

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/311589005>

# Cyclic Groups

Chapter · November 2016

---

CITATIONS

0

READS

2,444

1 author:



Rajesh Singh

University of Delhi

16 PUBLICATIONS 4 CITATIONS

SEE PROFILE


Some of the authors of this publication are also working on these related projects:



NMEICT MHRD PROJECT [View project](#)



GRAPHOIDAL LENGTH OF A GRAPH [View project](#)

The background of the page features a large, semi-transparent watermark of the University of Delhi logo. The logo is circular and contains the text 'UNIVERSITY OF DELHI' around the top and '1962' at the bottom. In the center, there is a shield with a yellow top section, a green middle section, and a white bottom section. The shield is flanked by two red flowers.

**SUBJECT : Algebra**

**Group Theory**

**Cyclic Groups**

**RAJESH SINGH**

**Department of Mathematics  
University of Delhi, Delhi, India**

[singh\\_rajesh999@outlook.com](mailto:singh_rajesh999@outlook.com)

[+91-9716618372](tel:+91-9716618372)

## Table of Contents

### Chapter: Cyclic Groups

1. Learning Outcomes
2. Prerequisites
3. Preliminaries
4. Cyclic Group
  - 4.1. Generators of Cyclic Group
  - 4.2. Subgroups of Cyclic Group
5. Solved Problems
6. Summary
7. Exercises
8. References

*"Asforeverythingelse, soforamathematicaltheory:  
beauty can be perceived but not explained."*

*Arthur Cayley, 1821- 1895*

## 1. Learning Outcome

We believe at the end of this chapter the reader will become well versed with the following topics:

- Cyclic Groups.
- Generators of a Finite and Infinite Cyclic Groups.
- Subgroups of a Finite and Infinite Cyclic Groups.

Also, with lots of solved examples in text it will give the reader a depth into the concept.

## 2. Prerequisites

We expect the reader is well acquainted with the following concepts:

- Partially Ordered Sets and Lattices
- Group and its order
- Subgroup of a Group

## 3. PRELIMINARIES

To make the text self-contained we list some of the basic definitions and results that we require to study this chapter.

**Definition 3.1** A non-empty set  $P$  along with a binary relation  $R$  on  $P$  is said to form a **poset (partially ordered set)** if following condition are satisfied:

- P1.** Reflexivity:  $aRa \quad \forall a \in P$
- P2.** Anti-symmetry: If  $aRb$  and  $bRa$ , then  $a = b$ .  $[a, b \in P]$
- P3.** Transitivity: If  $aRc$  and  $bRc$ , then  $aRc$ .  $[a, b, c \in P]$

For convenience, we use the symbol  $\leq$  in place of  $R$ . The reason for using  $\leq$  is that it is in natural sync with the conditions above. Further, if  $a \leq b$  i.e.,  $aRb$ , then the two elements  $a$  and  $b$  are said to be comparable.

**Definition 3.2** Let  $S (\neq \emptyset)$  be a subset of a poset  $(P, \leq)$ . An element  $a \in P$  is an **upper bound of  $S$**  if  $x \leq a \quad \forall x \in S$ . Further, if  $a$  is an upper bound of  $S$  such that  $a \leq b$  for any upper bound  $b$  of  $S$ , then  $a$  is called the **supremum (or least upper bound)** of  $S$ . We write  $\sup S$  for supremum of  $S$ .

**Definition 3.3** Let  $S (\neq \emptyset)$  be a subset of a poset  $(P, \leq)$ . An element  $a \in P$  is called a lower bound of  $S$  if  $a \leq x \quad \forall x \in S$  and  $a$  will be called **infimum (or greatest lower bound)** of  $S$  if  $b \leq a$  for all lower bound  $b$  of  $S$ . We write  $\inf S$  for infimum of  $S$ .

**Definition 3.4** A poset  $(L, \leq)$  is called a **lattice** if for every  $a, b \in L$

$$\sup\{a, b\} \text{ and } \inf\{a, b\} \text{ belong to } L.$$

Let  $X (\neq \emptyset)$  be any set, the power set  $\mathcal{P}(X)$  of  $X$  forms a poset under  $\subseteq$  (usual set containment). Further, it is easy to observe that for any  $A, B \in \mathcal{P}(X)$

$$\sup\{A, B\} = \begin{cases} B & \text{if } A \subseteq B \\ A & \text{if } B \subseteq A \end{cases} \quad \text{and} \quad \inf\{A, B\} = \begin{cases} B & \text{if } B \subseteq A \\ A & \text{if } A \subseteq B \end{cases}$$

and hence both  $\sup\{A, B\}$  and  $\inf\{A, B\}$  exist in  $\mathcal{P}(X)$ . Thus the **poset**  $(\mathcal{P}(X), \subseteq)$  **forms a lattice.**

### DIAGRAMMATIC REPRESENTATION OF A POSET

To draw a poset, we represent each element by a small black-filled circle and any two comparable elements are joined by line(s) in such a way that if  $a \leq b$  then  $a$  lies below  $b$  in the diagram. Non-comparable elements are not joined. Clearly, there will be no horizontal lines in the diagram of a poset. Figure illustrates the poset  $P = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$  under divisibility.

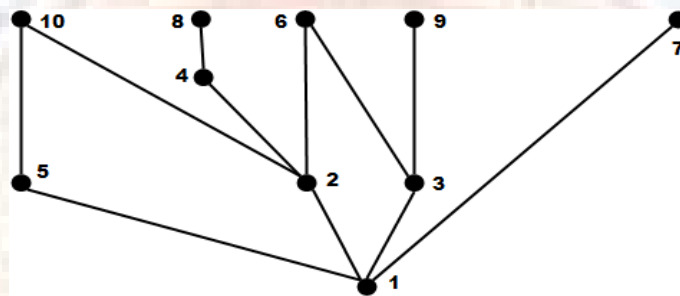


Figure 1.1

**Definition 3.5** A **binary operation** on a given set  $X$  is a function with **domain**  $X \times X$  and **co-domain**  $X$  i.e., it assigns each element of  $X \times X$  a unique element of  $X$ .

Thus a binary operation can be considered as a method by which two members (may or may not be distinct) of  $G$  combine to again give an element of  $X$ . Addition, subtraction and multiplication over the set of integers are some of the familiar examples of binary operation. Also, it is known that division over integers is not a binary operation as we may not always get an integer when an integer is divided by another integer.

**Definition 3.6** Let  $G$  be any non-empty set and  $*$  be a binary operation on  $G$ . Then we say that  $G$  forms a **group** w.r.t the operation  $*$  if the following conditions are satisfied:

1. **Associativity.**  $a * (b * c) = (a * b) * c \forall a, b, c \in G$ .
2. **Identity.** There exists  $e \in G$  such that  $a * e = e * a = a \forall a \in G$ .
3. **Inverse.** For each element  $a \in G$ , there exists an element  $b \in G$  such that

$$a * b = b * a = e.$$

If there is no ambiguity on the binary operation considered, then for simplicity we denote  $a * b$  by  $ab$ . It is important to note that in a group, identity element exists uniquely and each element of the group has an inverse which exists uniquely (prove yourself).

Also, it is worthwhile to mention here that some authors prefer to add the fourth condition which is also known as **closure property** ( $a * b \in G \forall a, b \in G$ ) while defining groups. But since we are considering binary operation, it takes care of the closure property required in the definition of groups. Thus if somebody equips a given set with some operation to make it a group, then it should be checked that the operation is indeed a binary operation i.e.,  $G$  is closed w.r.t the operation in consideration along with the other three properties of the groups.

**Definition 3.7** A group  $G$  is an **Abelian group** if  $ab = ba \forall a, b \in G$ . Otherwise, we say that the group  $G$  is a **non-Abelian group** i.e.,  $\exists a, b \in G$  such that  $ab \neq ba$ .

**Definition 3.8** The **order of a group  $G$** , denoted by  $|G|$ , is the cardinality of  $G$ . If  $G$  is finite then  $G$  has finite order otherwise the order is infinite.

**Definition 3.9** The **order of an element  $g$  of a group  $G$** , denoted by  $|g|$  is the smallest positive integer (if it exists)  $n$  such that  $g^n = \underbrace{g \cdot g \dots g}_{n \text{ times}} = e$  (identity of  $G$ ). If such an integer does not exist then we say that the element  $g$  has *infinite order*.

Thus to compute order of an element  $g$  of a group  $G$ , one just need to find the sequence  $g, g^2, g^3, \dots$ , until the identity is achieved for the first time. If identity is never achieved, then in that case order of  $g$  is infinite. Clearly, in a finite group, order of every element is finite.

**Definition 3.10** A subset  $H$  of a group  $G$  is said to be a **subgroup of  $G$**  if  $H$  itself forms a group under the operation of  $G$ . If  $H$  is a subgroup of  $G$ , then it is denoted by  $H \leq G$ . Further to indicate that  $H$  is a proper subgroup of  $G$  (proper in the sense of containment), then we use  $H < G$ . The subset  $\{e\}$  of  $G$  is trivially a subgroup of  $G$ .

$$H \leq G \Leftrightarrow \text{for any } a, b \in H, ab^{-1} \in H.$$

## 4. CYCLIC GROUP

Consider any group  $G$  and any arbitrary element  $a$  of  $G$ . The subgroup  $\{a^n : n \in \mathbb{Z}\}$  of  $G$ , denoted by  $\langle a \rangle$ , is called the **cyclic subgroup of  $G$  generated by  $a$** .

