# SuccessClap

## Best Coaching for UPSC MATHEMATICS

# UPSC MATHEMATICS STUDY MATERIAL

## BOOK- 08 Algebra

---

## Important Links

**Checklist for UPSC Mathematics: Click Here**

**Strategy for UPSC Mathematics: Click Here**

**22 Weeks Study Plan: Click Here**

**Download Question Bank Questions: Click Here**

**Our Courses: Click Here**

---

**Website: www.SuccessClap.com**

**Download Android App: Click Here**

**Join our Telegram Group: https://t.me/SuccessClap**

**For Query and Guidance WhatsApp: 9346856874**

# Table of Contents

# Number Theory

**0.1**. Theory of numbers deals with the properties of integers, $Z = \{.....,-3,-2,-1,0,1,2,3,.....\}$. We begin our study of number theory by first listing basic arithmetic properties and their elementary consequence of $Z$.

**0.2.** There exist two binary operations addition (+) and multiplication $(\bullet)$ in Z. For $a,b \in Z, a+b$ is called the sum and $a.b$ is called the product of $a$ and $b$. The basic properties are given below;

**$A_1$.** If $a,b,c \in Z$ , then $(a+b)+c = a+(b+c)$

**$A_2$.** If $a,b \in Z$ then $a+b = b+a$

**$A_3$.** There exists unique integer 0 such that $a+0 = a$ for each $a \in Z$. '0' is called the additive identity.

**$A_4$.** For an integer $a$ there exists a unique integer denoted by $-a$ such that $a+(-a) = 0$. $-a$ is called the negative of $a$, or the additive inverse of $a$.

**$M_1$.** If $a,b,c \in Z$, then $(a.b).c = a.(b.c)$.

**$M_2$.** If $a,b \in Z$ then $a.b = b.a$

**$M_3$.** There exists unique integer 1 such that $a.1 = a$ for each $a \in Z$. 1 is called the multiplicative identity.

**$M_4$.** If $a,b,c \in Z$ and $a \neq 0$ then $a.b = a.c \Rightarrow b = c$.

**D.** If $a,b,c \in Z$ then $a.(b+c) = a.b + a.c$.

**Def.** *If $a,b \in Z$ the difference of a and b, denoted by $a-b$, is defined as $a+(-b)$.*

**Some elementary consequences :**

1. If $a,b,c \in Z$ then $a+b = a+c \Rightarrow b = c$
2. $-0 = 0$
3. For $a \in Z, a.0 = 0$
4. For $a,b \in Z, a = b \Rightarrow -a = -b$.
5. For $a \in Z, -(-a) = a$.
6. For $a,b \in Z, -(a+b) = -a-b$.
7. For $a,b \in Z, a(-b) = -(ab)$
8. For $a,b \in Z, (-a)(-b) = ab$.
9. For $a,b \in Z, ab = 0 \Rightarrow a = 0$ or $b = 0$.
10. For $a,b \in Z, ab \neq 0 \Rightarrow a \neq 0, b \neq 0$.

**Def.** *If $a,b \in Z$ and $ab = 1$ then $a$ or $b$ is called a unit. The only units in Z are 1 and $-1$.*

For $a,b \in Z, ab = 1 \Rightarrow a = b = 1$ or $a = b = -1$

## 0. 3. THE ORDERING OF THE INTEGERS

There exists a subset N of Z, called the set of positive integers, with the following properties :

**$Q_1$.** If $a \in Z$, then one and only one of the following is true :

$(i)$ $a \in N$ $(ii)$ $a = 0$ $(iii)$ $-a \in N$

**$Q_2$.** If $a, b \in N$ then $a + b \in N$ and $a . b \in N$

From $Q_1$ and $Q_2$ we observe that (1) $0 \in N$ and (2) $1 \in N$

In view of the definition of N, if $a \in N$ , we say that *a is positive.*

Thus the set of integers is separated into three exhaustive and mutually exclusive sets : namely the set of positive integers N, the singleton set (0) and the set of negative integers.

**Definition.** *If $a, b \in Z$ and $b - a \in N$, then we say that a is less than b and write $a < b$. Alternatively we say that b is greater than a and write $b > a$.*

If $a < b$ or $a = b$, we write $a \le b$. If $a > b$ or $a = b$, we write $a \ge b$.

**Definition.** *If $a \in Z$ and $-a \in N$, then we say that a is a negative integer.*

Thus $a$ is negative, if $-a$ is positive.

If $a$ is positive, then $a > 0$. If $a$ is negative, then $a < 0$.

**Note :** If $a \in Z$, one and only one of the following is true :

$a \in N,\ a = 0,\ -a \in N$ or $a > 0, a = 0, a < 0$

## 0. 4. SOME IMPORTANT PROPERTIES OF ORDER IN Z

1. If $a, b \in Z$, then one and only one of the following is true : $a < b, a = b, a > b$
2. If $a, b, c \in Z$ then $(i)$ $a < b, b < c \Rightarrow a < c$ $(ii)$ $a > b, b > c \Rightarrow a > c$
3. If $a, b, c \in Z$, then $(i)$ $a < b \Rightarrow a + c < b + c$ $(ii)$ $a > b \Rightarrow a + c > b + c$
4. If $a, b, c \in Z$ then

   $(i)$ $a > b, c > 0 \Rightarrow ac > bc$, $(ii)$ $a > b, c < 0 \Rightarrow ac < bc$ $(iii)$ $a < b, c < 0 \Rightarrow ac > bc$
5. If $a \in Z, a \ne 0$, then $a^2 = a . a > 0$

## 0. 5. LEAST AND GREATEST INTEGERS IN A SUBSET OF Z.

Let $S \subset Z$ and $S \ne \phi$. If there exists an integer $n \in S$ such that $n \le m$ for all $m \in S$, we call $n$ the smallest or least integer in S. In such a case we say that S has a least member.

If there exists an integer $n \in S$ such that $n \ge m$ for all $m \in S$, we call $n$ the greatest integer in S.

## 0.6. WELL-ORDERING PRINCIPLE.

*Every non-empty set of positive integers has a least member.*

From the above principle we have two elementary consequences, namely,

$(i)$ 1 is the smallest positive integer and

$(ii)$ for $n \in N$ there does not exist an integer $a$ such that $n < a < n + 1$.

From the law of well ordering we can derive a principle known as principle of mathematical induction.

## 0.7. PRINCIPLE OF MATHEMATICAL INDUCTION

**First form :** Let S be a subset of N such that

$(i)$ $1 \in S$ and $(ii)$ $n \in S \Rightarrow n + 1 \in S$ then $S = N$.

**Second form :** Let $S$ be a subset of N such that $(i)$ $1 \in S$ and $(ii)$ $k \in S$ for all $k$ satisfying $1 \le k < n \Rightarrow n \in S$, then $S = N$.

## 0.8. MODULUS OR ABSOLUTE VALUE OF AN INTEGER

**Def.** *Let* $a \in Z$. *The modulus or absolute value of a denoted, by* $|a|$ *is defined as* $|a| = a$ *if* $a \geq 0$ and $|a| = -a$ *if* $a < 0$.

1. If $a \in Z, a \neq 0$, then $|a| \in N$ and hence $|a| > 0$
2. $|a| = 0$, if and only if $a = 0$.
3. For $a, b \in Z, |a| = |b| \Leftrightarrow a = \pm b$
4. For $a \in Z, -|a| \leq a \leq |a|$
5. For $a, b \in Z, |a+b| \leq |a| + |b|$
6. For $a, b \in Z, |a.b| = |a|.|b|$
7. For $c > 0, -c \leq b \leq c \Leftrightarrow |b| \leq c$

## 0.9. THE EUCLID'S DIVISION ALGORITHM

The theorem known as division algorithm plays an important role in the development of number theory. The proof of this theorem is based on the well ordering principle of positive integers.

