = \frac{1000}{\gcd(1000, 185)} = \frac{1000}{20} = 50$$

and

$\langle a_{185} \rangle = \langle a_{20} \rangle = \{a_{20}, a_{40}, \ldots, a_{980}, a_{1000} = e\}$

Theorem 3 (Fundamental Theorem of Cyclic Groups)

Every subgroup of a cyclic group is cyclic. If $G = \langle a \rangle$ is a cyclic group of order n, then the order of any subgroup of G divides n. Moreover, for each positive divisor k of n, there exists a unique subgroup of the cyclic group G of order k.

Proof

Suppose H is a subgroup of the cyclic group $G = \langle a \rangle$. Let us consider the set S defined by:

$$S = \{t \mid t > 0 \text{ and } a^t \in H\}$$

In case $t < 0$, then $a^{-t} \in H$ and $-t > 0$ so that $-t \in S$. It follows that S is a nonempty subset of the set of positive integers and therefore, by the Well-Ordering Principle, the set S has a minimal (least) element m (say). We now try to show that $H = \langle a^m \rangle$.

Clearly, $a^m \in H$ because $m \in S$. For any $a^k \in H$, by the Division Algorithm we have:

$$k = qm + r \quad \text{where} \quad 0 \le r < m$$

This implies:

$$a_k = (a_m)_q \cdot a_r \qquad \Rightarrow \qquad a_r = a_k \cdot (a_m)_{-q} \in H$$

which means $r \in S$ ...

But this contradicts our initial assumption that m is the least element of the set S and therefore we must have $r = 0$ for which $a^k = (a^m)^q$ and hence $H \subseteq \langle a^m \rangle$.

Since H is a subgroup and $a^m \in H$, therefore we have $\langle a^m \rangle \subseteq H$.

It follows that $H = \langle a^m \rangle$.

Suppose that $\gcd(n,m) = d$. Then,

$$|H| = \frac{n}{d} \quad \Rightarrow \quad |G| = d \cdot |H|$$

It follows that the order of the subgroup H divides the order of the group G.

Suppose that k is a positive divisor of n (the order of the cyclic group $G = \langle a \rangle$). Then there exists a positive integer s (say) such that $n = ks$.

Let us consider the subgroup $K = \langle a^s \rangle$ of the cyclic group $G = \langle a \rangle$. Clearly, $\gcd(n,s) = s$ so that

$$|K| = \frac{n}{s} = k$$

If possible, suppose there exists another subgroup $K' = \langle a^t \rangle$ of order k in the group G.

It follows that t is the least positive integer such that $a^t \in K'$ and $\gcd(n,t) = t$.

It follows that:

$$k = |K'| = \frac{n}{t} \quad \Rightarrow \quad kt = n = ks \quad \Rightarrow \quad t = s$$

i.e. $K = \langle a^s \rangle = \langle a^t \rangle = K'$.

It follows that there exists a unique subgroup of the cyclic group G corresponding to each positive divisor of the order of the group G.

This completes the proof.

Theorem 4. Let $G = \langle a \rangle$ be a cyclic group of order n and d be a positive divisor of n. Then the number of elements in the group G of order d is precisely $\varphi(d)$.

Proof. Since d is a positive divisor of n, therefore by the fundamental theorem of cyclic groups, there exists a unique subgroup H (say) of order d of the cyclic group G.

In case $a^k \in G$ such that $H = \langle a^k \rangle$, we must have $|a^k| = d$. But:

$$|a^k| = \frac{d}{\gcd(d,k)}$$

and hence $\gcd(d,k) = 1$, i.e., k is co-prime to d. The number of such k is given by $\varphi(d)$.

This completes the proof.

Theorem 5. Let G be a finite group of order n and d be a positive divisor of n. Then the number of elements in the group G of order d is precisely $k\varphi(d)$ for some integer $k \geq 0$.

Proof. In case the group G has no elements of order d, then we are through as $0 = 0 \cdot \varphi(d)$.

Suppose that the group G has an element a of order d. Then the cyclic subgroup $H = \langle a \rangle = \{e, a, a^2, \ldots, a^{d-1}\}$ of the group G has $\varphi(d)$ number of elements of order d. In case all the elements in the group G of order d lie in the cyclic subgroup, then we are through, for in such case $\varphi(d) = 1 \cdot \varphi(d)$. Suppose that there exists $b \in G \setminus H$ and $|b| = d$. Then the cyclic subgroup $K = \langle b \rangle$ will have precisely $\phi(d)$ number of elements of order d.It

follows that the group G has $2.\phi(d)$ number of elements of order d, provided H and K has no elements in common of order d.

One must note that $b \not\in H$ for which $H \neq K$. Let $c \in G$ such that $c \in H \cap K$ and order of c is d. But then $H =< c >= K$. This contradicts the fact that $H \neq K$. This contradiction leads us in to the conclusion that H and K has no elements in common of order d.

If we proceed in this fashion with the same set of arguments then in the kth step we shall arrive in a conclusion that the group G has $k.\phi(d)$ number of elements of order d. This complete the proof.

Example: A group of prime order is cyclic.