What if  $G = \langle a \rangle$  for some  $a \in G$ ? Does such groups enjoys some special properties? We call such groups as cyclic groups and such elements as generator of that group. In this chapter we try to explore properties associated with cyclic groups.

**Definition 4.1** A group  $G$  is a **cyclic group** if

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\} \text{ for some } a \in G.$$

In this case we say that  $G$  is a **cyclic group generated by  $a$** . Obviously, a cyclic group is always an abelian group.

**Example 4.2** The set  $\mathbb{Z}$  of integers under usual addition is a cyclic group. Recall that when the operation is addition then  $a^n$  in that group means  $na$ . Therefore

$$\{1^n : n \in \mathbb{Z}\} = \{n1 : n \in \mathbb{Z}\} = \{n : n \in \mathbb{Z}\} = \mathbb{Z}.$$

Thus 1 is the generator of  $\mathbb{Z}$  and hence  $\mathbb{Z}$  is a cyclic group. Further on the similar lines it can be shown that  $-1$  is also a generator of  $\mathbb{Z}$ . It is important to note here that 1 and  $-1$  are the only generators of  $\mathbb{Z}$ . This also shows that a group may have more than one generator i.e., generator of a cyclic group need not be unique.

**Example 4.3** The set  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  ( $n \geq 1$ ) under addition modulo  $n$  is a cyclic group. Again, 1 and  $-1 (= n-1)$  are generators of  $\mathbb{Z}_n$ . It is worthwhile to note here that while the set of integers  $\mathbb{Z}$  has only two generators 1 and  $-1$ ,  $\mathbb{Z}_n$  depending on the value of  $n$  may have more generators apart from 1 and  $-1$ . For example,  $\mathbb{Z}_{10}$  has 1, 3, 7, 9 ( $= -1$ ) as its generators and  $\mathbb{Z}_{12}$  has 1, 5, 7, 11 ( $= -1$ ) as its generators.

**Example 4.4** Consider the group  $U(n)$  under multiplication modulo  $n$ , where

$$U(n) = \{k \in \mathbb{N} : k < n \text{ and } g.c.d(k, n) = 1\}.$$

Now for  $n = 10$ ,  $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^3, 3^2\} = \langle 3 \rangle$ . Also,  $U(10) = \{1, 3, 7, 9\} = \{7^0, 7^3, 7, 7^2\} = \langle 7 \rangle$ . Thus both 3 and 7 are generators of  $U(10)$ . Hence  $U(10)$  is a cyclic group.

Now we will show that  $U(8) = \{1, 3, 5, 7\}$  is not a cyclic group. But how to show it? For that we will find subgroup generated by each of the elements in  $U(8)$ . Observe that

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{1, 3\} = \{3^0, 3^1\} \\ \langle 5 \rangle &= \{1, 5\} = \{5^0, 5^1\} \\ \langle 7 \rangle &= \{1, 7\} = \{7^0, 7^1\}. \end{aligned}$$

Therefore,  $U(8) \neq \langle a \rangle$  for any  $a \in U(8)$  and hence the claim.

Thus we have seen that  $U(n)$  is a cyclic group or not depends on the choice of  $n$ . So for which values of  $n$ , the group  $U(n)$  is cyclic? For now we will not be discussing this, but it is a good practice to have some values of  $n$ , for which  $U(n)$  is cyclic and some values of  $n$  for which  $U(n)$  is not cyclic.

## 4.1. GENERATORS OF A CYCLIC GROUP

**Theorem 4.1.1** For any element  $a$  in a group  $G$ ,  $\langle a^{-1} \rangle = \langle a \rangle$ . In particular, if an element  $a$  is a generator of a cyclic group then  $a^{-1}$  is also a generator of that group.

**Proof:** Consider any  $b \in \langle a \rangle$ . Then  $b = a^k$  for some  $k \in \mathbb{Z}$ . Now

$$b = a^k = (a^{-k})^{-1} = (a^{-1})^{-k} \in \langle a^{-1} \rangle.$$

Since  $b \in \langle a \rangle$  is arbitrary, therefore

$$\langle a \rangle \subseteq \langle a^{-1} \rangle.$$

Then it implies that

$$\langle a^{-1} \rangle \subseteq \langle (a^{-1})^{-1} \rangle = \langle a \rangle.$$

Hence we have

$$\langle a \rangle = \langle a^{-1} \rangle.$$

Second part immediately follows from the first part. ■

$$\langle a \rangle = \langle a^{-1} \rangle \text{ for any } a \in G.$$

**Theorem 4.1.2** For any element  $a$  in a group  $G$ , following holds:

1. If order of  $a$  is infinite, then all distinct powers of  $a$  are distinct elements i.e.,

$$a^i \neq a^j \text{ whenever } i \neq j, i, j \in \mathbb{Z}.$$

2. If order of  $a$  is  $n$  for some  $n \in \mathbb{N}$ , then  $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$  and

$$a^i = a^j \Leftrightarrow n \text{ divides } i - j.$$

**Proof: 1.** Order of  $a$  is infinite i.e.,  $a^k \neq e \forall k \in \mathbb{Z} \setminus \{0\}$ .

Suppose  $\exists i, j \in \mathbb{Z}$  ( $i \neq j$ ) such that  $a^i = a^j$ . But then it implies that  $a^{i-j} = e$ , which contradicts the fact  $a^k \neq e \forall k \in \mathbb{Z} \setminus \{0\}$ . Thus  $a^i \neq a^j$  whenever  $i \neq j, i, j \in \mathbb{Z}$ .

**2.** Order of  $a$  is  $n$  i.e.,  $n$  is the smallest positive integer such that  $a^n = e$ .

**Claim 1:**  $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ .

By definition,  $\{e, a, a^2, \dots, a^{n-1}\} \subseteq \langle a \rangle$ . For the converse consider any  $k \in \mathbb{Z}$ . By division algorithm,  $\exists q, r \in \mathbb{Z}$  such that

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

Now consider

$$a^k = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = a^r \in \{e, a, a^2, \dots, a^{n-1}\}.$$

Thus it follows that  $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ .

**Claim 2:**  $a^i = a^j \Leftrightarrow n \text{ divides } i - j$ .

Let  $a^i = a^j$  for some  $i, j \in \mathbb{Z}$ . Then  $a^{i-j} = e$  and by minimality of  $n$ , it follows that  $n \leq |i - j|$ .

Again by division algorithm,  $\exists q, r \in \mathbb{Z}$  such that

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

Now  $e = a^{i-j} = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = a^r$ . Thus  $a^r = e$  where  $0 \leq r < n$  and due to the minimality of  $n$  we must have  $r = 0$ . Thus  $i - j = qn$  i.e.,  $n$  divides  $i - j$ .



**Conversely**, if  $n$  divides  $i - j$ , then  $i - j = sn$  for some  $s \in \mathbb{Z}$  and therefore  $a^{i-j} = a^{sn} = (a^n)^s = e^s = e$ . Thus it follows that  $a^i = a^j$  whenever  $n$  divides  $i - j$ . ■

Next there is an immediate corollary to this theorem, which needs to be mentioned separately because of its importance in the study of theory of groups.

**Corollary 4.1.3** Let  $G$  be any group and  $a \in G$  be an element of finite order  $n$ . If  $a^k = e$  for some  $k \in \mathbb{Z}$ , then  $n$  divides  $k$ .

**Proof:** Now

$$\begin{aligned} a^k = e &\Rightarrow a^k = a^0 \\ &\Rightarrow n \text{ divides } k - 0 = k \quad [\text{Theorem 4.1.2}] \quad \blacksquare \end{aligned}$$

$$a^k = e \Rightarrow |a| \text{ divides } k$$

**Corollary 4.1.4** Order of a cyclic group is equal to the order of its generators i.e., if  $G = \langle a \rangle$  for some  $a \in G$ , then  $|G| = |a|$ .

**Proof:** We will discuss this in two cases:

**Case I**  $|a|$  is infinite.

Then by Theorem 4.1.2 all distinct powers of  $a$  are distinct members of  $G$  and hence cardinality of  $G$  is infinite. Hence  $|G| = |a|$ .

**Case II**  $|a|$  is finite say  $n$ .

Then again by Theorem 4.1.2  $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$  and thus  $|G| = n = |a|$ . ■

$$\begin{aligned} G = \langle a \rangle &\Rightarrow |G| = |a| \quad \text{and} \\ \text{in case } G \text{ is finite then } &|G| = |a| \Rightarrow G = \langle a \rangle. \end{aligned}$$

**Corollary 4.1.5** Order of any element of a finite cyclic group  $G$  divides the order of group  $G$  i.e.,  $|b|$  divides  $|G| \forall b \in G$ .