**Theorem : If $a, b \in Z$ and $a \neq 0$, then there exist unique integers $q, r$ such that $b = aq + r, 0 \leq r < |a|$.**

**Note 1. :** If $a, b$ are positive integers, then there exist unique pair of integers $q, r$ such that $b = aq + r, 0 \leq r < a$.

**2.** The above theorem establishes uniqueness of division.

**3.** If $b = aq + r, \quad 0 \leq r < |a|$ then

$b$ is called the **dividend,** $a$ is called the **divisor,**

$q$ is called the **quotient** and $r$ is called the **remainder.**

**4.** When $b$ is any integer and $a = 2$, by division algorithm $b = 2q + r, 0 \leq r < 2$. In this case the possible values of $r = 0, 1$.

If $r = 0$ then $b = 2q$ and $b$ is called **even integer.**

If $r = 1$ then $b = 2q + 1$ and $b$ is called **odd integer.**

**5.** In the division algorithm, if $r = 0$ then $b = aq$.

## 0. 10. DIVISOR

**Definition.** *Let* $a, b$ *be two integers and* $a \neq 0$. *If there exists an integer* $q$ *such that* $b = aq$, *then we say that* **a divides b** *or* **a is a factor of b** *or* **a is a divisor b** *or* **b is a multiple of a.**.

$a$ divides $b$ is denoted by $a | b$. If $a$ is not a divisor of $b$, then we write $a \nmid b$.

**$a | b \Leftrightarrow b = aq$, where $q$ is an integer.** If $b$ is a multiple of $a$, we write $b = M(a)$

***e.g.*** $5 | 20,\ 3 | 12,\ 4 \nmid 21 \Rightarrow 20 = M(5), 12 = M(3), 21 \neq M(4)$.

**Note 1.** Since $0 = a.0$, 0 is a multiple of every integer.

*i.e.* $a | 0$, for every non-zero integer $a$.

**2.** For a non-zero integer '$a$' we have $a = a.1 = (-a).(-1)$.

Therefore $a, -a, +1, -1$ are divisors of $a$.

**3.** If $a \neq 0$, then $a$ has at least two divisors.

If $a \neq 0$ and $a \neq \pm 1$, then $a$ has atleast four divisors.

**Properties** **1.** If $\mathbf{a,b\in Z}$ then $\mathbf{a\mid b\Rightarrow b=0}$ **or** $\mathbf{|a|\le|b|}$

**2. If** $\mathbf{a,b,c\in Z}$ **then** $\mathbf{a\mid b,b\mid c\Rightarrow a\mid c}$

**3. If** $\mathbf{a,b\in Z}$ **then** $\mathbf{a\mid b}$ **and** $\mathbf{b\mid a\Rightarrow a=\pm b}$

**4.** $\mathbf{a\mid b,a\mid c\Rightarrow a\mid bx+cy;x,y\in Z}$ **and in particular,**

$a\mid b,a\mid c\Rightarrow a\mid b+c$ and $a\mid b-c$

## 0. 11. EVEN AND ODD INTEGERS

**Definition.** If $a\in Z$ and $2\mid a$ then '$a$' is called *even integer*

If $a\in Z$ and $2\nmid a$ then '$a$' is called odd integer.

From Note (4) or Art. 8.9 we have '$a$' is even integer $\Leftrightarrow a=2q$ where $q\in Z$

'$a$' is odd integer $\Leftrightarrow a=2q+1$ where $q\in Z$

**Some properties :** 1. The sum and product of two even integers is even integer.

2. The sum of two odd integers is even integer

3. The product of two odd integers is odd integer.

4. The sum of even integer and odd integer is odd integer.

5. The product of even integer and odd integer is even integer.

6. The product of two consecutive integers is divisible by 2.

For, the product consists of an even integer which is divisible by 2.

**Ex. 1.** *Find* $q,r$ *of the division algorithm if* $b=-2044$ *and* $a=130$

**Sol.** By long division : $2044=130(15)+94\Rightarrow -2044=-130(15)-94$

(Note that $r\neq -94$ as $0<-94<130$ is not true)

$\therefore -2044=[-130(15)-130]+130-94=130(-16)+36$. Which is of the form $b=aq+r$, where $q=-16\in Z$ and $r=36\in Z$ such that $0<r<130$.

**Ex. 2.** *If* $n$ *is even positive integer, prove that* $2^{2n}-1$ *is divisible by 15.*

**Sol.** $n$ is even integer $\Rightarrow n=2m,m\in N$

$2^{2n-1}=2^{4m}-1=(2^4)^m-1=16^m-1=(16-1)(16^{m-1}+16^{m-2}+....+1)=15q$

where $q=16^{m-1}+16^{m-2}+....+1\in N$. $\therefore$ 15 divides $2^{2n-1}$ when $n$ is even.

**Ex. 3** *Prove that every odd integer is of the form* $4n+1$ *or* $4n-1$

**Sol.** Let $p$ be an odd integer.

By division algorithm : $p=4n+r$ where $n,r\in Z$ and $0\le r<4$

$\therefore p=4n+0$ or $4n+1$ or $4n+2$ or $4n+3$

Since $p$ is odd; $p\neq 4n$ and $p\neq 4n+2$ which are even.

$\therefore p=4n+1$ or $4n+3$. But $p=4n+3=4n+4-1=4(n+1)-1=4m-1$

$\therefore p$ is of the form $4n+1$ or $4n-1$ where $n\in Z$.

**EXERCISE 0 ( *a* )**

1. Find $q,r$ of the division algorithm if (*i*) $b=7153,a=17$ (*ii*) $b=-6080,a=-42$
2. Prove that $a\mid b\Leftrightarrow|a|\mid|b|$.
3. If $a\mid b$ and $c\in Z$ then prove that $a\mid bc$.
4. If $a,b,c\in Z$ then prove that $ac\mid bc\Rightarrow a\mid b$.

5. If $a \mid b$ and $c \mid d$ then prove that $ac \mid bd$.
6. Prove that the sum and product of two even integers is even integer.
7. Prove that the product of even integer and odd integer is even integer.
8. If $a, b$ are odd integers prove that $a^2 + b^2$ is even.
9. If $n$ is an odd integer prove that $(n^2 - 1)$ is divisible by 8.
10. By induction prove that the product of three consecutive integers is divisible by 6.

**ANSWERS**

1. $(i)\ q = 420, r = 13\ \ (ii)\ q = 145, r = 10$

## 0. 12. GREATEST COMMON DIVISOR (G. C. D)

On the basis of simple divisibility properties, the integers are separated into four mutually exclusive categories - Zero, Unit, Prime and Composite. In this chapter we study the properties of primes as the fundamental building blocks in terms of which all the composite numbers may be uniquely represented.

**Definition. Common Divisor :** *Let $a, b$ be integers. If $d \in Z$ is such that $d \mid a$ and $d \mid b$ then $d$ is called a common divisor of $a$ and $b$.*

**e.g. 1.** $3 \mid -15$ and $3 \mid 21 \Rightarrow 3$ is a common divisor of $-15, 21$.

**2.** $\pm 1$ are common divisors of $a, b$ where $a, b \in Z$.

**Note 1.** For any two integers $a, b$ there exists a common divisor which is positive.

**2.** If $a, b \in Z$ and $a \neq 0$ then the set of common divisors of $a, b$ is finite.

**Definition. G. C. D. :** *Let $a, b$ be two integers so that atleast one of them is not equal to zero. If there exists a positive integer 'd' such that (i) d is a common divisor of a, b and*

*(ii) every common divisor of a, b is a divisor of d, then d is called the Greatest Common Divisor (G. C.D) of a, b.*

**Notation :** G. C. D. of $a, b = (a, b) > 0$

***e.g.*** 2,3 and 6 are the common divisors of 18,24.

Also $2 \mid 6$ and $3 \mid 6$. Therefore $6 = (18, 24)$.