Solution: Suppose that G is group of order p where p is a prime number. It follows that $|G| \geq 2$. Thus there exists an element $a (\neq e) \in G$.We now have,

$$|a| \mid p \Rightarrow |a| = 1 \text{ or } p$$
$$\Rightarrow |a| = p \qquad [\because a \neq e]$$
$$\Rightarrow G =< a >$$

rk One should note that the order of a cyclic group is not necessarily prime number. For instance the order of the cyclic group Z_8 under *addition*(*mod* 8) is 8 which is not a prime number.

Chapter 3

Order of an Element

Previously, we discussed the concepts of finite and infinite groups. You already know how to determine the order of a finite group. For example, the order of the cyclic group D_n is $2n$ and the order of the symmetric group S_n is $n!$, where n is a natural number. In this chapter, we will focus on a more specific idea: the order of an individual element within a group. You will come to see that the order of an element relates to the size of the subgroup that is generated by that element.

Let's recall something from Unit 3. We learned that the set

$$Z = \{\ldots,-2m,-m,0,m,2m,\ldots\}$$

is a subgroup of Z for any integer m. Now, suppose H is a subgroup of Z that contains the element m. What connection do you think exists between mZ (the set of all integer multiples of m) and H? You might find it interesting that actually, $mZ \subseteq H$. Why is this so? Well, if $m \in H$, then its negative $-m$ must also be in H, because a subgroup must be closed under inverses. That means all multiples of m, both positive and negative (like $2m,3m,-2m,-3m$, and so on), must also belong to H. Therefore, all of mZ is contained within H.

This tells us something important: the set mZ is actually the smallest subgroup of Z that contains the element m.

What's fascinating is that this idea doesn't just apply to the group of integers Z; it holds true in any group. Let's now see a general proof.

Theorem 1

Let G be any group and let a be an element in G. Then, the set

$$A = \{\ldots,a^{-2},a^{-1},e,a,a^2,\ldots\}$$

is the smallest subgroup of G that contains a.

Proof

First, we need to verify that A is indeed a subgroup of G.

Since G is a group, its operation is associative, and this associativity naturally applies to the elements of A as well.

We also know that the identity element e is in A, because $e = a^0$.

Furthermore, for each element a^n in A, there exists an inverse element a^{-n} in A such that:

$$a_n \cdot a_{-n} = e$$

These facts satisfy the subgroup test (which you may recall from Unit 3), so we can conclude that A is a subgroup of G.

Now, suppose there is another subgroup H of G that contains the element a. Since H is a subgroup and $a \in H$, it must also contain all positive powers of a, such as a^2, a^3, and so on.

Because H is closed under inverses, it must also contain all negative powers of a, such as a^{-1}, a^{-2}, and so forth.

Additionally, H must include the identity element e.

This shows that all elements of A must also be in H, which means that $A \subseteq H$. In other words, A is contained in every subgroup of G that includes a. Therefore, A is the smallest subgroup of G that contains a.

Theorem 1 gives us a foundation for defining the concept of the order of an element, which we will explore in the next section.

Chapter 4

Properties of Cyclic Groups: A Natural and Intuitive Exploration

4.1 Introduction: The Beauty of Simplicity

Cyclic groups are among the most fundamental structures in abstract algebra, admired for their elegance and simplicity. Unlike more complicated groups, cyclic groups are generated by a single element, making them easy to visualize and understand. Think of them like a clock—each tick moves you to the next number, and after a full cycle, you return to the start. This intuitive behavior makes cyclic groups a favorite topic for students and mathematicians alike.

But what truly makes cyclic groups special are their properties—predictable, clean, and deeply interconnected. Whether finite or infinite, every cyclic group follows a set of rules that reveal hidden symmetries in mathematics. In this discussion, we'll explore these properties in a way that feels natural, almost like uncovering the hidden patterns of a well-designed puzzle.

4.2 Fundamental Properties of Cyclic Groups

Generators: The Heart of Cyclic Groups

A cyclic group is like a machine powered by a single element—the **generator**. Just as a single seed can grow into an entire plant, one generator can produce every element in the group through repeated operations.

> **Example**: In the group $Z_6 = \{0,1,2,3,4,5\}$ under addition modulo 6, the element **1** is a generator because:
>
> $$1 \to 2 \to 3 \to 4 \to 5 \to 0 \to 1 \text{ (cycle repeats)}$$
>
> Interestingly, **5** is also a generator since adding it repeatedly cycles backward:
>
> $$5 \to 4 \to 3 \to 2 \to 1 \to 0 \to 5 \text{ (same cycle, reversed)}$$

This shows that a cyclic group can have multiple generators, each weaving the same structure in different ways.

Cyclic Groups Are Always Abelian (Commutative)

One of the most comforting properties of cyclic groups is that they are **abelian**, meaning the order of operations doesn't matter. If you think of a merry-go-round, it doesn't matter if you hop on first and then spin or spin first and then hop on—the result is the same.

Mathematically, if $G = \langle g \rangle$, then for any two elements g^a and g^b, we have:

$$g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a$$

This commutativity makes computations straightforward, unlike in non-abelian groups where operations can get tangled.

Subgroups of Cyclic Groups Are Also Cyclic

A remarkable feature of cyclic groups is that their subgroups are perfectly structured—**every subgroup is itself cyclic**. If you take a cyclic group and pick elements at regular intervals, they form a smaller cycle within the larger one.

> **Example**: Consider Z_{12}. Its subgroups correspond to the divisors of 12:
>
> $$\text{Subgroups: } Z_1, Z_2, Z_3, Z_4, Z_6, Z_{12}$$
>
> Each subgroup is generated by $\frac{12}{d}$, where d is a divisor. This predictable lattice of subgroups makes cyclic groups a joy to study.