**Proof:** Let  $G = \langle a \rangle$  for some  $a \in G$  and  $b \in G$  be any arbitrary element. Then  $\exists k \in \mathbb{Z}$  such that  $b = a^k$ . But then

$$b^{|G|} = (a^k)^{|G|} = (a^{|G|})^k = e \quad [\text{since } |a| = |G| \text{ Corollary 4.1.4}]$$

From Corollary 4.1.3, it follows that  $|b|$  divides  $|G|$ . ■

**Corollary 4.1.6** For any element  $a$  in a group  $G$ ,  $|a| = |a^{-1}|$ .

**Proof:** From Theorem 4.1.1 we have  $\langle a \rangle = \langle a^{-1} \rangle$  and hence from Corollary 4.1.4 it follows that

$$|a| = |\langle a \rangle| = |\langle a^{-1} \rangle| = |a^{-1}|. \quad \blacksquare$$

**Theorem 4.1.7** Every group of prime order is cyclic and every element other than identity is a generator of the group.

**Proof:** Let  $G$  be a group with  $|G| = p$  (prime) and  $a (\neq e) \in G$  be any element. Then from Corollary 4.1.5,  $|a|$  divides  $|G| (= p)$  and therefore  $|a| = 1$  or  $|a| = p$ . Since  $a \neq e$ , therefore  $|a|$  must be prime  $p$ . Hence from Corollary 4.1.5, order of the subgroup  $\langle a \rangle$  of  $G$  is  $p$ . Thus it follows that  $G = \langle a \rangle$ . Further, since  $a (\neq e)$  is an arbitrary element of  $G$ , therefore  $G = \langle a \rangle \forall a (\neq e) \in G$ . ■

$$|G| = p \text{ (prime)} \Rightarrow G = \langle a \rangle \forall a (\neq e) \in G$$

From Theorem 4.1.2, it is easy to deduce that if  $a$  is an element of order  $n$ , then multiplication between elements in  $\langle a \rangle$  is done by addition modulo  $n$  i.e.,  $a^i \cdot a^j = a^k$  where  $k = (i + j) \bmod n$ . Thus given any group  $G$  and an arbitrary element  $a$  of  $G$  of finite order  $n$ , multiplication in  $\langle a \rangle$  behaves in a similar manner as addition in  $\mathbb{Z}_n$ . Similarly, if  $a$  is an element of infinite order, then  $a^i \cdot a^j = a^{i+j}$  and thus multiplication in  $\langle a \rangle$  behaves in a manner similar to addition in  $\mathbb{Z}$ .

Based on these discussion, every cyclic group of finite order  $n$  can be regarded as  $\mathbb{Z}_n$  in the abstract sense i.e., in view of group theoretic properties and every group of infinite order can be thought of as the group of integers  $\mathbb{Z}$  under usual addition.

In Example 4.3, we saw that 1, 3, 7, 9 were generators of  $\mathbb{Z}_{10}$  whereas 2, 4, 5, 8 were not. Similarly, 1, 5, 7, 11 were generators of  $\mathbb{Z}_{12}$  and 2, 3, 4, 6, 8, 9, 10 are not. Notice here that each of 1, 3, 5, 7 are relatively prime to 10 and each of 1, 5, 7, 11 are relatively prime to 12. Is this giving us a trend here? We will see in the next theorem and its subsequent corollaries that this is indeed a trend.

**Theorem 4.1.8 (Generator of finite Cyclic Groups)** Let  $G = \langle a \rangle$  be a finite cyclic. Then

$$G = \langle a^k \rangle \Leftrightarrow g.c.d(k, n) = 1, \quad \text{where } |G| = n.$$

**Proof:** Let  $g.c.d(k, n) = 1$ , then there exist integers  $s, t \in \mathbb{Z}$  such that  $ks + nt = 1$ . But then

$$a = a^1 = a^{ks+nt} = a^{ks} a^{nt} = (a^k)^s (a^n)^t = (a^k)^s \in \langle a^k \rangle.$$

Thus  $a \in \langle a^k \rangle$ , which further implies that all the powers of  $a$  belongs to  $\langle a^k \rangle$  i.e., every element of  $G$  is in  $\langle a^k \rangle$ . Hence  $G = \langle a^k \rangle$ .

**Conversely,** let  $G = \langle a^k \rangle$ . Since  $a \in G = \langle a^k \rangle$ , there exists  $m \in \mathbb{Z}$  such that  $a = (a^k)^m = a^{km}$ . Now  $a^{km} = a$  implies that  $a^{km-1} = e$ , then from Corollary 4.1.3 it follows that  $|a|$  divides  $km - 1$  i.e.,  $n$  divides  $km - 1$ . Therefore  $km - 1 = nr$  for some  $p \in \mathbb{Z}$ . Thus  $1 = km + nr$  for  $m, r \in \mathbb{Z}$  and therefore we must have  $g.c.d(k, n) = 1$ . ■

**If  $a$  is a generator of a finite cyclic group, then  $a^k$  is a generator of the group if and only if  $k$  is relatively prime to order of  $a$ . Thus a finite cyclic group of order  $n$  has  $\phi(n)$  generators, where  $\phi(n)$  is the number of positive integers less than  $n$  and relatively prime to  $n$ .**

**Corollary 4.1.9**  $\mathbb{Z}_n$  is generated by an integer  $k$  in  $\mathbb{Z}_n$  if and only if  $\text{g.c.d}(k, n) = 1$ . That is, the generators of  $\mathbb{Z}_n$  are precisely the elements of  $U(n)$ .

**Proof:** Note that  $\mathbb{Z}_n$  is a cyclic group with 1 as one of the generators. Thus taking  $G = \mathbb{Z}_n$  and  $a = 1$  in Theorem 4.1.8 yields the desired result. ■

The importance of Theorem 4.1.8 lies in the fact that if one of the generators of a cyclic group is known, then it gets relatively easier to find the other generators of that group. We illustrate this with the help of the example of  $U(50)$  under multiplication modulo 50. Now

$$U(50) = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49\}$$

and therefore  $|U(50)| = 20$ . Further, from the table it is easy to see that  $U(50)$  is a cyclic group with 3 as one of its generators. Since 1, 3, 7, 9, 11, 13, 17, 19 are relatively prime to  $20 (= |U(50)|)$ , therefore from Theorem 4.1.8, we have that  $3^1, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}$  are all the generators of  $U(50)$ . Thus

$$U(50) = \langle 3 \rangle = \langle 27 \rangle = \langle 37 \rangle = \langle 33 \rangle = \langle 47 \rangle = \langle 23 \rangle = \langle 13 \rangle = \langle 17 \rangle.$$

$3^0 \text{ mod } 50 = 1$	<b><math>3^1 \text{ mod } 50 = 3</math></b>	$3^2 \text{ mod } 50 = 9$	<b><math>3^3 \text{ mod } 50 = 27</math></b>	$3^4 \text{ mod } 50 = 31$
$3^5 \text{ mod } 50 = 43$	$3^6 \text{ mod } 50 = 29$	<b><math>3^7 \text{ mod } 50 = 37</math></b>	$3^8 \text{ mod } 50 = 11$	<b><math>3^9 \text{ mod } 50 = 33</math></b>
$3^{10} \text{ mod } 50 = 49$	<b><math>3^{11} \text{ mod } 50 = 47</math></b>	$3^{12} \text{ mod } 50 = 41$	<b><math>3^{13} \text{ mod } 50 = 23</math></b>	$3^{14} \text{ mod } 50 = 19$
$3^{15} \text{ mod } 50 = 7$	$3^{16} \text{ mod } 50 = 21$	<b><math>3^{17} \text{ mod } 50 = 13</math></b>	$3^{18} \text{ mod } 50 = 39$	<b><math>3^{19} \text{ mod } 50 = 17</math></b>

Though we had to do some calculations to find all the generators, but still the effort was much less than finding all the generators using direct calculations without taking the help of Theorem 4.1.8.

Theorem 4.1.8 depicts all the generators of a cyclic group of finite order. Now the question to be answered is how many generators an infinite cyclic group would have and what are they. We answer this in our next few theorems.

**Theorem 4.1.10** Order of every non-identity element in an infinite cyclic group is infinite.

**Proof:** Let  $G = \langle a \rangle$  be a cyclic group of infinite order. Then order of  $a$  is infinite. We claim that order of every non-identity element is infinite. Suppose on the contrary, there exists  $b (\neq e) \in G$  of finite order  $m$ . Since  $b \in G$ ,  $\exists k \in \mathbb{Z}$  such that  $b = a^k$ . Now  $e = b^m = (a^k)^m = a^{km}$ , a contradiction to the fact  $|a|$  is infinite. Thus our assumption is wrong and order of every non-identity element is infinite. ■

**Every non-identity element of a cyclic group of infinite order is of infinite order.**

Now if  $x$  is an element of a finite cyclic group  $G$  such that  $|x| = |G|$ , then obviously,  $G = \langle x \rangle$ . Is there the same trend in case of cyclic group of infinite order? In other words, if  $x \in G$  is such that  $|x| = |G| = \infty$ , then  $G = \langle x \rangle$ ? Further, since from Theorem 4.1.10 every element of an infinite cyclic group has infinite order, does it imply that every element of an infinite cyclic group is a generator? This is not true. For example, the group  $\mathbb{Z}$  of integers under ordinary addition is an infinite cyclic group with 1 and  $-1$  as their only generators. In fact in the next theorem we show that an infinite cyclic group has only two generators.