**Definition.** *Let $\{a_1, a_2, ....., a_n\}$ be a finite set of integers, not all zero. If there exists a positive integer 'd' such that (i) d is a common divisor of $a_1, a_2, ....., a_n$ and*

*(ii) every common divisor of $a_1, a_2, ....., a_n$ is a divisor of d, then d is called the greatest common divisor of $a_1, a_2, ....., a_n$. We write $d = (a_1, a_2, ....., a_n)$*

**Note 1.** $(a, b) = (b, a)$ **2.** If $d = (a, b)$ then $d \geq 1$

**3.** If $d = (a, b)$ then $d$ is unique. **4.** $(a, a) = |a|$ **5.** $(a, b) = |a| \Leftrightarrow a \mid b$.

**6.** $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ or $(a, b) = (|a|, |b|)$

**7.** G. C. D. of two consecutive natural numbers = 1.

**Theorem 1.** ***If*** $\mathbf{a, b \in Z, b \neq 0}$ ***and*** $\mathbf{a = bq + r, 0 \leq r < |b|}$ ***then*** $\mathbf{(a, b) = (b, r)}$.

**Proof :** Let $(a, b) = d_1$ and $(b, r) = d_2$.

$(a, b) = d_1 \Rightarrow d_1 \mid a$ and $d_1 \mid b \ \Rightarrow d_1 \mid (a - bq)$ where $q \in Z \Rightarrow d_1 \mid r$. $(\because a - bq = r)$

$d_1 \mid b$ and $d_1 \mid r \Rightarrow d_1$ is a common divisor of $b$ and $r$.

Since $(b, r) = d_2$, by def. of G. C. D., $d_1 \mid d_2$ .... (1)

Similarly starting with $(b,r)=d_2$ we can prove that $d_2 \mid d_1$ .... (2)

From (1) and (2), $d_1=d_2$ (since $d_1,d_2$ are positive).

**Theorem 2.** ***If*** **a,b,c** ***are integers, not all zero, then*** **(a, b, c) = ((a, b), c).**

**Theorem 3.** ***If*** **(a, b) = d** ***there exist*** **x,y∈ z** ***such that*** **d = ax + by.** ***Further the elements of*** **{ax + by/x,y∈ z}** ***are the multiples of*** **d.**

**Note. 1.** If d = $(a, b)$ the $d = ax+by;\ x,y \in Z$ is not unique.

For, $d = ax + by = a(x - b) + b(y + a) = ax_1 + by_1$ where $x_1 = x - b$ and $y_1 + a \in Z$.

**2.**For $d = (a, b)$ and $c = ax+by \in z \Leftrightarrow d/c$.

**3.** $(a, b, c) = d$ then there exist $x, y, z \in z$ such that $d = ax+by+cz$.

**e.g.** If possible, find $x, y \in z$ such that $15 = 6x + 12y$. We have $(6, 12) = 6 = d$ and $c = 15 \in 6 \nmid 15$. From Note (2) we cannot write 15 in the form $6x + 12y$.

### 0. 13. CONSTRUCTION OF G. C. D. FROM DIVISION ALGORITHM

Let $a,b$ be two integers such that at least one of $a,b$ is non-zero.

**Case (1).** If $a=0$, then $(a,b)=|b|$. If $b=0$, then $(a,b)=|a|$

**Case (2).** Let $a\neq 0$ and $b\neq 0$

By division algorithm we have the following finite sequence of divisions :

$a=bq_1+r_1;\ 0\le r_1<|b|;\quad b=r_1q_2+r_2;\ 0\le r_2<r_1;\quad r_1=r_2q_3+r_3;\ 0\le r_3<r_2;$

$-------;\ -------\ -------;\ -------\ -------;\ -------$

$r_{k-2}=r_{k-1}\,q_k+r_k;\ 0\le r_k<r_{k-1},\quad r_{k-1}=r_k\,q_{k+1}+r_{k+1};\ 0\le r_{k+1}<r_k$

Since $0\le r_{k+1}<r_k<r_{k-1}<.....<r_1<|b|$, the successive remainders form a decreasing sequence of positive integers. It follows that in a finite number of steps, say, $(k+1)^{th}$ step the process will terminate so that $r_{k+1}=0$.

Therefore the last non-zero remainder in the above process is $r_k$.

Hence from the above theorem, $(a,b)=(b,r_1)=(r_1,r_2)=.....=(r_{k-1},r_k)=(r_k,0)=r_k$

$\therefore$ the last non-zero remainder $r_k$ is the G. C. D. of the given numbers $a,b$.

**Theorem 3.** ***If*** **(a,b) = d** ***then there exists*** **x,y ∈ Z** ***such that*** **d = ax + by** ***and d is the least positive value of ax+by where x, y range over all integers.***

**Note 1.** If $d=(a,b)$, the numbers $x,y\in Z$ such that $d=ax+by$ are not unique.

For, if $d=ax+by$ then $d=a(x-b)+b(y+a)=ax_1+by_1; x_1=x-b, y_1=y+a.$

**2.** If $d=(a,b)$ then for $c\in Z, c=ax+by$ if and only if $d$ is $a$ divisor of $c$.

**3.** The G. C. D. of $a,b$ is the least positive value of $ax+by$ where $x,y$ range over all integers.

**4.** If $(a,b,c)=d$ then there exist $x,y,z\in Z$ such that $d=ax+by+cz$.

The G. C. D. of $a,b,c$ is the least positive value of $ax+by+cz$ where $x,y,z$ range over all integers.

***e.g.*** *Find* $x,y\in Z$ *such that* $15=6x+12y$ *if possible.*

We have $(12,6)=6=d$ and $c=15$.

Since 6 is not a divisor of 15, it is not possible to write 15 in the form $6x+12y$.

## 0.14. RELATIVELY PRIME OR MUTUALLY PRIME OR COPRIME INTEGERS

**Definition.** *If* $(a,b)=1$ *then* $a,b$ *are said to be relatively prime or mutually prime.*

***e.g.*** Since (15,8)=1, 15 and 8 are relatively prime.

**Note.** If $a,b$ are relatively prime then $a,b$ have no common divisor.

**Theorem 1.** $\mathbf{a,b\in Z}$ ***are relatively prime iff there exist*** $\mathbf{x,y\in Z}$ ***such that*** $\mathbf{ax+by=1}$.

**Theorem 2.** ***If*** $\mathbf{(a,b)=1}$ ***and*** $\mathbf{a\mid bc}$ ***then*** $\mathbf{a\mid c}$.

**Proof.** $a\mid bc \Rightarrow bc=aq_1; q_1\in Z$

$(a,b)=1\Rightarrow$ there exist $x,y\in Z$ such that $ax+by=1$

$ax+by=1\Rightarrow c(ax+by)=c \Rightarrow c(ax)+(cb)y=c \Rightarrow a(cx)+(aq_1)y=c$

$\Rightarrow a(cx+q_1y)=c \Rightarrow aq=c$ where $q=cx+q_1y\in Z\Rightarrow a\mid c$

**Theorem 3.** ***If*** $\mathbf{(a,b)=d,}$ ***then*** $\mathbf{(ka,kb)=\mid k\mid d}$ ***where*** $\mathbf{k\in Z-\{0\}}$.