Classification: Finite vs. Infinite Cyclic Groups

Cyclic groups come in two flavors:

1. **Finite Cyclic Groups** (e.g., Z_n): These loop back after n steps, like a clock.
2. **Infinite Cyclic Groups** (e.g., Z): These extend forever, like counting numbers.

The beauty here is that **all cyclic groups of the same order are essentially identical** (isomorphic). Whether you're working with rotations of a pentagon (Z_5) or hours on a clock (Z_{12}), the underlying structure remains the same.

4.3 Advanced Insights: Uniqueness and Homomorphisms

Uniqueness Up to Isomorphism

Imagine two different-looking clocks—one digital, one analog. Despite their appearance, both tell time the same way. Similarly, any two cyclic groups of order n are **isomorphic**, meaning they have the same algebraic structure.

Key Result:

- Every infinite cyclic group is isomorphic to $\mathbb{Z}$.
- Every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

This universality makes cyclic groups a cornerstone in algebra—once you understand one, you understand them all.

Homomorphisms: Structure-Preserving Maps

Functions between cyclic groups (homomorphisms) are refreshingly simple. Since the whole group is generated by one element, the map is entirely determined by where the generator goes.

Example: A homomorphism $\phi : \mathbb{Z}10 \to \mathbb{Z}20$ sending $1\ 7\to 2$ will:

$$\phi(k) = 2k \mod 20$$

This predictability is rare in more complex groups, making cyclic groups a great starting point for studying group theory.

4.4 Why Cyclic Groups Matter in Real-World Applications

a)Cryptography: Secure Communication

Many encryption schemes (like RSA and Diffie-Hellman) rely on the hardness of problems in cyclic groups. The fact that exponentiation is easy, but reversing it (discrete logarithm) is hard, makes them ideal for secure communication.

b)Symmetry in Nature and Art

Cyclic groups model rotational symmetries—think of snowflakes, starfish, or Ferris wheels. Their repeating patterns are governed by cyclic structures.

c)omputer Science: Hashing and Randomness

Algorithms use cyclic groups to generate pseudorandom numbers, ensuring fairness in simulations and cryptography.

d)Music Theory and Art

Cyclic groups are like the musical scales of algebra—simple, yet capable of infinite variations. Their properties (abelian nature, cyclic subgroups, and universal structure) make them a gateway to deeper mathematical concepts. Whether in pure theory or real-world applications, cyclic groups continue to reveal hidden symmetries, proving that sometimes, the simplest structures hold the greatest beauty.

Chapter 5

Subgroup of Cyclic Group

5.1 Introduction to Cyclic Groups and Their Subgroups

A cyclic group is a group that is generated by a single element. If G is a cyclic group of an element g, then each element of G is expressible as g^n for some integer n. Cyclic groups may be finite or infinite, depending on whether the generator is of finite or infinite order.

Since they are so simple, the following question comes naturally: *What are the subgroups of a cyclic group?* The answer is a lovely and orderly one—each subgroup of a cyclic group is cyclic. And for finite cyclic groups, there is a bijective correspondence between the divisors of the order of the group and its subgroups.

a) Subgroups of Infinite Cyclic Groups

Let us first discuss the infinite cyclic group $\mathbb{Z}$, which is formed by 1 (or −1) under addition. The group $\mathbb{Z}$ contains all integer multiples of 1, i.e., $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$.

Theorem 5.1. *Any nontrivial subgroup of* $\mathbb{Z}$ *is of the type* $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ *for some positive integer n.*

Proof. Let H be a nontrivial subgroup of $\mathbb{Z}$. As H is nonempty and has positive integers (since if $h \in H$, then $-h \in H$), let n be the smallest positive integer in H.

We claim that $H = n\mathbb{Z}$.

> **Inclusion** $n\mathbb{Z} \subseteq H$**:** Because $n \in H$, by closure of addition, all integer multiples of n are in H.
>
> **Inclusion** $H \subseteq n\mathbb{Z}$**:** Suppose $h \in H$. By the division algorithm, $h = qn + r$ where $0 \leq r < n$. Since $h, qn \in H$, $r = h - qn \in H$. But n is the smallest positive element of H, so $r = 0$. Therefore, $h = qn$, i.e., $h \in n\mathbb{Z}$.

Therefore, $H = n\mathbb{Z}$, i.e., every subgroup of $\mathbb{Z}$ is cyclic. □

Corollary 5.2. *The infinite cyclic group* $\mathbb{Z}$ *contains an infinite number of subgroups, each of which is generated by a distinct positive integer n.*

b) Subgroups of Finite Cyclic Groups

Now let's consider finite cyclic groups. Let G be a finite cyclic group of order m, and let it be generated by an element g, thus $G = \{e, g, g^2, \ldots, g^{m-1}\}$.

Theorem 5.3. *For every positive divisor d of m, there is a unique subgroup H of G of order d, namely:*

$$H = \langle g^{m/d} \rangle$$

Proof. Let d be a divisor of m, and let $k = m/d$. Consider the element g^k. The order of g^k is d, because:

$$(g^k)^d = g^{kd} = g^m = e$$

and no smaller positive power of g^k results in the identity. Therefore, $H = \langle g^k \rangle$ is a cyclic subgroup of order d.