**Theorem 4.1.11 (Generators of an infinite cyclic groups)** Let  $G = \langle a \rangle$  be a cyclic group of infinite order. Then  $G$  has precisely two generators  $a$  and  $a^{-1}$ .

**Proof:** Since  $a$  is a generator, therefore  $a^{-1}$  is also a generator of  $G$ . Thus it is enough to prove that no element other than  $a$  and  $a^{-1}$  is a generator of  $G$ . Let  $b \in G$  be any generator of  $G$ . Then  $G = \langle a \rangle = \langle b \rangle$  and therefore there exist  $p, q \in \mathbb{Z}$  such that  $a = b^p$  and  $b = a^q$ . Consider

$$\begin{aligned} a &= b^p = (a^q)^p = a^{pq} \\ &\Rightarrow a^{pq-1} = e \\ &\Rightarrow pq - 1 = 0 \quad \text{[Since } |a| \text{ is infinite]} \\ &\Rightarrow p = q = 1 \text{ or } p = q = -1. \end{aligned}$$

Thus either  $b = a$  or  $b = a^{-1}$  and hence  $a$  and  $a^{-1}$  are precisely the generators of  $G$ . ■

We can summarize the above results as follows :

**Theorem 4.1.12** Let  $G$  be a group and let  $a$  be any element of  $G$ . Then

1.  $\langle a \rangle = \langle a^{-1} \rangle$  and  $|a| = |a^{-1}| = |\langle a \rangle|$ .
2.  $|a| = n \Leftrightarrow \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$
3.  $a^k = e \Leftrightarrow |a|$  divides  $k$
4.  $G$  is finite cyclic group  $\Rightarrow |a|$  divides  $|G|$
5.  $|G| = p$  (prime) and  $a (\neq e) \in G \Rightarrow G = \langle a \rangle$
6.  $G = \langle a \rangle$  finite cyclic group. Then  $G = \langle a^k \rangle \Leftrightarrow g.c.d(k, n) = 1$ .

Thus we now know about all the generators of a given cyclic group (finite or infinite). In the next section we will be discussing some of the problems in order to get more depth into the topic.

## 4.2. SUBGROUPS OF A CYCLIC GROUP

**Theorem 4.2.1** A subgroup of a cyclic group is cyclic. Further, if  $G = \langle a \rangle$  is a finite cyclic group and  $H$  is any subgroup of  $G$  then  $|H|$  divides  $|G|$ . In other words, order of any subgroup of a finite cyclic group divides the order of that group.

**Proof:** Let  $G = \langle a \rangle$  be a cyclic group and  $H$  be any subgroup of  $G$ . Since  $G$  is generated by  $a$ , therefore every element of  $H$  is some power of  $a$ . Now let  $m$  be the least positive integer such that  $a^m \in H$ . We claim that  $H = \langle a^m \rangle$ .

Let  $x \in H$  be any element. As  $x \in G$  there exists  $s \in \mathbb{Z}$  such that  $x = a^s$ . By division algorithm, there exist  $q, r \in \mathbb{Z}$  such that  $s = qm + r$  where  $0 \leq r < m$ . Now

$$\begin{aligned} x &= a^s = a^{qm+r} = a^{qm} a^r \\ \Rightarrow a^r &= x \cdot (a^m)^{-q} \in H \text{ [since } x, a^m \in H \text{]}. \end{aligned}$$

If  $0 < r < m$ , then  $a^r \in H$  contradicts the minimality of  $m$ . Hence we must have  $r = 0$  i.e.,  $s = qm$  which further implies that  $a^s = a^{qm} \in \langle a^m \rangle$ . Thus it follows that  $H = \langle a^m \rangle$ .

Now if  $G$  is finite, then from Theorem 4.1.12,  $|H| = |a^m|$  and  $|a^m|$  divides  $|G|$ . Hence  $|H|$  divides  $|G|$ . ■

Thus a subgroup of a cyclic group is always cyclic. Is the converse true? In other words, is the subgroup of a non-cyclic group always non-cyclic. In our next example we show that converse need not be true.

**Example 4.2.2** Consider the example of  $U(8) = \{1, 3, 5, 7\}$ , group under multiplication modulo 8. Observe that

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{1, 3\} = \{3^0, 3^1\} \\ \langle 5 \rangle &= \{1, 5\} = \{5^0, 5^1\} \\ \langle 7 \rangle &= \{1, 7\} = \{7^0, 7^1\}. \end{aligned}$$

Therefore,  $U(8) \neq \langle a \rangle$  for any  $a \in U(8)$  and hence  $U(8)$  is not a cyclic group. But it is interesting to note that every subgroup of  $U(8)$  is cyclic. To prove this we will show that  $\langle 1 \rangle, \langle 3 \rangle, \langle 5 \rangle$  and  $\langle 7 \rangle$  are the only proper subgroups of  $U(8)$ . Let  $H \neq \langle i \rangle$  for  $i = 1, 3, 5, 7$  be any subgroup of  $U(8)$ . Now we have three possibilities:

**Case 1.**  $3, 5 \in H$

Then  $3 \cdot 5 = 7 \in H$  and therefore  $7 \cdot 7 = 1 \in H$ . Thus  $H = U(8)$ .

**Case 2.**  $3, 7 \in H$ 

Then  $3 \cdot 7 = 5 \in H$  and  $7 \cdot 7 = 1 \in H$ . Thus  $H = U(8)$ .

**Case 3.**  $5, 7 \in H$ 

Then  $5 \cdot 7 = 3 \in H$  and  $7 \cdot 7 = 1 \in H$ . Thus  $H = U(8)$ .

Thus in all the cases we get  $H = U(8)$ . It follows that  $\langle 1 \rangle, \langle 3 \rangle, \langle 5 \rangle$  and  $\langle 7 \rangle$  are the only proper subgroups of  $U(8)$ . Hence  $U(8)$  serves as an example of a non-cyclic group, all of whose proper subgroups are cyclic.

**Theorem 4.2.3** Let  $G = \langle a \rangle$  be a finite cyclic group of order  $n$ . For each positive divisor  $k$  of  $n$ ,  $\langle a^{n/k} \rangle$  is the unique subgroup of order  $k$ .

**Proof:** First we claim that  $|\langle a^{n/k} \rangle| = k$ . For that we just need to show that  $|a^{n/k}| = k$  (Theorem 4.1.12). Let  $|a^{n/k}| = t$ .

Consider  $(a^{n/k})^k = a^n = e$ , thus  $|a^{n/k}|$  divides  $k$  i.e.,  $t | k$ . Now  $e = (a^{n/k})^t = a^{nt/k}$  and therefore by  $n \leq nt/k$ . Now consider

$$\begin{aligned} n &\leq \frac{nt}{k} \leq \frac{nk}{k} = n && [\because t \leq k] \\ \Rightarrow \frac{nt}{k} &= \frac{nk}{k} && \Rightarrow t = k. \end{aligned}$$

Thus  $|a^{n/k}| = k$  and hence order of  $\langle a^{n/k} \rangle$  is  $k$ .

Now we shall prove that  $\langle a^{n/k} \rangle$  is the only subgroup of  $G$  of order  $k$ . Let  $H$  be any subgroup of order  $k$ . Then by Theorem 4.2.1,  $H$  is a cyclic subgroup of  $G$  and  $H = \langle a^m \rangle$  where  $m$  is the smallest positive integer such that  $a^m \in H$ . By division algorithm  $\exists q, r \in \mathbb{Z}$  with  $0 \leq r < m$  such that  $n = mq + r$ . Now

$$\begin{aligned} e &= a^n = a^{mq+r} = a^{mq} a^r \\ \Rightarrow a^r &= a^{-mq} \in H = \langle a^m \rangle \\ \Rightarrow r &= 0 && [\text{since } m \text{ is the smallest positive integer such that } a^m \in H] \end{aligned}$$

Therefore  $m$  is a divisor of  $n$ , hence as proved earlier in the theorem  $|a^m| = n/m$ . Hence

$$q = n/m = |a^m| = |H| = k.$$

Consequently  $m = n/k$  and  $H = \langle a^m \rangle = \langle a^{n/k} \rangle$ . Thus  $\langle a^{n/k} \rangle$  is unique subgroup of order  $k$ . ■

Given any positive integer  $n \in \mathbb{N}$ , let  $\mathcal{F}(n)$  denote the set of all positive factors of  $n$  i.e.,

$$\mathcal{F}(n) = \{k \in \mathbb{N} : k \text{ divides } n\}.$$

Also, let  $\mathcal{H}_G$  denote the set of all subgroups of  $G$  i.e.,

$$\mathcal{H}_G = \{H : H \text{ is a subgroup of } G \text{ i.e., } H \leq G\}.$$

Now putting Theorem 4.2.1 and Theorem 4.2.3 together we obtain a well known theorem.