**Note 1 :** If $m>0,(ma,mb)=m(a,b)$ **2.** If $(a,b)=d$ then $(a/d,b/d)=1$

**3.** If $(a,b)=d$ and $a=Al, b=Bl$ then $(A,B)=d/l$

**4.** If $d\mid a, d\mid b$ and $d>0$ then $(a/d,b/d)=1/d(a,b)$

**Theorem 4.** ***If*** $\mathbf{(a,b)=1}$ ***and*** $\mathbf{(a,c)=1}$ ***then*** $\mathbf{(a,bc)=1.}$

**Note 1.** Conversely, $(a,bc)=1\Rightarrow (a,b)=1,(a,c)=1$

**2.** By induction $(a,b)=1\Rightarrow (a,b^n)=1$ where $n\in N$

## 0.15. LEAST COMMON MULTIPLE (L.C.M)

**Definition.** *Let a,b be two non-zero integers. The L.C.M. of a,b is the unique positive integer m such that* $(i)$ $a\mid m, b\mid m$ *and* $(ii)$ $a\mid k, b\mid k\Rightarrow m\mid k$. )

**Notation :** L.C.M. of $a,b=[a,b]$. ***e.g.*** $[5,-10]=10,[16,20]=80$

**Note 1. :** The L.C.M. of two consecutive natural numbers is equal to their product. That is, $[2,3]=6,[14,15]=210$

**2.** $[a,b]=[-a,b]=[a,-b]=[-a,-b]$

**3.** The L.C.M. of two integers is **positive integer.**

**4.** If $a\neq 0, b\neq 0\in Z$ then $|ab|$ is a common multiple of $a,b$. Hence $[a,b]\mid\mid ab\mid$.

**Some Properties :**

1. If $m>0; a,b\in Z$ then $[ma,mb]=m[a,b]$
2. If $a\neq 0, b\neq 0\in Z$ then $a\mid c, b\mid c\Rightarrow [a,b]\mid c$
3. $a\mid ab, b\mid ab\Rightarrow [a,b]\mid ab$
4. If $(a,b)=d$ and $[a,b]=m$ then $dm=\mid ab\mid$
5. If two integers are relatively prime i.e. $(a,b)=1$ then $[a,b]=\mid ab\mid$

**Ex. 1.** *If* $d=(826,1890)$ *using division algorithm compute d and then express as a linear combination of 826, 1890.*

**Sol** : By Euclid algorithm :

$1890=826(2)+238; r_1=238$ ... (1) $\qquad 826=238(3)+112; r_2=112$ ... (2)

$238=112(2)+14; r_3=14$ ...(3) $\qquad 112=14(8)+0; r_4=0$ ... (4)

$\therefore r_3=14$ is the last non-zero remainder $\qquad \therefore d=$ G. C. D. of 826, 1890 = 14.

Again, $d=14=238+(-2)112$ using (3) $=238+(-2)\{826+(-3)238\}$ using (2)

$=(-2)826+(7)238$ $=(-2)\,826+7\{1890+(-2)826\}$ using (1)

$=(-16)826+(7)1890$

**Ex. 2 :** *If* $a = 2210, b = 493$ *find* $(a,b)$ *and hence* $[a,b]$.

**Sol.** By Euclid algorithm : $2210 = 493(4) + 238;\ r_1 = 238$

$493 = 238(2) + 17;\ r_2 = 17$ $\qquad 238 = 17(14) + 0;\ r_3 = 0$

$\therefore\ (a,b) = (2210,493) = 17$ $\qquad$ and $|ab| = 2210 \times 493$

$$\therefore\ [a,b] = \frac{|ab|}{(a,b)} = \frac{2210 \times 493}{17} = 130 \times 493$$

**Ex. 3. :** *If* $(a,b) = 1$ *show that* $(a+b, a-b) = 1$ *or* $2$

**Sol.** Let $(a+b, a-b) = d$

$\therefore d \mid a+b$ and $d \mid a-b \Rightarrow d \mid a+b+a-b$ and $d \mid a+b-a+b$

$\Rightarrow d \mid 2a$ and $d \mid 2b$. $\Rightarrow d$ is a common divisor of $2a, 2b$.

But $(a,b) = 1 \Rightarrow (2a, 2b) = 2$ $\therefore d \mid 2$ and hence $d = 1$ or $2$

**Ex. 4 :** *If* $a \mid x, b \mid x$ *and* $(a,b) = 1$ *then prove that* $ab \mid x$. *Give an example to prove that* $a \mid x, b \mid x$ *need not imply* $ab \mid x$.

**Sol.** $a \mid x, b \mid x \Rightarrow x = aq_1, x = bq_2$ where $q_1, q_2 \in Z$

$(a,b) = 1 \Rightarrow$ there exist $l, m \in Z$ such that $al + bm = 1$

$\Rightarrow alx + bmx = x \Rightarrow al(bq_2) + bm(aq_1) = x \Rightarrow ab(lq_2 + mq_1) = x$

$\Rightarrow x = (ab)q$ where $q = lq_2 + mq_1 \in Z$ $\qquad \therefore\ ab \mid x$

We have $2 \mid 12,\ 4 \mid 12$ does not imply $2.4 = 8 \mid 12$ because $(2,4) = 2 \neq 1$.

## EXERCISE 0 ( *b* )

1. Find the G.C.D. of $(i)$ $1128, 33$ $(ii)$ $-308, 136$.
2. Find $d = (1819, 3587)$ and hence express $d$ as a linear combination of 1819and 3587.
3. Find integers $x, y$ such that $243x + 198y = 9$.
4. If $n \in N$ find $(n, n+1)$ and $[n, n+1]$.
5. If $a \mid b$ find $(a,b)$ and $[a,b]$.
6. If $a \mid c, b \mid c$ and $(a,b) = d$ prove that $d \mid c$.
7. Show that $(a,b) = (a, a+b)$.
8. If $d = (a,b) = ax + by$ prove that $x, y$ are relatively prime.
9. If $(a,b) = d$ and $K \in Z - \{0\}$ then prove that $(Ka, Kb) = |K| d$.
10. Find $[a,b]$ if $(i)$ $a = 60, b = 61$ $(ii)$ $a = 482, b = 1687$.
11. Prove that $(a,m) = (b,m) = 1 \Leftrightarrow (ab,m) = 1$.
12. If $(a,b) = d$ and $[a,b] = m$ prove that $dm = |ab|$.
13. If $ax + by = 1$ show that $(a,b) = (a,y) = (x,b) = (x,y) = 1$.
14. If $(a,b) = 1$ prove that $(a^2, ab, b^2) = 1$.
15. Prove that $(a,b) = 1 \Leftrightarrow$ there exist $x, y \in Z$ such that $ax + by = 1$.

## ANSWERS

1. $(i)$ 3 $(ii)$ 4 $\qquad$ 2. $d = 17, x = 71, y = -36$ $\qquad$ 3. $x = 9, y = -11$ $\qquad$ 4. $1, n(n+1)$
5. $a, b$ $\qquad$ 10. $(i)$ 3660 $(ii)$ 3374

## 0.16. PRIMES AND COMPOSITE NUMBERS

**Definition.** *The positive integer* $p>1$ *is said to be a* **prime** *if the only divisors of p are* $\pm 1$ *and* $\pm p$. *The other positive integers greater than 1 are called* **composite.**

'$a$' is a prime $\Rightarrow$ $a = a(1)$ and $a = 1(a)$.

'$a$' is composite $\Rightarrow$ there exist integers. $b, c$ such that $a = bc$ where $1 < b < a, 1 < c < a$.

**Note 1.** 2 is the only even integer which is a prime. Every other even integer has 2 as a factor. Therefore $p$ is a prime and $p \neq 2$ then $p$ is an odd integer.

**2.** 1 is neither considered as a prime number nor composite and 1 is called unit.

**3. Imp.** If $p$ is a prime and $a \in Z$ then $p \mid a$ or $(p, a) = 1$

**4.** A composite number has atleast 3 divisors.

**Theorem 1. (Euclid's Lemma).**

**If p is a prime and a, b ∈ Z then p | ab ⇒ p | a or p | b .**

**Proof.** If $p \mid b$, then the theorem is proved.

Let $p \nmid b$. Then $(p, b) = 1$, as $p$ is a prime.