For uniqueness, let K be any other subgroup of order d.

As G is cyclic, K is generated by an element g^t, where t is the smallest positive integer such that $(g^t)^d = e$. This means m divides td, so $t = m/d = k$. So, $K = \langle g^k \rangle = H$. □

Corollary 5.4. *The number of subgroups of a finite cyclic group G of order m is equal to the number of positive divisors of m.*

c)Lattice of Subgroups

The subgroups of a cyclic group constitute a lattice that is analogous to the divisibility in integers.

> **For** $\mathbb{Z}$**:** The subgroups $n\mathbb{Z}$ are ordered by inclusion, with $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if m divides n.
>
> **For finite** G**:** If G has order m, the subgroups correspond to the divisors of m, with containment $H_1 \subseteq H_2$ if and only if the order of H_2 divides the order of H_1.

This duality between divisibility and inclusion of subgroups is one of the essential features of cyclic groups.

5.2 Applications and Examples

Example 1:

Take the cyclic group Z_{12} (integers modulo 12 with addition). The divisors of 12 are 1,2,3,4,6,12, and so the subgroups are:

⟨0⟩ = {0} (order 1)

⟨6⟩ = {0,6} (order 2)

⟨4⟩ = {0,4,8} (order 3)

⟨3⟩ = {0,3,6,9} (order 4)

⟨2⟩ = {0,2,4,6,8,10} (order 6)

Z_{12} itself (order 12)

Example 2:

In the multiplicative group $\mathbb{Z}_7^*$ (nonzero integers modulo 7 under multiplication), which is cyclic of order 6, the subgroups are equal to the divisors of 6:

⟨1⟩ = {1}

⟨6⟩ = {1,6} (because $6 \equiv -1 \bmod 7$)

⟨2⟩ = {1,2,4} (because $2^3 \equiv 1 \bmod 7$)

The entire group $\mathbb{Z}_7^*$

5.3 Conclusion

Cyclic groups have a very neat subgroup structure. Finite or infinite, their subgroups are all cyclic, and in the finite situation, they correspond one-to-one with divisors of the order of the group. This beautiful connection between number theory and group theory makes cyclic groups a foundation of abstract algebra.

Knowledge of these subgroups not only gives insight into cyclic groups themselves but is also a basis for the exploration of more complicated algebraic structures. The interaction between generators, orders, and divisors shows deep relationships that still have an impact on contemporary mathematics.

Chapter 6

Applications

6.1 Applications of cyclic group

a)Cyclic group in Symmetry and Crystallography

Perhaps one of the most geometrically intuitive uses of subgroups is in the field of **symmetry**. Numerous natural objects and scientific structures display symmetrical characteristics, and group theory offers the vocabulary to discuss them.

Crystal Structures: Crystallography works on the principle that the atoms in a crystal are arranged in a pattern which repeats. The symmetries of these patterns are accounted for by **space groups**, which are infinite groups with translations, rotations, and reflections. Subgroups of these space groups are useful in distinguishing among various crystal structures. Diamond and graphite, for instance, both made of carbon atoms, have distinct symmetry subgroups and hence differ enormously in physical properties.

Molecular Symmetry: Point groups (finite symmetry groups) are employed by chemists to analyze molecules. Molecular vibrations, optical activity, and chemical reactivity are predicted by the subgroups of these point groups. For example, the water molecule (H_2O) is characterized by the $\mathbf{C_{2v}}$ point group, and this point group's subgroups explain why it possesses certain infrared absorption spectra.

By studying subgroups, researchers are able to forecast material behavior and create new materials with desired properties.

b)Cyclic group in Cryptography and Data Security

Contemporary cryptography depends considerably on algebraic structures, especially groups and their subgroups.

Discrete Logarithm Problem (DLP): Various encryption schemes, including the **Diffie-Hellman key exchange**, rely on the difficulty of DLP in finite cyclic groups. The security of such systems relies on the nature of subgroups of multiplicative groups of integers modulo a prime. If an attacker succeeds in identifying small subgroups, then he/she can take advantage of vulnerabilities in the encryption.

Elliptic Curve Cryptography (ECC): ECC relies on subgroups of points on elliptic curves to provide secure keys. The selection of a subgroup with a large prime order guarantees security against attacks. Cryptographers are able to develop secure encryption techniques protecting online communications and transactions through understanding the properties of subgroups.

Without subgroup theory, modern-day cybersecurity would not have the mathematical underpinning to secure digital data.

c)Cyclic group in Physics: Particle Physics and Quantum Mechanics

Subgroups are essential in theoretical physics, especially in the understanding of fundamental particles and quantum states.

Standard Model of Particle Physics: Symmetries of the elementary particles are characterized by **Lie groups** (such as SU(3) for quantum chromodynamics). The subgroup of these Lie groups classifies the particles and predicts the interactions. For instance, the **SU(2) × U(1)** subgroup is central to electroweak theory, which combines electromagnetic and weak nuclear forces.

Quantum Computing: Quantum systems tend to display group-theoretic symmetries. Subgroup study assists in error correction and the construction of quantum gates. As an example, the **Pauli group** (a unitary matrix subgroup) plays a vital role in quantum error-correcting codes.

Subgroup decompositions are applied by physicists to reduce complicated systems, making predictions regarding particle behavior and quantum phenomena.

d)Cyclic group in Computer Science: Algorithms and Data Structures

Group theory, specifically subgroup analysis, has unexpected uses in computer science.