**Theorem 4.2.4 (FUNDAMENTAL THEOREM OF CYCLIC GROUPS)**

Let  $G = \langle a \rangle$  be a cyclic group of order  $n$ . Then

$$\mathcal{H}_G = \{\langle a^k \rangle : k \in \mathcal{F}(n)\},$$

where for each  $k \in \mathcal{F}(n)$ , order of subgroup  $\langle a^k \rangle$  is  $n/k$ . In other words, if  $G = \langle a \rangle$  is a cyclic group of order  $n$  and  $k$  is a divisor of  $n$ , then  $\langle a^k \rangle$  is unique subgroup of order  $n/k$ .

**Proof:** Consequence of Theorem 4.2.1 and Theorem 4.2.3. ■

To illustrate what Theorem 4.2.4 means, consider a cyclic group  $G = \langle b \rangle$  of order 30. Here  $\mathcal{F}(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$  is the set of all factors of 30. The set of all subgroups of  $G$  is given by

$$\begin{aligned} \mathcal{H}_G &= \{\langle b^k \rangle : k = 1, 2, 3, 5, 6, 10, 15, 30\} \\ &= \{\langle b^1 \rangle, \langle b^2 \rangle, \langle b^3 \rangle, \langle b^5 \rangle, \langle b^6 \rangle, \langle b^{10} \rangle, \langle b^{15} \rangle, \langle b^{30} \rangle\}. \end{aligned}$$

Further,

$$\begin{array}{ll} \langle b \rangle = \{e, b, b^2, \dots, b^{29}\} = G & \text{order 30,} \\ \langle b^2 \rangle = \{e, b^2, b^4, \dots, b^{28}\} & \text{order 15,} \\ \langle b^3 \rangle = \{e, b^3, b^6, \dots, b^{27}\} & \text{order 10,} \\ \langle b^5 \rangle = \{e, b^5, b^{10}, b^{15}, b^{20}, b^{25}\} & \text{order 6,} \\ \langle b^6 \rangle = \{e, b^6, b^{12}, b^{18}, b^{24}\} & \text{order 5,} \\ \langle b^{10} \rangle = \{e, b^{10}, b^{20}\} & \text{order 3,} \\ \langle b^{15} \rangle = \{e, b^{15}\} & \text{order 2,} \\ \langle b^{30} \rangle = \langle e \rangle = \{e\} & \text{order 1.} \end{array}$$

Thus we see that every subgroup of  $G$  is cyclic and corresponding to each divisor  $k$  of 30, there exists exactly one subgroup, namely,  $\langle b^k \rangle$  of  $G$  of order  $n/k$ .

We have an obvious but important consequence of Theorem 4.2.4. We take the special case when the given group is  $Z_n$ .

**Corollary 4.2.5 (Subgroups of  $Z_n$ )**

For each factor  $k$  of  $n$ ,  $\langle k \rangle$  is the unique subgroup of  $Z_n$  of order  $n/k$ . Furthermore, these are the only possible subgroups of  $Z_n$  i.e.,

$$\mathcal{H}_{Z_n} = \{\langle k \rangle : k \text{ divides } n \text{ i.e., } k \in \mathcal{F}(n)\}.$$

**Proof:** Since  $Z_n$  is a cyclic group with 1 as one of its generator i.e.,  $Z_n = \langle 1 \rangle$ . Therefore taking  $G = Z_n$  and  $a = 1$  in Theorem 4.2.4, we get the required result. ■

List of all subgroups of  $Z_{20}$  along with their generators:

$$\begin{aligned} \langle 1 \rangle &= \{0, 1, \dots, 19\} \\ \langle 2 \rangle &= \{0, 2, \dots, 18\} \end{aligned}$$

$$\langle 4 \rangle = \{0, 4, 8, 12, 16\}$$

$$\langle 5 \rangle = \{0, 5, 10, 15\}$$

$$\langle 10 \rangle = \{0, 10\}$$

$$\langle 20 \rangle = \{0\} = \langle 0 \rangle$$

Since 1, 2, 4, 5, 10, 20 are divisors of  $20 (= |Z_{20}|)$ , therefore from **Fundamental Theorem of Cyclic Groups (Corollary 4.2.5)**, we have

$$\begin{aligned} \mathcal{H}_{Z_n} &= \{\langle k \rangle : k \in \{1, 2, 4, 5, 10, 20\}\} \\ &= \{\langle 1 \rangle, \langle 2 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 10 \rangle, \langle 0 \rangle\}. \blacksquare \end{aligned}$$

After having seen the method of finding all possible subgroups of a cyclic group of finite order. One might be tempted to think : "Does there exist a method for counting elements of each order in a cyclic group of finite order?" To answer this question we introduce an important function  $\phi: \mathbb{N} \rightarrow \mathbb{N}$ , which is used frequently in number theoretic problems, called the **Euler Phi Function** and is defined as

$$\phi(n) = \begin{cases} 1 & \text{if } n = 1 \\ |U(n)| & \text{if } n > 1. \end{cases}$$

Given any  $n \in \mathbb{Z}^+$ ,

$$\phi(n) = n \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdots \frac{p_n - 1}{p_n}. \quad [\text{cf. Theorem 11 Page 24 [3]}]$$

where

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad (p_i \text{'s are distinct primes})$$

is the prime factorization of  $n$ .

#### Theorem 4.2.6 (Number of Elements of Each Order in a Finite Cyclic Group)

Let  $G$  be a cyclic group of order  $n$  and  $d$  be a positive divisor of  $n$ . Then the number of elements in  $G$  of order  $d$  is  $\phi(d)$ . In other words, if  $d \in \mathcal{F}(n)$ , then there are  $\phi(d)$  elements of order  $d$  in a cyclic group of order  $n$ .

**Proof:** Let  $G$  be any cyclic group of order  $n$ . Since  $d$  is a positive divisor of  $n$ , therefore by **Fundamental Theorem of Cyclic Groups** there exists only one subgroup (say)  $H$  of order  $d$ . Clearly,  $H$  is cyclic, so let  $H = \langle b \rangle$ . Since every element of order  $d$  generates a subgroup of order  $d$  and there is only one subgroup of order  $d$ , namely,  $H$ . Thus every element of order  $d$  must be a generator of subgroup  $H$ .

Now by Theorem 4.1.12,  $\{b^k : k \in U(d)\}$  is the set of all generators of  $H = \langle b \rangle$  and hence  $\{b^k : k \in U(d)\}$  is the set of all elements of order  $d$ . Since  $\phi(d) = |U(d)| = |\{b^k : k \in U(d)\}|$ , therefore there are  $\phi(d)$  elements in  $G$  of order  $d$ .  $\blacksquare$

**A finite cyclic group of order  $n$  has  $\phi(d)$  number of elements of order  $d$ , where  $d$  is a positive divisor of  $n$ .**



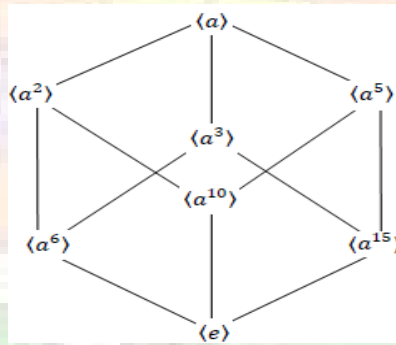
## SUBGROUP LATTICE OF A GROUP

Let  $G$  be a group and  $\mathcal{H}_G$  be the set of all subgroups of  $G$ . Consider the binary relation  $\leq$  on  $\mathcal{H}_G$  defined as : for  $A, B \in \mathcal{H}_G$

$$A \leq B \text{ if and only if } A \text{ is a subgroup of } B.$$

Then it can be easily seen that  $(\mathcal{H}_G, \leq)$  forms a lattice (*verify yourself*). The lattice  $(\mathcal{H}_G, \leq)$  is called a subgroup lattice of group  $G$ .

With the help of a subgroup lattice of a group one can easily depict the relationship between various subgroups of that group. The diagram of a subgroup lattice of a group includes all the subgroups and connects a subgroup  $A$  to a subgroup  $B$  which is at a level higher by a line or sequence of lines if and only if  $A$  is a proper subgroup of  $B$ .



**Figure 4.2.1** Subgroup Lattice of a cyclic group  $G = \langle a \rangle$  of order 30.

In Figure 4.2.1, we depict the lattice of a group of a cyclic group of order 30 and hence in particular, of the group  $\mathbb{Z}_{30}$ . Note here that we have the following chain of subgroups :

$$\begin{aligned} \langle e \rangle \leq \langle a^6 \rangle \leq \langle a^2 \rangle \leq \langle a \rangle, & \quad \langle e \rangle \leq \langle a^6 \rangle \leq \langle a^3 \rangle \leq \langle a \rangle \\ \langle e \rangle \leq \langle a^{10} \rangle \leq \langle a^5 \rangle \leq \langle a \rangle, & \quad \langle e \rangle \leq \langle a^{10} \rangle \leq \langle a^2 \rangle \leq \langle a \rangle \\ \langle e \rangle \leq \langle a^{15} \rangle \leq \langle a^5 \rangle \leq \langle a \rangle, & \quad \langle e \rangle \leq \langle a^{15} \rangle \leq \langle a^3 \rangle \leq \langle a \rangle. \end{aligned}$$

It is worthwhile here to note that the diagram can be drawn in many ways, but the connection between the two subgroups must be the same.