$(p, b) = 1 \Rightarrow$ there exist $x, y \in Z$ such that $px + by = 1 \Rightarrow apx + aby = a$. ... (1)

$p \mid ab \Rightarrow ab = pq$ where $q \in Z$ ..... (2)

$\therefore$ from (1) and (2) $apx + pqy = a \Rightarrow p(ax + qy) = a$

$\Rightarrow pq' = a$ where $q' = ax + qy \Rightarrow p \mid a$. Hence $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

**Cor.** If $p$ is a prime and $a_1, a_2, ....., a_n \in Z$ then

$p \mid (a_1, a_2, ....., a_n) \Rightarrow p \mid a_1$ or $p \mid a_2, ....., $ or $p \mid a_n$.

**Note.** If $p$ is not a prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ is not true.

***e.g.*** 6 is a factor of 144 = (9) (16). But $6 \nmid 9$ and $6 \nmid 16$ since 6 is not a prime.

**Cor.** If $p$ is a prime and $a, b \in Z$ are such that $0 < a, b < p$ then $p \nmid ab$.

**0.17.** The fundamental theorem of arithmetic, stated below, shows the importance of prime numbers, since they generate the set of all positive integers greater than one. Thus primes are fundamental numbers interms of which all the composite numbers may be conveniently and uniquely represented.

**Theorem 1.** ***(The fundamental theorem of arithmetic). Every positive integer a > 1 can be expressed as a product of primes uniquely.***

**Note 1. :** If $a \neq \pm 1$ and $a \in Z$ then by the above theorem $|a| = p_1, p_2 ..... p_n$ where $p_1, p_2 ..... p_n$ are primes. Therefore $a = \pm |a| = \pm (p_1 . p_2 ..... p_n)$

**2.** Every positive integer $a > 1$ can be written uniquely in the form $a = p_1^{\alpha_1} p_2^{\alpha_2} .....p_n^{\alpha_n}$, where $p_1, p_2, .....p_n$ are primes ; $1 < p_1 < p_2 < ..... < p_n$ and each $\alpha_1, \alpha_2, .....\alpha_n$ is a positive integer.

The above representation of '$a$' is called prime factorisation of '$a$' in **"canonical form"** or **"Prime power factorisation of a"**

**3.** If $a = p_1^{\alpha_1} p_2^{\alpha_2} .....p_n^{\alpha_n}$ and $b = q_1^{\beta_1} q_2^{\beta_2} .....q_m^{\beta_m}$ then

(*i*) $a = b \Leftrightarrow n = m, p_i = q_i$ and $\alpha_i = \beta_i$ for $i = 1, 2, ....., n$

(*ii*) G.C.D. of $a, b = p_1^{m_1} p_2^{m_2} .....p_r^{m_r}$ where $p_1, p_2, ....., p_r$ are common prime factors of $a, b$ and $m_i$ is the minimum exponent of $p_i$ as one compares the exponents of $p_i$ in $a, b$.

(*iii*) L.C.M. of $a,b = p_1^{m_1} p_2^{m_2} .....p_s^{m_s}$ where $p_1, p_2, ....., p_s$ are all prime factors of both $a,b$ and $m_i$ is the maximum exponent of $p_i$ as one compares the exponents of $p_i$ in $a,b$.

***e.g.*** $a = 2520 = 2^3 \times 3^2 \times 5^1 \times 7^1; b = 4950 = 2^1 \times 3^2 \times 5^2 \times 11^1$

$(a,b) = 2^1 \times 3^2 \times 5^1 = 90$ (minimum exponents of common factors)

$[a,b] = 2^3 \times 3^2 \times 5^2 \times 7^1 \times 11^1 = 138600$ (maximum exponents of all factors).

## 0. 18. THE NUMBER OF DIVISORS OF A POSITIVE INTEGER N

By fundamental theorem,

$N = p_1^{\alpha_1} p_2^{\alpha_2} .....p_r^{\alpha_r}$ where $1 < p_1 < p_2 < ..... < p_r$ and $\alpha_1, \alpha_2, .....\alpha_r$ are positive integers.

Consider the product

$P = (1 + p_1 + p_1^2 + ..... + p_1^{\alpha_1})(1 + p_2 + p_2^2 + ..... + p_2^{\alpha_2}) ..... (1 + p_r + p_r^2 + ..... + p_r^{\alpha_r})$

General term of this product is $p_1^{\beta_1} p_2^{\beta_2} .....p_r^{\beta_r}$

where $0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, .....0 \le \beta_r \le \alpha_r$

Clearly, $p_1^{\beta_1} p_2^{\beta_2} .....p_r^{\beta_r}$ is a factor of $p_1^{\alpha_1} p_2^{\alpha_2} .....p_r^{\alpha_r} = N$

Conversely, every factor of N is a term of P.

Hence, the number of factors of N = number of terms of P

$$= (1+\alpha_1)(1+\alpha_2).....(1+\alpha_r)$$

**Notation.** The number of positive integral divisors (factors) of a positive integer N is denoted by $\tau(N)$

## 0. 19. THE SUM OF ALL THE DISTINCT POSITIVE INTEGRAL DIVISORS OF A POSITIVE INTEGER

By fundamental theorem,

$N = p_1^{\alpha_1} . p_2^{\alpha_2} .....p_r^{\alpha_r}$ where $1 < p_1 < p_2 < ..... < p_r$ and $\alpha_1, \alpha_2, .....\alpha_r$ positive integers.

Consider the product

$P = (1 + p_1 + p_1^2 + ..... + p_1^{\alpha_1})(1 + p_2 + p_2^2 + ..... + p_2^{\alpha_2}) .....(1 + p_r + p_r^2 + ..... + p_r^{\alpha_r})$

General term of P is $p_1^{\beta_1} . p_2^{\beta_2} .....p_r^{\beta_r}$ where $0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, ....., 0 \le \beta_r \le \alpha_r$.

$\therefore$ Every term of P is a factor of N and conversely every factor of N is a term of P.

$\therefore$ the sum of all the distinct divisors of N = the sum of all the terms of P

$= (1 + p_1 + p_1^2 + ..... + p_1^{\alpha_1})(1 + p_2 + p_2^2 + ..... + p_2^{\alpha_2}) .....(1 + p_r + p_r^2 + ..... + p_r^{\alpha_r})$

$$= \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right) ..... \left(\frac{p_r^{\alpha_r+1} - 1}{p_r - 1}\right)$$

**Notation.** The sum of all the distinct positive integral divisors of $N > 1$ is denoted by $\sigma(N)$.

## 0. 20. PERFECT NUMBER

If the sum of all divisors of $n > 1$, is equal to $2n$ then $n$ is called a perfect number.