Algorithm Optimization: Certain algorithms, such as the **Fast Fourier Transform (FFT)**, take advantage of symmetry by dividing issues into smaller subgroups. This lowers computational complexity from $O(n^2)$ to $O(n \log n)$.

Permutation Groups in Databases: Database search optimizations sometimes employ permutation subgroups to index and retrieve data quickly.

Theory of Coding: Error-correcting codes (such as **Reed-Solomon codes**) are based on algebraic structures in which subgroups are used for the detection and correction of data corruption.

Computer scientists use subgroups to create faster algorithms and more trustworthy data storage.

e)Cyclic group in Music Theory and Art

Surprisingly, cyclic group show up in music and art as well!

Symmetry in Music and Group Theory: Certain musicians apply group theory to organize musical pieces. The **dihedral group D_{12}** is used to represent transpositions and inversions of music involving 12 tones, and its subgroups are utilized to analyze chord sequences.

Visual Art and Tessellations: Artists such as M.C. Escher applied symmetry groups to form repeating designs. The consideration of subgroups enables us to categorize various forms of tessellations (e.g., hexagonal versus square tilings).

This convergence of mathematics and art illustrates how subgroup theory shapes creative expression.

6.2 Conclusion: Why Cyclic groups Matter

From protecting online communications to forecasting quantum behavior, subgroups are invaluable tools in fields. They uncover concealed patterns, maximize calculations, and even influence works of art. Anything but a theoretical construct, subgroup theory ties pure mathematics to practical applications, demonstrating that sometimes the greatest wisdom comes from examining the “small pieces” of a grand puzzle. No matter who you are—mathematician, physicist, computer scientist, or artist—knowledge of subgroups unlocks greater understanding and creativity.

Chapter 7

Homomorphisms and Isomorphisms involving Cyclic Group

7.1 Introduction

Cyclic groups are among the most fundamental and straightforward group structures. Due to their well-behaved nature, they are a perfect place to begin exploring more intricate algebraic ideas. The two crucial concepts that are crucial in analyzing cyclic groups are **homomorphisms** (maps that respect structure) and **isomorphisms** (isomorphic homomorphisms). They enable us to compare groups, categorize them, and reveal deeper symmetries.

In this discussion, we learn about homomorphisms and isomorphisms between cyclic groups, discussing how they map, what they preserve, and how they enable us to compare various groups.

7.2 Cyclic Groups: A Quick Refresher

A group G is said to be **cyclic** if there is an element $g \in G$ (known as a **generator**) such that each member of G may be expressed in the form g^n for some integer n. Cyclic groups may be finite or infinite:

The infinite cyclic group is isomorphic to $(\mathbb{Z},+)$.

A cyclic group of order n is isomorphic to $(\mathbb{Z}_n,+)$.

Due to their basic structure, cyclic groups are used as the blocks for constructing more complex groups, just like prime numbers in number theory.

7.3 Homomorphisms of Cyclic Groups

A **homomorphism** is a map $\phi : G \to H$ from one group to another whose operation preserves the group operation:

$$\phi(ab) = \phi(a)\phi(b) \quad \forall a,b \in G.$$

Homomorphisms in the case of cyclic groups are very easy to define since the whole group structure is determined by a generator.

7.3.1 Homomorphisms from Z to Another Group

Let $\mathbb{Z} = \langle 1 \rangle$ be the infinite cyclic group under addition. Let H be any group, and we wish to define a homomorphism $\phi : \mathbb{Z} \to H$.

Because $\mathbb{Z}$ is generated by 1, the homomorphism is completely specified by the value of $\phi(1)$. Let $h = \phi(1)$. Then, for any integer k,

$$\phi(k) = \phi(1 + 1 + \cdots + 1) = h^k.$$

Thus, each homomorphism from $\mathbb{Z}$ to H is equivalent to selecting an element $h \in H$ and "extending" it multiplicatively.

7.3.2 Homomorphisms from Finite Cyclic Groups

Now consider a finite cyclic group $G = \langle g \rangle$ of order n. A homomorphism $\psi : G \to H$ is specified by $\psi(g)$, but with one extra condition: since $g^n = e_G$, we have

$$\psi(g)^n = e_H.$$

This implies that the picture of g should be an element of H whose order divides n.

Example: Let $G = \mathbb{Z}_6$ and $H = \mathbb{Z}_4$. Let us consider the mapping $\psi : \mathbb{Z}_6 \to \mathbb{Z}_4$ defined by $\psi(1) = 1$. Then:

$$\psi(2) = 2, \quad \psi(3) = 3, \quad \psi(4) = 0, \quad \text{etc.}$$

But $\psi(6) = 6 \bmod 4 = 2 \neq 0$, contradicting $\psi(0) = 0$. Therefore, this is **not** a valid homomorphism.

But if we rather fix $\psi(1) = 0$, then ψ is the trivial homomorphism. Or, fixing $\psi(1) = 2$ also works because $6 \times 2 \equiv 0 \bmod 4$.

7.4 Isomorphisms of Cyclic Groups

An **isomorphism** is a bijective homomorphism, i.e., one that provides a complete one-to-one correspondence between two groups that preserves the group operation.