**Theorem 4.2.7** If the number of subgroups of a group is finite, then the group must be a finite group. In other words, a group of infinite order has infinite number of subgroups.

**Proof:** Suppose  $G$  is an infinite group with finite number of subgroups. Let  $a (\neq e) \in G$  be an arbitrary element. Then for each  $i \in \mathbb{N}$ ,  $\langle a^i \rangle$  is a subgroup of  $G$ . Since  $G$  has finite number of subgroups, therefore there exist  $k, l (k \neq l) \in \mathbb{N}$  such that  $\langle a^k \rangle = \langle a^l \rangle$  which further implies that  $a^k = (a^l)^p$  and  $a^l = (a^k)^r$  for some  $p, r \in \mathbb{Z}$ . Thus  $a^{k-pl} = e = a^{l-kr}$ . Now if order of  $a$  is infinite then  $k = pl$  and  $l = kr$  which is only possible in the case when  $k = l$  and  $p = r = 1$ , a contradiction to the fact that  $k \neq l$ . Thus order of  $a$  is finite. Since  $a \neq e$  was an arbitrary element of  $G$ . Hence every element in  $G$  has finite order. Thus we

can partition the set  $G$  as  $G = \cup_{a \in \Delta} H_a$ , where  $H_a = \{a, a^2, \dots, a^{|a|-1}\}$  and  $\Delta$  is the maximal subset of  $G$  such that

$$a \in \Delta \Rightarrow a \neq b^n \forall n \in \mathbb{N} \text{ and } \forall b \in \Delta - \{a\}.$$

Since for each  $a \in \Delta$ ,  $H_a$  is a finite set and as  $G$  is infinite, therefore the set  $\Delta$  is infinite. Now clearly, by the choice of  $\Delta$ , for any  $a, b \in \Delta (a \neq b)$ , the subgroups  $\langle a \rangle$  and  $\langle b \rangle$  are unequal. Thus the set  $\{\langle a \rangle : a \in \Delta\}$  is an infinite set consisting of subgroups of  $G$ , a contradiction to the fact that  $G$  has finite number of subgroups. ■

**Theorem 4.2.8** Cyclic groups of prime orders and the group  $\{e\}$  are the only groups with no non-trivial proper subgroups.

**Proof:** Let  $G$  be any group with no non-trivial proper subgroup. Then  $G$  has finite subgroups and hence is of finite order say  $p$ . If  $G = \{e\}$ , then we are through. Let  $G \neq \{e\}$  and  $a (\neq e)$  in  $G$  be any element. Then  $\langle a \rangle$  is a non-trivial subgroup of  $G$ , therefore we must have  $G = \langle a \rangle$ . Thus  $\mathcal{H}_G = \{\{e\}, G\}$ , the set of all subgroups of  $G$ . Therefore by **Fundamental Theorem of Cyclic Groups**  $\mathcal{F}(n) = \{1, p\}$ . This further implies that  $p$  is prime. Hence the proof follows. ■

**Theorem 4.2.9** If  $G$  is a group with exactly one non-trivial proper subgroup, then  $G$  is cyclic and  $|G| = p^2$  for some prime  $p$ .

**Proof:** Since  $G$  has 3 subgroups, therefore order of  $G$  is finite say  $n$ . Let  $H$  be the non-trivial proper subgroup of  $G$  and let  $|H| = p$ . Let  $a (\neq e) \in G - H$ . Clearly,  $\langle a \rangle$  is a non-trivial subgroup of  $G$ . Since  $G$  has exactly one non-trivial subgroup and  $H \neq \langle a \rangle$ , therefore  $G = \langle a \rangle$ . Thus  $G$  is cyclic group and every element of  $G$  which is not in  $H$  is a generator of  $G$ . Further,  $G$  is cyclic implies that  $H$  is cyclic.

Now since  $\mathcal{H}_H = \{\{e\}, H\}$  and  $\mathcal{H}_G = \{\{e\}, H, G\}$ , therefore by **Fundamental Theorem of Cyclic Groups**  $\mathcal{F}(p) = \{1, p\}$  and  $\mathcal{F}(n) = \{1, p, n\}$ . This further implies that  $p$  is prime and  $n = p^2$ . ■

## 5. SOLVED PROBLEMS

**Question 5.1.** Show that the group  $\mathbb{Q}^+$  under multiplication is not cyclic.

**Solution:** Let if possible, the group  $\mathbb{Q}^+$  is cyclic i.e.,  $\mathbb{Q}^+ = \langle p/q \rangle$  for some  $p, q \in \mathbb{Z}^+$  such that  $p$  and  $q$  are relatively prime. Now since  $1 \in \mathbb{Q}^+$ , therefore for some integer  $n$  we have

$$(p/q)^n = 1 \Rightarrow p^n = q^n \Rightarrow p = q.$$

Thus  $\mathbb{Q}^+ = \langle 1 \rangle = \{1\}$ , a contradiction. Hence our assumption is wrong and it follows that group  $\mathbb{Q}^+$  is not cyclic. ■

**Question 5.2.** Find generator for the subgroup  $\langle m \rangle \cap \langle n \rangle$  of the group  $\mathbb{Z}$ .

**Solution:** We claim that  $\langle m \rangle \cap \langle n \rangle = \langle l.c.m(m, n) \rangle$ . Let  $k = l.c.m(m, n)$ . Since  $k$  is a multiple of both  $m$  and  $n$ , therefore  $\langle k \rangle \subseteq \langle m \rangle \cap \langle n \rangle$ . For the converse, let  $a \in \langle m \rangle \cap \langle n \rangle$ . Then  $a = mr = ns$  for some  $r, s \in \mathbb{Z}$ . But then it implies that  $a$  is a multiple of both  $m$  and  $n$ , which further implies that  $a$  is a multiple of  $k$ . Therefore  $a \in \langle k \rangle$ . Thus  $\langle m \rangle \cap \langle n \rangle \subseteq \langle k \rangle$ . Hence we have

$$\langle m \rangle \cap \langle n \rangle = \langle k \rangle = \langle l.c.m(m, n) \rangle. \blacksquare$$

**Question 5.3.** Let  $a$  and  $b$  be group elements which commutes and are of order  $m$  and  $n$ , respectively. If  $\langle a \rangle \cap \langle b \rangle = \{e\}$ , prove that there exists an element whose order is  $l.c.m(m, n)$ . Show that the result might fail to be true if  $a$  and  $b$  do not commute.

**Solution:** Let  $k = l.c.m(m, n)$ . We claim that  $|ab| = k$ . Consider

$$(ab)^k = a^k b^k = e \cdot e = e.$$

Therefore  $|ab|$  divides  $k$ . Now let  $0 < r \leq k$  be such that  $(ab)^r = e$ . Then

$$\begin{aligned} a^r b^r = e &\Rightarrow a^r = b^{-r} \in \langle a \rangle \cap \langle b \rangle = \{e\} \\ &\Rightarrow a^r = e \text{ and } b^r = e \\ &\Rightarrow m|r \text{ and } n|r \\ &\Rightarrow k|r. \end{aligned}$$

Thus  $k$  is the least positive integer such that  $(ab)^k = e$ . Hence  $|ab| = k = l.c.m(m, n)$ .

Now to prove that the result may not hold if we drop the condition of commutativity, consider the general linear group  $GL(2, \mathbb{Z}_2)$  of  $2 \times 2$  matrices over  $\mathbb{Z}_2$ , where

$$\begin{aligned} GL(2, \mathbb{Z}_2) &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_2 \text{ and } (ad - bc) \bmod 2 = 1 \right\} \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}. \end{aligned}$$

Now consider the matrices  $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$  and  $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ . Then

$$AB = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = BA.$$

Thus  $A$  and  $B$  does not commute. Now

$$A^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |A| = 2 \text{ and}$$

$$B^3 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |B| = 3.$$

Observe that  $l.c.m(|A|, |B|) = l.c.m(2, 3) = 6$  and  $GL(2, \mathbb{Z}_2)$  has no element of order 6. In fact

$$\left| \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right| = 1, \quad \left| \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right| = \left| \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right| = \left| \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right| = 2 \text{ and } \left| \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right| = \left| \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right| = 3. \blacksquare$$

**Question 5.4.** Find the number of generators of  $U(49)$  by using the fact that  $U(49)$  is a cyclic group of order 42.