**Note.** If $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is a perfect number.

***e.g.*** $n = 28 = 2^2 \times 7^1$ is a perfect number, for,

$$\sigma(28) = \left(\frac{2^3 - 1}{2 - 1}\right)\left(\frac{7^2 - 1}{7 - 1}\right) = 7 \times 8 = 56 = 2 \times 28$$

## 0.21. BRACKET FUNCTION

**Definition.** *The function* $I: R \to Z$ *defined by* $I(x) = n$ *where* $n \le x < n+1$ *is called the* ***bracket function*** *or the* ***step function*** *or the* ***integral part function.***

**Notation.** Integral part of $x \in R$ is denoted by $I(x)$ or $[x]$.

**Definition.** *If* $x \in R, x-[x]$ *is called the* ***Fractional part*** *of* $x$.

**Note 1.** $[x] \le x < [x]+1$ or $x-1 < [x] \le x$.

**2.** For every $x \in R, x \ge [x]$ i.e. $x-[x] \ge 0$ and hence the fractional part of any $x \in R$ is non-negative. **3.** $x \in Z \Leftrightarrow [x] = x$

***e.g.*** **1.** $4 < \frac{14}{3} = 4\frac{2}{3} < 5 \Rightarrow \left[\frac{14}{3}\right] = 4$ **2.** $0 < \frac{3}{4} < 1 \Rightarrow \left[\frac{3}{4}\right] = 0$

**3.** $-4 \le -\sqrt{10} < -3 \Rightarrow [-\sqrt{10}] = -4$ **4.** $3 < \pi = \frac{22}{7} < 4 \Rightarrow [\pi] = 3$

**Some important properties :**

1. For $x \in R, [x] \le x < [x]+1 \Rightarrow x$ lies between $[x]+0$ and $[x]+1 \Rightarrow x = [x]+\theta$ where $0 \le \theta < 1$.
2. If $a \in Z$ and $b \in N$ then $\left[\frac{a}{b}\right]$ = the quotient when '$a$' is divided by '$b$'
3. If $m \in Z$ and $x \in R$ then $[x+m] = [x]+m$.
   For; $x = [x]+\theta$ where $0 \le \theta < 1 \Rightarrow x+m = [x]+m+\theta$ where $0 \le \theta < 1$
   $\Rightarrow [x]+m \le x+m < [x]+m+1 \Rightarrow [x+m] = [x]+m$
4. If $x \in R$ then $[x]+[-x] = 0$ when $x$ is integer and $[x]+[-x] = -1$ when $x$ is non-integer.
5. $x, y \in R \Rightarrow [x+y] \ge [x]+[y]$
6. If $p$ is a prime number in $n!$ then the highest power of $p$ contained in $n!$
   $= \sum_{r=1}^{\alpha} I\left(\frac{n}{p^r}\right)$ where $p^{\alpha} < n < p^{\alpha+1}$.
   ***e.g.*** As $5^1 < 14 < 5^2$, , highest power of 5 in $14! = \sum_{r=1}^{1} I\left(\frac{n}{p^r}\right) = I\left(\frac{14}{5}\right) = I\left(2\frac{4}{5}\right) = 2$
7. The product of $r$ consecutive integers is divisible by $r!$
   For $x \in N$, product of $r$ consecutive integers
   $= P = (x+1)(x+2).....(x+r) = \frac{(x+r)!}{x!} \Rightarrow \frac{P}{r!} = \frac{(x+r)!}{x!\,r!} = {}^{x}C_r =$ +ve integer.
8. **The number of pairs of factors of a given number N which are prime to each other:**
   Let $N = p_1^{\alpha_1} p_2^{\alpha_2} .....p_r^{\alpha_r}$.
   Since any two factors into which N is resolved are prime to each other, if one factor contains $p_1$ then the other does not contain $p_1$.
   The factors under consideration = the different terms of the product
   $(1+p_1^{\alpha_1})(1+p_2^{\alpha_2}).....(1+p_r^{\alpha_2}) = (1+1)(1+1).....(1+1)$ to $r$ factors $= 2^r$
   $\therefore$ Number of pairs $= \frac{1}{2} \times 2^n = 2^{n-1}$

9. **If** $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ **is not a perfect square then the number ways in which N can be resolved into two factors** $= \frac{1}{2}(1+\alpha_1)(1+\alpha_2)\ldots\ldots(1+\alpha_r)$

If N is a perfect square then the number of ways $= \frac{1}{2}\{(1+\alpha_1)(1+\alpha_2)\ldots\ldots(1+\alpha_r)+1\}$

**Ex. 1.** *Express 67375 as the product of primes.*

**Sol.** $67375 = 5\times13475 = 5^2\times2695 = 5^3\times539 = 5^3\times7\times77 = 5^3\times7^2\times11^1$

**Ex. 2.** *By writing* $a = 6540, b = 1206$ *in the canonical form find* $(a,b)$ *and* $[a,b]$. *Also verify* $(a,b)[a,b] = |ab|$.

**Sol.** $a = 6540 = 2\times3270 = 2^2\times1635 = 2^2\times3\times545 = 2^2\times3^1\times5^1\times109$

$b = 1206 = 2\times603 = 2^1\times3^1\times201^1 = 2^1\times3^2\times67$

Common prime factors in $a,b = 2,3$ and their minimum exponents = 1,1

$\therefore$ G. C. D of $a,b = 2^1\times3^1 = 6$

All prime factors in $a,b = 2,3,5,67,109$ and their maximum exponents = 2, 2, 1, 1, 1

$\therefore$ L.C.M. of $(a,b) = 2^2\times3^2\times5^1\times67^1\times109^1$

Also $|ab| = ab = 2^3\times3^3\times5\times67\times109 = (a,b)[a,b]$

## EXERCISE 0 ( *c* )

1. Write each in canonical form :

(*i*) 2560 (*ii*) 4116 (*iii*) 29645

2. By writing each set in the cannonical form find G.C.D. and L.C.M

(*i*) 1337,−501 (*ii*) 3367,3219 (*iii*) 1274,3087,1085

3. Find the number of divisors and their sum :

(*i*) 3675 (*ii*) 18375 (*iii*) 74088

4. Find the highest power of (*i*) 5 *in* 80! ***(A.U. 05)*** (*ii*) 3 *in* 1000! (*iii*) 7 *in* 50!

5. If $n \in Z$ prove that (*i*) $n(n+1)(n+5) = M(6)$ (*ii*) $n^5 - n = M(30)$

(*iii*) $n(n^2-1) = M(24)$ when $n$ is odd.

6. If $p$ is a prime and $a \in Z$ then prove that $p \mid a$ or $(p,a) = 1$.

7. Prove that every odd prime can be put in the form $4n-1$ or $4n+1$

8. Prove that every odd prime greater than 3 can be put in the form $6n-1$ or $6n+1$.

9. Show that there are infinitely many primes of the form (*i*) $4n-1$ (*ii*) $6n-1$

10. If $x, y \in R$ prove that $[x+y] \geq [x]+[y]$.

11. If $2^n+1$ is a prime show that $n$ is a power of 2.

12. If $(a,b) = 1$ then show that $(a+b, a^2-ab+b^2) = 1$ or 3 ***(A.U. 05)***

13. If $n > 2$ is a positive integer show that $n^5 - 5n^3 + 4n$ is divisible by 120. ***(S. V. U. 05)***

## ANSWERS

1. (*i*) $2^9\times5$ (*ii*) $2^2\times3\times7^3$ (*iii*) $5\times7^2\times11^2$

2. (*i*) $1; 3\times7\times167\times191$ (*ii*) $37; 7\times13\times37\times3\times29$ (*iii*) $7; 2\times3^2\times5\times7^3\times13\times31$

3. (*i*) $18, 57\times124$ (*ii*) $24; 57\times624$ (*iii*) $64; 240000$ 4. (*i*) 19 (*ii*) 498 (*iii*) 8

## 0. 22. CONGRUENCES

The property of congruence provides a way of classifying integers according to the remainder obtained upon division by a fixed positive integer. In fact the remainder is the only thing of interest. In this section we study a relation on the integers that is defined in terms of remainders.

**Definition.** *Let* $m$ *be a fixed positive integer and* $a,b\in \mathrm{Z}$. *'a' is said to be congruent to 'b' modulo m, if* $m\,|\,(a-b)$.

**Notation.** '$a$' is congruent to '$b$' modulo $m$ is denoted by $a\equiv b\,(\mathrm{mod}\,m)$

If $m\nmid(a-b)$, then we say that '$a$' is not congruent to '$b$' modulo $m$ and write $a\not\equiv b(\mathrm{mod}\,m)$.