7.4.1 Classifying Cyclic Groups up to Isomorphism

An important theorem is that two cyclic groups are isomorphic if and only if they are of the same order:

Every infinite cyclic group is isomorphic to $\mathbb{Z}$.

Every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Proof Sketch:

If G is infinite cyclic, it contains a generator g such that all powers g^k are distinct. The mapping $k \mapsto g^k$ is an isomorphism $\mathbb{Z} \to G$.

If G is finite cyclic of order n, then $G \cong \mathbb{Z}_n$ via $k \mapsto g^k$.

7.4.2 Automorphisms of Cyclic Groups

An **automorphism** is an isomorphism of a group with itself. The group of all automorphisms of G is a group, denoted $\mathrm{Aut}(G)$.
For a cyclic group $G = \langle g \rangle$ of order n, an automorphism has to map g to another generator of G. The generators of $\mathbb{Z}_n$ are exactly the integers k with $\gcd(k,n) = 1$.
Therefore,

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*,$$

the multiplicative group of integers modulo n that are relatively prime to n. **Example:** Take $\mathbb{Z}_8$. Its generators are $\{1,3,5,7\}$. The automorphism group $\mathrm{Aut}(\mathbb{Z}_8)$ is the maps:

$$\phi_k : x \mapsto kx \mod 8, \qquad k \in \{1,3,5,7\}.$$

This group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

7.5 Applications and Further Insights

Knowledge about homomorphisms and isomorphisms of cyclic groups has various implications:

Group Classification: As all cyclic groups are defined by their order, we can easily classify them.

Subgroup Structure: Homomorphic images of any cyclic group are cyclic, and subgroups of cyclic groups are also cyclic.

Fundamental Theorem of Finite Abelian Groups: Cyclic groups are the basic blocks in the factorization of finite abelian groups.

7.6 Conclusion

Cyclic groups, though straightforward, offer profound insights into group theory via homomorphisms and isomorphisms. These maps enable us to find analogies between groups, determine structural equivalences, and construct intricate algebraic systems from simple building blocks. Through analysis of how such functions act on cyclic groups, we better understand symmetry, periodicity, and classification in algebra. This investigation highlights the beauty of cyclic groups and their dominant place in abstract algebra. Whether in theoretical studies or applied mathematics, their properties remain invaluable in contemporary mathematics.

Chapter 8

Role of Cyclic Groups in Field Theory

Introduction

Field theory is a core area of abstract algebra and deals with fields—algebraic structures in which addition, subtraction, multiplication, and division (by other than zero) are defined. Cyclic groups, i.e., groups generated by one element, find applications in interpreting field extensions, Galois theory, and roots of unity. This essay examines how cyclic groups impact field theory, specifically in finite fields, Galois extensions, and roots of polynomials.

8.1 Cyclic Groups: Definition and Basic Properties

A cyclic group is a group G whose every element is the power of one element g, also referred to as the generator. In mathematical terms, $G = ⟨g⟩ = \{g^n \mid n \in \mathbb{Z}\}$. Cyclic groups may be finite or infinite based on the generator order.

Key Properties:

Structure: All cyclic groups are isomorphic to either $\mathbb{Z}$ (infinite) or $\mathbb{Z}/n\mathbb{Z}$ (finite of order n).

Subgroups: All subgroups of a cyclic group are cyclic.

Generators: A finite cyclic group of order n has $\phi(n)$ generators, where ϕ is Euler's totient function.

These are the reasons why cyclic groups are easy but useful tools of field theory.

8.2 Cyclic Groups in Finite Fields

Finite fields, or Galois fields, have order p^n (where p is a prime and $n \geq 1$). The multiplicative group of any finite field is cyclic.

Multiplicative Group of a Finite Field

In a finite field $\mathbb{F}_q$ (where $q = p^n$), the group of nonzero elements $\mathbb{F}_q^*$ is a cyclic group under multiplication. That is:

> There is a primitive element α such that $\mathbb{F}_q^* = \langle \alpha \rangle$.
>
> Primitive elements play a key role in building finite fields and conducting algorithms in coding theory and cryptography.

Applications:

> **Discrete Logarithm Problem:** Cryptographic systems such as Diffie-Hellman key exchange utilize the cyclic nature of $\mathbb{F}_q^*$.
>
> **Error-Correcting Codes:** Cyclic groups assist in constructing cyclic codes, a family of error-correcting codes that appear in digital communications.

8.3 Cyclic Extensions and Galois Theory

Galois theory relates field extensions to group theory. A **cyclic extension** is a Galois extension whose Galois group is cyclic.

Kummer Theory

For fields with primitive n-th roots of unity, cyclic extensions of degree n are intimately connected with radicals. Namely:

> If F has a primitive n-th root of unity, then any cyclic extension E/F of degree n is of type $E = F(\sqrt[n]{a})$ for some $a \in F$.

Artin-Schreier Theory

In characteristic p, cyclic extensions of exponent p are characterized by Artin-Schreier polynomials $x^p - x - a$.

These theories emphasize how cyclic groups classify certain field extensions, making them easier to study.

8.4 Roots of Unity and Cyclotomic Fields

The n-th roots of unity (solutions to $x^n = 1$) are a cyclic group under multiplication.

Cyclotomic Fields

A cyclotomic field $\mathbb{Q}(\zeta_n)$ is obtained by adjoining a primitive n-th root of unity ζ_n to $\mathbb{Q}$. The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, which is not necessarily cyclic but has cyclic subgroups.