**Solution:** From **Theorem 4.1.8 (Generators of Cyclic groups)**, it is easy to see that  $U(49)$  has  $\Phi(42) = 12$  generators. ■

**Question 5.5.** Let  $a$  and  $b$  be group elements such that  $|a| = 10$  and  $|b| = 21$ . Prove that

$$\langle a \rangle \cap \langle b \rangle = \{e\}.$$

**Solution:** Let  $x \in \langle a \rangle \cap \langle b \rangle$ . Then  $x = a^m = b^n$  for some  $m, n \in \mathbb{Z}$ . Now

$$\begin{aligned} a^m &= b^n \\ \Rightarrow a^{10m} &= b^{10n} \\ \Rightarrow b^{10n} &= e \\ \Rightarrow 21 \text{ divides } 10n \\ \Rightarrow 21 \text{ divides } n & \quad [\because g.c.d(10,21) = 1] \\ \Rightarrow x = b^n &= e. \end{aligned}$$

Thus we have  $\langle a \rangle \cap \langle b \rangle = \{e\}$ . ■

**Question 5.6.** For  $n > 2$ , show that there are even number of generators of  $\mathbb{Z}_n$ .

**Solution:** We know that if  $k \in \mathbb{Z}_n$  is a generator of  $\mathbb{Z}_n$ , then  $k^{-1} = n - k$  is also a generator of  $\mathbb{Z}_n$ . Further,  $k = n - k$  implies that  $n = 2k$ . Since  $n > 2$ , therefore

$$n = 2k \Rightarrow g.c.d(n, k) = k > 1. \quad [A]$$

But from Corollary 4.1.9, since  $k \in \mathbb{Z}_n$  is a generator of  $\mathbb{Z}_n$  therefore  $g.c.d(n, k) = 1$ , a contradiction to [A]. Clearly, the set

$$K = \cup_{k \in \Delta} \{k, n - k\} \text{ where } \Delta = \left\{ k : k \leq \left\lfloor \frac{n}{2} \right\rfloor \right\}$$

is the set of all generators of  $\mathbb{Z}_n$  and consists of even number of elements. Hence  $\mathbb{Z}_n$  has an even number of generators.

#### Alternate Proof

Since  $\mathbb{Z}_n = \langle 1 \rangle$  is a cyclic group and order of  $\mathbb{Z}_n$  is  $n$ , therefore from **Theorem 4.1.8 (Generators of Cyclic groups)**,  $\mathbb{Z}_n$  has  $|\Phi(n)|$  of generators. Now we need to show that  $\Phi(n)$  is even whenever  $n > 2$ . By Fundamental Theorem of Arithmetic, we have

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \text{ where } p_i \text{'s are distinct primes.}$$

Then we have

$$\Phi(n) = n \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \dots \frac{p_n - 1}{p_n}. \quad [\text{cf. Theorem 11 Page 24 [3]}]$$

Now since for each  $i$ ,  $p_i$  is odd and therefore  $p_i - 1$  is even. Thus  $\Phi(n)$  is even. ■

**Question 5.7.** Let  $G$  be a finite group in which order of every non-identity element is prime. If  $Z(G)$  is not trivial, show that order of every non-identity element is same.

**Solution:** Let  $a(\neq e) \in Z(G)$ . Then by the hypothesis, we have  $|a| = p$ , for some prime  $p$ . Now let  $b(\neq e) \in G$  be any non-identity element of  $G$  and let  $|b| = q$  for some prime  $q$ . We claim that  $p = q$ . On the contrary, suppose that  $p \neq q$ . Then  $ab$  is not identity, for otherwise if  $ab = e = ba$ , then  $|a| = |b|$ , a contradiction to the assumption that  $p \neq q$ . Also, since  $p \neq q$  and  $p$  and  $q$  are primes, therefore  $\text{g.c.d}(p, q) = 1$ . We will first show that  $|ab| = pq$ . Consider

$$\begin{aligned}(ab)^{pq} &= a^{pq} b^{pq} && \text{[Since } a \in Z(G), a \text{ commutes with } b \text{]} \\ &= e \cdot e = e\end{aligned}$$

therefore  $|ab|$  divides  $pq$ . Now let  $r \leq pq$  be any positive integer such that  $(ab)^r = e$ . Then we have

$$\begin{aligned}a^r b^r &= e \\ \Rightarrow a^r &= b^{-r} \\ \Rightarrow (a^r)^q &= (b^{-r})^q = (b^q)^{-r} = e \\ &\Rightarrow p|rq \\ &\Rightarrow p|r \text{ [Since } \text{g.c.d}(p, q) = 1 \text{]}\end{aligned}$$

Similarly, we have  $q|r$ . Since  $\text{g.c.d}(p, q) = 1$ , therefore it follows that  $pq|r$ . Thus  $pq$  is the least positive integer such that  $(ab)^{pq} = e$ . Hence we have  $|ab| = pq$ . Since  $ab$  is not identity, by the hypothesis it follows that  $pq$  is prime, contradiction. Thus our assumption is wrong and hence  $p = q$ . Since  $b$  is an arbitrary non-identity element of  $G$ , it follows that every non-identity element of  $G$  has the same order. ■

**Question 5.8.** Let  $G = \langle a \rangle$  be a cyclic group of order 24. Find all generators of the subgroup of order 8.

**Solution:** Since  $G$  is a cyclic group, from **Fundamental Theorem of Cyclic Groups (Theorem 4.2.4)**, it follows that  $G$  has exactly one cyclic subgroup of order 8, namely

$$\langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}(= 1)\}.$$

Now since  $|a^3| = 8$  and 1, 3, 5, 7 are relatively prime to 8, so by **Theorem 4.1.12 (Generators of finite Cyclic groups)**, the generators for the subgroup  $\langle a^3 \rangle$  of order 8 are

$$\begin{aligned}a^3, (a^3)^3, (a^3)^5, (a^3)^7 \\ \text{i.e., } a^3, a^9, a^{15}, a^{21} \blacksquare\end{aligned}$$

**Question 5.9.** If  $|a| = n$ , show that

$$\langle a^k \rangle = \langle a^{\text{g.c.d}(n, k)} \rangle$$

and that

$$|a^k| = \frac{n}{\text{g.c.d}(n, k)}.$$

**Solution:** Let  $|a^k| = m$  and  $d = \text{g.c.d}(n, k)$  i.e.,  $\text{g.c.d}\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ . We claim that that

$$d = \frac{n}{m}.$$

Now consider

$$\begin{aligned} (a^k)^{\frac{n}{d}} &= (a^n)^{\frac{k}{d}} = e \\ \Rightarrow m \text{ divides } \frac{n}{d}. \end{aligned}$$

Again since  $(a^k)^m = e$ , therefore

$$\begin{aligned} n \text{ divides } km \\ \Rightarrow \frac{n}{d} \text{ divides } \frac{k}{d} m. \end{aligned}$$

Since  $g.c.d(\frac{n}{d}, \frac{k}{d}) = 1$  it follows that

$$\frac{n}{d} \text{ divides } m.$$

Hence we have

$$m = \frac{n}{d} i. e., d = \frac{n}{m}. \text{ ----- (A)}$$

Now since  $|\langle a^k \rangle| = m$  and from **Fundamental Theorem of Cyclic Groups (Theorem 4.2.4)**, there is exactly one subgroup of order  $m$ , namely  $\langle a^{n/m} \rangle = \langle a^d \rangle = \langle a^{g.c.d(n,k)} \rangle$ .

Thus it follows that

$$\langle a^k \rangle = \langle a^{g.c.d(n,k)} \rangle.$$

Also, from **(A)** we have

$$|a^k| = \frac{n}{g.c.d(n,k)}. \blacksquare$$

**Question 5.10.** Let  $|a| = 24$ . Find a generator for the subgroup  $\langle a^{21} \rangle \cap \langle a^{10} \rangle$ . In general, find the generator for  $\langle a^m \rangle \cap \langle a^n \rangle$ ?

**Solution:** Observe that

$$|\langle a^{21} \rangle| = |a^{21}| = \frac{24}{g.c.d(21,24)} = \frac{24}{3} = 8.$$

Now by **Fundamental Theorem of Cyclic Groups (Theorem 4.2.4)**, there is exactly one subgroup of order 8, namely  $\langle a^{24/8} \rangle = \langle a^3 \rangle$ . It follows that  $\langle a^{21} \rangle = \langle a^3 \rangle$ .

Similarly, since

$$|\langle a^{10} \rangle| = |a^{10}| = \frac{24}{g.c.d(10,24)} = \frac{24}{2} = 12,$$

therefore,  $\langle a^{10} \rangle = \langle a^2 \rangle$ .

Then

$$\langle a^{21} \rangle \cap \langle a^{10} \rangle = \langle a^3 \rangle \cap \langle a^2 \rangle = \langle a^6 \rangle.$$

Let  $p = g.c.d(m, 24)$  and  $q = g.c.d(n, 24)$ . Then from **Question 5.9**, it follows that

$$\langle a^m \rangle = \langle a^p \rangle \text{ and } \langle a^n \rangle = \langle a^q \rangle.$$

We claim that

$$\langle a^m \rangle \cap \langle a^n \rangle = \langle a^p \rangle \cap \langle a^q \rangle = \langle a^t \rangle$$

where  $t = l.c.m(p, q)$

Obviously, we have

$$\langle a^t \rangle \subseteq \langle a^p \rangle \cap \langle a^q \rangle.$$

Now let  $b \in \langle a^p \rangle \cap \langle a^q \rangle$ . Then  $b = a^{pr}$  and  $b = a^{qs}$  for some  $r, s (1 \leq r, s \leq 24)$  such that  $pr \leq 24$  and  $qs \leq 24$ . But then it implies that  $a^{pr} = a^{qs}$ , which further implies that

$$pr = qs \quad [ \text{since } pr, qs \leq 24 ]$$

Therefore  $pr$  is a multiple of both  $p$  and  $q$  and hence  $t$  divides  $pr$  i.e.,  $pr = tk$  for some  $k \in \mathbb{Z}$ . Thus we have  $b = a^{pr} = a^{tk} \in \langle a^t \rangle$ . Hence it follows that

$$\langle a^m \rangle \cap \langle a^m \rangle = \langle a^t \rangle. \quad \blacksquare$$

**Question 5.11.** Is every subgroup of the group of integers  $\mathbb{Z}$  cyclic? Why? Discuss all the subgroups of  $\mathbb{Z}$ .