**Note 1.** $a\equiv b\,(\mathrm{mod}\,m)\Leftrightarrow m\,|\,(a-b)\Leftrightarrow a-b=qm;\ q\in \mathrm{Z}$

$\Leftrightarrow (a-b)$ is a multiple of $m$ *i.e.* $a-b=\mathrm{M}(m)$

**2.** The congruence relation has properties similar to the equality relation.

**3.** $m\,|\,a\Leftrightarrow a\equiv 0\,(\mathrm{mod}\,m)$.

***e.g.*** 1. $5\,|\,(18-3)\Leftrightarrow 18\equiv 3\,(\mathrm{mod}\,5)$ 2. $4\,|\,(-8)-4\Leftrightarrow -8\equiv 4\,(\mathrm{mod}\,4)$

3. $7\,|\,17-(-4)\Leftrightarrow 17\equiv -4\,(\mathrm{mod}\,7)$ 4. $2\nmid(8-1)\Leftrightarrow 8\not\equiv 1\,(\mathrm{mod}2)$.

**Theorem 1.** ***Two integers a and b are congruent modulo m iff they leave the same remainder when divided by m.***

**Note 1.** If $a\equiv b\,(\mathrm{mod}\,m)$ then $(a,m)=(b,m)$

**2.** If $a\equiv b\,(\mathrm{mod}\,m)$ then $a^n\equiv b^n\,(\mathrm{mod}\,m)\ \forall\ n\in \mathrm{Z}^+$

**Theorem 2.** ***For a fixed integer*** $\mathbf{m>0}$ ***the relation*** $\mathbf{a\equiv b(mod\,m)}$ ***is an equivalence relation on the set of integers Z.***

**Theorem. 3 :** ***If*** $\mathbf{a\equiv b(mod\,m)}$ ***and*** $\mathbf{x\in Z}$ ***then***

**(i)** $\mathbf{a\pm x\equiv b\pm x(mod\,m)}$ **(ii)** $\mathbf{ax\equiv bx(mod\,m)}$

**Theorem. 4.** ***If*** $\mathbf{a\equiv b(mod\,m)}$ ***and*** $\mathbf{c\equiv d(mod\,m)}$ ***then***

**(i)** $\mathbf{a+c\equiv b+d(mod\,m)}$ **(ii)** $\mathbf{ac\equiv bd(mod\,m)}$

**Note 1.** $a\equiv b(\mathrm{mod}\,m), c\equiv d(\mathrm{mod}\,m)\Rightarrow a-c\equiv b-d(\mathrm{mod}\,m)$

***e.g.*** **1.** $14\equiv 2(\mathrm{mod}\,12)\Rightarrow -14\equiv -2(\mathrm{mod}\,12)$ **2.** $12\equiv 5(\mathrm{mod}\,7)\Rightarrow 24\equiv 10(\mathrm{mod}\,7)$

**3.** $12\equiv 5(\mathrm{mod}\,7);\ 16\equiv 2(\mathrm{mod}\,7)\Rightarrow 28\equiv 7(\mathrm{mod}\,7)$ and $192\equiv 10(\mathrm{mod}\,7)$

**2.** If $a_1\equiv b_1(\mathrm{mod}\,m), a_2\equiv b_2(\mathrm{mod}\,m),.....a_n\equiv b_n(\mathrm{mod}\,m)$ then

$a_1a_2.....a_n\equiv b_1b_2.....b_n(\mathrm{mod}\,m)$

**3.** We also write $a+c\equiv b+d(\mathrm{mod}\,m)$ as $a+_m c=b+_m d$ and $ac\equiv bd(\mathrm{mod}\,m)$ as $a\times_m c\equiv b\times_m d$

**Theorem 5.** ***If*** $\mathbf{ab\equiv ac\,(mod\,m)}$ ***and (a, m) =1, then*** $\mathbf{b\equiv c\,(mod\,m)}$.

**Note 1.** This is cancellation law in congruences and is valid only when $(a,m)=1$..

$21\equiv 14\,(\mathrm{mod}\,7)$ i.e. $7.3\equiv 7.2\,(\mathrm{mod}\,7)$ does not imply $3\equiv 2\,(\mathrm{mod}\,7)$ as $(7,7)\neq 1$.

**2. Imp.** $ab\equiv ac\,(\mathrm{mod}\,m)\Leftrightarrow b\equiv c\,(\mathrm{mod}\,m/(a,m))$

**Ex. 1 :** *Find the least positive integer modulo 7 to which 323 is congruent.*

**Sol.** Dividing 323 by 7 we have $323 = 7(46) + 1$

$\therefore 323 - 1 = 7(46) \Rightarrow 7 \mid (323-1) \Rightarrow 323 \equiv 1 \pmod 7$

**Ex. 2 :** *If* $a \equiv b \pmod m$ *and* $n$ *is a positive divisor of* $m$ *then* $a \equiv b \pmod n$

**Sol.** $a \equiv b \pmod m$ and $n \mid m \Rightarrow a - b = mq_1, m = nq_2$ where $q_1, q_2 \in Z$

$\Rightarrow (a-b) = (nq_2)q_1 = nq$ where $q = q_2 q_1 \in Z \Rightarrow a \equiv b \pmod n$

**Ex. 3 :** *Prove that* $ax \equiv ay \pmod m \Leftrightarrow x \equiv y \left(\mod \frac{m}{(a,m)}\right)$

**Sol.** If $(a, m) = d$ then $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$. $\quad ax \equiv ay \pmod m \Leftrightarrow ax - ay = m_1,\ q \in Z.$

$\Leftrightarrow \frac{a}{d}(x-y) = \frac{m}{d}q \Leftrightarrow \frac{m}{d} \left| \frac{a}{d}(x-y) \right. \Leftrightarrow \frac{m}{d} \left| (x-y) \right. \left(\because \left(\frac{a}{d}, \frac{m}{d}\right) = 1\right) \Leftrightarrow x \equiv y \left(\mod \frac{m}{d}\right).$

## 0. 23. RESIDUE CLASSES OR CONGRUENCE CLASSES

We know that an equivalence relation on a set splits the set into a number of subsets. Since congruence modulo $m$ is an equivalence relation on Z, this relation partitions Z into a collection of disjoint subsets, "called residue classes" or "Congruence classes".

**Theorem. 1.** ***Let m be a positive integer and*** $\mathbf{S = \{0,1,2,.....,m-1\}}$. ***Then no two integers of S are congruent modulo m.***

**Proof.** Let $a, b \in S$ and $a > b$. Then $0 \le a < m$ and $0 \le b < m \Rightarrow 0 < a - b < m$

So, $m \nmid (a-b)$ and $a \not\equiv b \pmod m$. Hence no two integers of S are congruent mod $m$.

**Theorem. 2 :** ***Let m be a positive integer and*** $\mathbf{S = \{0,1,2,.....,m-1\}}$. ***Then every*** $\mathbf{x \in Z}$ ***is congruent modulo m to one of the integers of S.***

**Proof.** By division algorithm, for $x \in Z$ there exist uniqe integers $q, r$ such that $x = qm + r, 0 \le r < m$ and $r$ is unique. $\quad \therefore x - r = qm, r \in S \Rightarrow x \equiv r \pmod m.$

Hence for $x \in Z$ there exists one and only one integer $r \in S$ such that $x \equiv r \pmod m$.

**Definition**. *The remainder* $r$*, upon division of x by m, is called the residue of x mod m. The set of integers* $Z_m = \{0,1,2,.....,m-1\}$ *is called the set of least positive residues modulo m.*

***e.g.*** $\{0,1,2,3,4,5,6\}$ is the set of least positive residues modulo 7. These integers are such that each $x \in Z$ is congruent mod 7 to exactly one of them.