Applications:

Polynomial Solvability: Cyclic Galois groups assist in determining the solvability by radicals of a polynomial.

Fermat's Last Theorem: Cyclotomic fields played a key role in early proofs of some special cases of Fermat's theorem.

8.5 Conclusion

Cyclic groups are basic building blocks in field theory, providing organization and elegance to intricate algebraic structures. Ranging from finite fields through Galois extensions to roots of unity, their behaviors facilitate profound understanding of polynomial equations, cryptography, and error correction. Knowledge about cyclic groups is crucial for the development of both theoretical and applied mathematics.

Final Remarks

The interaction between cyclic groups and field theory exemplifies the beauty of algebraic structure. Through the use of their appropriately understood properties, engineers and mathematicians are able to find sensible solutions to real-world problems in secure communication, coding theory, and more.
This account emphasizes the inexorable place of cyclic groups in contemporary algebra, and their versatility and continued relevance

Chapter 9

Set of Generators in Cyclic Group

9.1 Introduction to Cyclic Groups and Generators

A **cyclic group** is a central concept in group theory where every element of the group can be represented as a power (or multiple, in additive form) of one single element.

Such a special element is referred to as a **generator** of the group.

Formally, a group G is said to be **cyclic** whenever there is an element $g \in G$ such that:

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} \qquad \text{(in case of multiplicative groups)}$$

or

$$G = \langle g \rangle = \{n \cdot g \mid n \in \mathbb{Z}\} \qquad \text{(in case of additive groups).}$$

The **generator set** of a cyclic group is the set of all elements that can generate the group. This set is important because it shows the symmetry and structure of the group.

9.2 Generator Sets in Finite and Infinite Cyclic Groups

Cyclic groups are either **finite** or **infinite**, and their generator sets are different in both cases.

1. Infinite Cyclic Groups

The easiest example of an infinite cyclic group is $(\mathbb{Z},+)$, the group of integers under addition. In this case, the generators are 1 and -1, because each integer can be expressed as $n \cdot 1$ or $n \cdot (-1)$.

Theorem 9.1. *An infinite cyclic group has exactly two generators.*

Proof. Let $G = \langle g \rangle$ be an infinite cyclic group. Assume h is another generator of G. Then, $h = g^k$ for some $k \in \mathbb{Z}$, and $g = h^m$ for some $m \in \mathbb{Z}$. Replacing, we obtain:

$$g = (g^k)^m = g^{km} \Rightarrow g^{km-1} = e.$$

Since G is infinite, there is only one possibility, i.e., $km = 1$. So, $k,m \in \{1,-1\}$, i.e., the only generators are g and g^{-1}. □

2. Finite Cyclic Groups

A cyclic group of finite order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n with respect to addition. The generators in this case are given by number-theoretic characteristics.

Theorem 9.2. *Let $G = ⟨g⟩$ be a cyclic group of order n. Then an element g^k is a generator of G if and only if* $\gcd(k,n) = 1$.

Proof. (⇒) Assume g^k is a generator of G. Then, there is an integer m such that $(g^k)^m = g$. Therefore, $km \equiv 1 \bmod n$, so k is a multiplicative inverse modulo n. That means $\gcd(k,n) = 1$.
(⇐) If $\gcd(k,n) = 1$, then by B´ezout's identity, there are integers x,y such that $kx + ny = 1$. Thus:

$$g = g^{kx+ny} = (g^k)^x \cdot (g^n)^y = (g^k)^x \cdot e^y = (g^k)^x.$$

Therefore, g is a power of g^k, so g^k generates G. □

Corollary 9.3. *The number of generators of a finite cyclic group of order n is $\phi(n)$, where ϕ is Euler's totient function.*

9.3 Examples of Generator Sets

Example 1: Infinite Cyclic Group

Let $G = \mathbb{Z}$. The generators are 1 and −1, since any integer is a multiple of these.

Example 2: Finite Cyclic Group of Order 6

Let $G = \mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$. The generators are the elements k where $\gcd(k,6) = 1$:

1 (since $\gcd(1,6) = 1$)

5 (since $\gcd(5,6) = 1$)

So the set of generators is $\{1,5\}$, and $\phi(6) = 2$, verifying the corollary.

Example 3: Multiplicative Cyclic Group

Let $G = \mathbb{Z}/7\mathbb{Z}^{\times}$, the group of integers under multiplication modulo 7. It is the cyclic group of order 6. The generators (primitive roots) are the elements whose powers run through all the non-zero residues modulo 7:

3 is a generator because $\{3^1, 3^2, \ldots, 3^6\} = \{3, 2, 6, 4, 5, 1\}$.

5 is also a generator because $\{5^1, 5^2, \ldots, 5^6\} = \{5, 4, 6, 2, 3, 1\}$.

The other members (1, 2, 4, 6) do not produce the entire group, since their orders divide but are not equal to 6.

9.4 Conclusion

The collection of generators in a cyclic group also reflects a lot about its structure. For infinite cyclic groups, there are only two generators, and for a finite cyclic group of order n, there are $\phi(n)$ generators. Knowledge about these generators facilitates problem-solving about symmetry, cryptography, and number theory. Through the examination of specific instances and the demonstration of pivotal theorems, we witness how beautifully group theory bridges abstract algebra and computational practice. Cyclic groups' beauty is in their simplicity and deep-reaching implications throughout mathematics.