**Solution:** Since  $\mathbb{Z} = \langle 1 \rangle$  is a cyclic group and from **Fundamental Theorem of Cyclic Groups (Theorem 4.2.4)**, every subgroup of a cyclic group is cyclic, therefore every subgroup of  $\mathbb{Z}$  is cyclic. The set of all subgroups of  $\mathbb{Z}$  is given by

$$\{ \langle n \rangle : n \in \mathbb{N} \cup \{0\} \}. \quad \blacksquare$$

**Question 5.12.** For distinct primes  $p$  and  $q$ , determine the subgroup lattice for  $\mathbb{Z}_{p^2q}$ .

**Solution:** Since order of  $\mathbb{Z}_{p^2q}$  is  $p^2q$  and  $\mathcal{F}(p^2q) = \{1, p, p^2, q, pq, p^2q\}$ . Therefore by **Fundamental Theorem of Cyclic Groups (Theorem 4.2.4)**,

$$\mathcal{H}_{\mathbb{Z}_{p^2q}} = \{ \langle 1 \rangle, \langle p \rangle, \langle p^2 \rangle, \langle q \rangle, \langle pq \rangle, \langle p^2q \rangle \}.$$

are the only subgroups of  $\mathbb{Z}_{p^2q}$ .

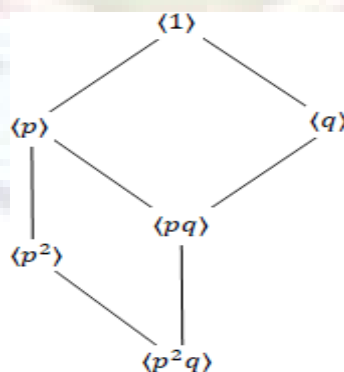
Observe that

$$\langle p^2q \rangle \subseteq \langle p^2 \rangle \subseteq \langle p \rangle \subseteq \langle 1 \rangle$$

$$\langle p^2q \rangle \subseteq \langle pq \rangle \subseteq \langle p \rangle \subseteq \langle 1 \rangle$$

$$\langle p^2q \rangle \subseteq \langle pq \rangle \subseteq \langle q \rangle \subseteq \langle 1 \rangle.$$

Figure 5.1 gives the required lattice.



**Figure 5.1** Subgroup lattice of  $\mathbb{Z}_{p^2q}$ .

**Question 5.13.** Prove that

$$H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{N} \right\} \subseteq GL(2, \mathbb{R})$$

is a cyclic subgroup.

**Solution:** We claim that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \forall n \in \mathbb{N}$$

We will prove the claim by induction on  $n$ . If  $n = 1$ , then it is trivially true. Suppose the claim holds  $n = k$  i.e.,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}.$$

We will show that it is true for  $n = k + 1$ . Consider

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Thus results holds for  $n = k + 1$ , therefore by induction it follows that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \forall n \in \mathbb{N}.$$

Thus

$$H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{N} \right\} = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle. \quad \blacksquare$$

**Question 5.14.** Let  $G$  be an abelian group. Show that  $H = \{g \in G : |g| \text{ divides } 12\}$  is a subgroup of  $G$ . What is the importance of 12 here? Will the proof be valid if we replace 12 by some other positive integer? State the general result.

**Solution:** Since  $|e| = 1$  which divides 12, therefore  $e \in H$  and hence  $H \neq \emptyset$ . Let  $g, h \in H$  be any two elements. Then  $g^{12} = e = h^{12}$ . Now consider

$$(gh^{-1})^{12} = g^{12}(h^{-1})^{12} = e. \quad [\because |h| = |h^{-1}| \Rightarrow (h^{-1})^{12} = e]$$

Thus  $|gh^{-1}|$  divides 12 and hence  $H$  is a subgroup of  $G$ . It is important to note that we did not use anything special about 12 here and hence we can easily generalize the result as follows: "If  $G$  be an abelian group, then for each  $n \in \mathbb{N}$ ,  $H_n = \{g \in G : |g| \text{ divides } n\}$  is a subgroup of  $G$ ". ■



## 6. SUMMARY

In this chapter, we defined cyclic group and generator of a cyclic group. We also noted that a generator of a cyclic group need not be unique. In fact we showed that if  $a$  is a generator of a cyclic group, then so would be  $a^{-1}$ . Also, we showed that order of every element of a finite cyclic group divides the order of that group. Further, we noticed that a group of prime order is always cyclic and that every element except identity is a generator of that group. If  $G$  is a cyclic group with  $a$  as one of its generator, then  $\{a^k : g.c.d(k, |G|) = 1\}$  is the set of all generators of  $G$  if  $G$  is finite and  $\{a, a^{-1}\}$  is the set of all generators if  $G$  is infinite. In addition to these, we saw that every non-identity element of an infinite cyclic group is of infinite order. In another section, we discussed subgroups of a cyclic group, what they inherit being the subgroup of a cyclic group? Is subgroup of a cyclic group cyclic? If yes, what about generators of a subgroup of a cyclic group? We saw that a subgroup of a cyclic group is cyclic and order of a subgroup is a divisor of the group. Further, in case of finite cyclic group we could describe all the possible subgroups. In fact, we showed that if  $G$  is a finite cyclic group of order  $n$ , then the number of distinct subgroups of  $G$  is the number distinct divisors of  $n$  and there is at most one subgroup of any given order. Also, we have seen that an infinite cyclic group has infinite number of subgroups.

## 7. EXERCISES

**Question 1.** Show that a group of order 3 must be cyclic. (Direct Proof)

**Question 2.** Let  $p$  be a prime. Show that a group with more than  $p - 1$  elements of order  $p$  is not cyclic?

**Question 3.** List all the elements of order 10 of  $\mathbb{Z}_{40}$ .

**Question 4.** Let  $|a| = n$ . Prove that  $\langle a^p \rangle = \langle a^q \rangle$  if and only if  $g.c.d(n, p) = g.c.d(n, q)$ .

**Question 5.** Show that for any finite group  $G$  there exists a positive integer (fixed)  $n$  such that  $a^n = e$  for all  $a \in G$ .

**Question 6.** Find all the generators of  $\mathbb{Z}$ .

**Question 7.** Let  $a$  and  $b$  be group elements such that order of  $a$  is odd and  $aba^{-1} = b^{-1}$ . Prove that  $b^2 = e$ .

**Question 8.** Let  $a$  be an element of a group and suppose that  $a$  has infinite order. How many generator does  $\langle a \rangle$  have?

**Question 9.** Let  $G$  cyclic group of order  $n$  and let  $k$  be any integer relatively prime to  $n$ . Prove that the map  $\Psi : G \rightarrow G$  defined as  $\Psi(x) = x^k$ .

**Question 10.** Let  $G = \langle a \rangle$  be a cyclic group of infinite order. Then there exists a map  $\Phi : \mathbb{Z} \rightarrow G$  such that :

(a)  $\Phi$  is bijective.

(b)  $\Phi(m + n) = \Phi(m)\Phi(n)$ .

**Question 11** How many elements of finite order does a cyclic group of infinite order have?

**Question 12** Let  $p$  be a prime and let  $n$  be a positive integer. Show that if  $x$  is an element of the group  $G$  such that  $x^{p^n} = 1$  then  $|x| = p^m$  for some  $m \leq n$ .

**Question 13.** Suppose that  $a$  has infinite order. Find all generators of the subgroup  $\langle a^3 \rangle$ .

**Question 14.** Let  $G$  be a cyclic group having exactly three subgroups:  $G$ ,  $\{e\}$ , and a subgroup  $H$  of order 7. Find the order of  $G$ ?

**Question 15.** Find the subgroup lattice for  $\mathbb{Z}_{12}$ .

**Question 16.** For a given prime  $p$  and a positive integer  $n$ , find the subgroup lattice for  $\mathbb{Z}_{p^n}$ .

**Question 17.** List the cyclic subgroups of  $U(30)$ .

**Question 18.** Show that  $U(20)$  is not cyclic.

**Question 19.** Let  $G$  be a group with exactly two non-trivial proper subgroups. Show that  $G$  is cyclic group. Also, prove that either  $|G| = p^3$  for some prime  $p$  or  $|G| = pq$  for distinct primes  $p, q$ .

## 8. REFERENCES

- [1] Joseph A. Gallian, Contemporary Abstract Algebra (Fourth Edition), Narosa Publishing House, India 1999.
- [2] Trygve Nagell, Introduction to Number Theory, John Wiley & Sons, New York, 1951.
- [3] Vijay K Khanna, Lattices and Boolean Algebras (Second Edition), 2004.
- [4] I.N Herstein, Topics in Algebra (Second Edition), Wiley Eastern Limited.
- [5] David S. Dummit and Richard M. Foote, Abstract Algebra, Third Edition, John Wiley & Sons, Inc.