Chapter 10

Conclusion

10.1 Conclusion: The Central Role of Cyclic Groups in Algebra

Cyclic groups have a special position in group theory on account of their simplicity, their geometric charm, and their enormously broad application to mathematics at large. They are the most fundamental type of group, and they are the building blocks out of which all the higher structures of algebra are constructed. Their study illuminates deep conclusions regarding the symmetry, the periodicity, and the factorization in finite and infinite situations.

10.2 Simplicity and Classification

The most incredible thing about cyclic groups is that they are structurally clean. Any cyclic group is either isomorphic to the infinite group $(\mathbb{Z},+)$ or to a finite group $(\mathbb{Z}_n,+)$ modulo n. This is strong because it means that, in a way, all cyclic groups are familiar, up to isomorphism. The generator of a cyclic group—an element whose powers (or multiples) generate the entire group—does a beautiful job of introducing the idea of minimal generation and makes computation more easy and proof simpler. Finite cyclic groups, in fact, have extremely valuable applications in number theory and cryptography. For example, the group of integers under multiplication modulo a prime p, $(\mathbb{Z}_p^*, \times)$, is a cyclic group, and this is the base of most such algorithms like the **Diffie-Hellman key exchange** and **RSA encryption**. The existence of primitive roots (the group generators) guarantees secure crypto protocols and thus cyclic groups are a part of computer science much so.

10.3 Subgroups and Homomorphisms

Another essential property of cyclic groups is that all of their subgroups are cyclic. This renders them structurally easy to analyze. For an infinite cyclic group $\mathbb{Z}$, all of its proper subgroups are isomorphic to $\mathbb{Z}$ itself, while in $\mathbb{Z}_n$, the subgroups correspond to the divisors of n. This divisibility condition has a direct correspondence with number theory, reinforcing the interdependence between number theory and algebra. In addition, cyclic group homomorphisms are especially nice. Any homomorphism of a cyclic group is determined entirely by the image of its generator. This leads us to nice consequences, such as the **First Isomorphism Theorem**, simplifying the investigation

of quotient groups of cyclic groups to mere computations. These features render cyclic groups unavoidable in constructing and deconstructing more complex algebraic structures.

10.4 Cyclic Groups in Advanced Contexts

Other than elementary group theory, cyclic groups appear in more advanced mathematical structures like **Galois theory**, **topology**, and **representation theory**. Galois theory, the Galois group of a finite extension field over a prime field is cyclic, which is used to solve polynomial equations. Topology, the fundamental group of the circle is isomorphic to Z, demonstrating how the cyclic groups retain fundamental geometric invariants.

Also, cyclic groups provide a route to the study of **abelian groups** through the **Fundamental Theorem of Finitely Generated Abelian Groups**, that every finitely generated abelian group is a direct sum of cyclic groups. This factorization is analogous to prime factorization of integers, and implies structure parallelism between number systems and group theory.

10.5 Conclusion

Briefly, cyclic groups are not only a novice topic in algebra but also a profound idea with implications that go far and wide. Because they are simple, they can be explained easily, but because they are rich, they are connected to advanced mathematical ideas. Cyclic groups extend from cryptography to topology, a single theory that combines discrete and continuous mathematics.

Much more can be explored on cyclic generalizations, such as **procyclic groups** in profinite group theory or **quantum cyclic groups** in non-commutative algebra. As mathematics evolves into tomorrow, the intrinsic importance of cyclic groups ensures that they will continue to be of interest to both theoretical and applied mathematics.

Bibliography

[1] Gallian, J. A. *Contemporary Abstract Algebra*. 9th ed., Cengage Learning, 2017. (A widely adopted text known for its approachable style, with strong focus on cyclic groups and practical examples.)

[2] Vijay K. Khanna & S. K. Bhambri. *A Course in Abstract Algebra*, fifth edition, 2016.

[3] Artin, M. *Algebra*. 2nd ed., Pearson, 2010. (A modern introduction to algebra with clear coverage of cyclic groups and their role in the structure of groups.)

[4] Dummit, D. S., and Foote, R. M. *Abstract Algebra*. 3rd ed., Wiley, 2004. (A comprehensive and widely used textbook that covers cyclic groups in depth, including their classification and properties.)

[5] Fraleigh, J. B. *A First Course in Abstract Algebra*. 7th ed., Pearson, 2002. (An accessible introduction to abstract algebra with clear explanations of cyclic groups and numerous examples.)

[6] Herstein, I. N. *Topics in Algebra*. 2nd ed., Wiley, 1975. (A classic algebra text that introduces cyclic groups early and provides solid foundational theory.)

[7] Rotman, J. J. *An Introduction to the Theory of Groups*. 4th ed., Springer, 1995. (Offers both introductory and advanced material on group theory, with detailed treatment of cyclic groups and their applications.)

[8] Robinson, D. J. S. *A Course in the Theory of Groups*. 2nd ed., Springer, 1996. (An advanced resource for deeper theoretical understanding of groups, including cyclic groups.)

[9] Scott, W. R. *Group Theory*. Dover Publications, 1987. (A classic and economical text that thoroughly covers the essential concepts of group theory, including cyclic groups.)

[10] Hall, M., Jr. *The Theory of Groups*. AMS Chelsea Publishing, 1999. (Advanced text providing rigorous theoretical background, including detailed treatment of cyclic and other finite groups.)