If $m$ is a positive integer, then there exist exactly $m$ equivalence classes for the equivalence relation **"Congruence modulo *m* "**. The equivalence class $\bar{r}$ or $[r]$ is the set $\{x \in Z \mid x \equiv r \pmod m\}$. It is also called $r$ – residue class or $r$ – congruence class. The set of $m$ equivalence classes or residue classes or congruence classes is denoted by $\bar{Z}_m = J_m = \{\bar{0}, \bar{1}, \bar{2}, ....., \overline{m-1}\}$ or $\bar{Z}_m = J_m = \{[0],[1],[2],..... [m-1]\}$.

If $x \in \bar{r}$ then $\bar{x} = \bar{r}$. So, if $x_0 \in \bar{0}, x_1 \in \bar{1}, x_2 \in \bar{2}, .....x_{m-1} \in \overline{m-1}$ then the set

$\{\bar{x}_0, \bar{x}_1, \bar{x}_2, ....., \overline{x_{m-1}}\}$ consists of all the congruence classes modulo - $m$.

**Note :** Two congruent classes $\bar{a}, \bar{b} \in \bar{Z}_m$ or $J_m$ are distinct, for, $\bar{a} = \bar{b} \Rightarrow 0 \le a < b < m$ and $m \mid (b-a)$ which is impossible.

**Definition.** *If* $\bar{a},\bar{b} \in \bar{Z}_m$ *or* $J_m$ *the sum of* $\bar{a}$ *and* $\bar{b}$ *is the congruence class* $\overline{a+b}$ *and the product of* $\bar{a}$ *and* $\bar{b}$ *is the congruence class* $\overline{a.b}$.

Thus we have (*i*) $\bar{a}+\bar{b}=\overline{a+b}$ or $[a]+[b]=[a+b]$ (*ii*) $\bar{a}\,\bar{b}=\overline{ab}$ or $[a]\,[b]=[ab]$

The above two operations are respectively called (i) addition and (ii) multiplication of congruence classes.

The above two operations defined in $\bar{Z}_m$ clearly satisfy the following properties :

For $\bar{a},\bar{b},\bar{c} \in \bar{Z}_m$; (1) $\bar{a}+\bar{b}=\bar{b}+\bar{a}$ and $\bar{a}\,\bar{b}=\bar{b}\,\bar{a}$

(2) $(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c})$ and $(\bar{a}\,\bar{b})\,\bar{c}=\bar{a}\,(\bar{b}\,\bar{c})$

(3) $\bar{a}\,(\bar{b}+\bar{c})=\bar{a}\,\bar{b}+\bar{a}\,\bar{c}$ (4) $\bar{0}+\bar{a}=\bar{a}$ (5) $\bar{1}\,\bar{a}=\bar{a}$

(The proofs of the above statements are left as an exercise)

**Note :** If $m=p$ is a prime number then $J_p$ the set of congruence classes modulo $p$ is such that $\bar{a}\neq\bar{0}\in J_p \Rightarrow$ there exists $\bar{b}\in J_p$ with the condition $\bar{a}\,\bar{b}=\bar{1}$.

## 0. 24. LINEAR CONGRUENCES

**Definition. 1.** *If* $f(x)=a_0x^n+a_1x^{n-1}+.....+a_{n-1}x+a_n$ *is a polynomial with integral coefficients and* $a_0 \not\equiv 0 \pmod m$ *then* $f(x)\equiv 0 \pmod m$ *is called a polynomial congruence of nth degree.*

*A polynomial congruence of first degree is called* ***linear congruence.***

**Definition. 2 :** *If there exists* $x_0 \in Z$ *such that* $f(x_0)\equiv 0 \pmod m$ *then* $x_0 \in Z$ *is called a solution of* $f(x)\equiv 0 \pmod m$.

*Any linear congruence can be put in the form* $ax\equiv b \pmod m$ *where* $a\neq 0 \pmod m$.

**Note 1.** $x_0$ is a solution of the congruence $ax\equiv b \pmod m \Leftrightarrow ax_0\equiv b \pmod m$

***e.g.*1.** 3 is a solution of $7x\equiv 5 \pmod 8$ because $7.3\equiv 5 \pmod 8$ *i.e.* $21\equiv 5 \pmod 8$

**2.** 7 is a solution of $3x\equiv 1 \pmod 4$ because $3.7\equiv 1 \pmod 4$ *i.e.* $21\equiv 1 \pmod 4$

**3.** 2 is a not a solution of $3x\equiv 4 \pmod 5$ because $6\not\equiv 4 \pmod 5$.

**Theorem 1.** ***If*** $\mathbf{x_0}$ ***is a solution of*** $\mathbf{ax\equiv b \pmod m}$ ***and*** $\mathbf{x_1\equiv x_0 \pmod m}$ ***then*** $\mathbf{x_1}$ ***is also a solution of*** $\mathbf{ax\equiv b \pmod m}$.

**Note.** From the above theorem we observe that, if $x_0$ is a solution of $ax\equiv b \pmod m$ then every integer $x_1$ congruent to $x_0$ under modulo $m$ is also a solution. The solutions $x_0, x_1$ are not counted as different and say that $x\equiv x_0 \pmod m$ is a solution of the congruence $ax\equiv b \pmod m$.

**Imp. When we say that $\mathbf{x\equiv x_0 \pmod m}$ is a solution of $\mathbf{ax\equiv b \pmod m}$ we mean that $\mathbf{x=x_0+tm, t\in Z}$ is a complete solution (a set of congruent solutions) of $\mathbf{ax\equiv b \pmod m}$.**

**Definition.** *Let* $\{x_0,x_1,x_2,.....,x_{m-1}\}$ *be a complete set of residues modulo - m. The number of solutions of* $ax\equiv b \pmod m$ *is the number of* $x_i (i=0,1,2,.....,m-1)$ *such that* $ax_i\equiv b \pmod m$.

**Note 1**. The number of solutions is independent of the choice of the complete set of residues modulo $m$.

**2.** The number of solutions cannot exceed the modulus $m$.

**e.g.** Consider the congruence $3x\equiv 4 \pmod 5$

A complete set of residues modulo $5 = \{0,1,2,3,4\}$

$3.3 \equiv 4 \pmod 5$ because $5 \mid (9-4) \Rightarrow 3$ is a solution of $3x \equiv 4 \pmod 5$

Hence $x \equiv 3 \pmod 5$ is a solution of the congruence.

We also see that, $3.0 \neq 4 \pmod 5$, $3.1 \neq 4 \pmod 5$, $3.2 \neq 4 \pmod 5$ and $3.4 \neq 4 \pmod 5$.

$\therefore$ $x \equiv 3 \pmod 5$ is the unique solution.

**Theorem 2.** ***If*** $\mathbf{(a,m) = 1,}$ ***then the linear congruence*** $\mathbf{ax \equiv b \pmod m}$ ***has a unique solution.***

**Note 1.** The linear congruence $3x \equiv 4 \pmod 5$ has a unique solution $x \equiv 3 \pmod 5$ since $(3,5) = 1$ and the set of all congruent solutions is given by $x = 3 + t$ where $t \in Z$.

**2.** The congruence $x \equiv b \pmod m$ has a unique solution because $(1, m) = 1$. It is given by $x = b + mt$ where $t \in Z$.

**Theorem 3.** ***If*** $\mathbf{(a,m) = d}$ ***and*** $\mathbf{d \nmid b}$ ***then the congruence*** $\mathbf{ax \equiv b \pmod m}$ ***has no solution.***

**e.g.** Consider the congruence $20x \equiv 30 \pmod 4$ Here $a = 20, b = 30, m = 4$

$\Rightarrow d = (a,m) = (20,4) = 4 \Rightarrow 20x \equiv 30 \pmod 4$ has no solution as $d = 4 \nmid b = 30$.

**Theorem 4.** ***If*** $\mathbf{(a,m) = d}$ ***and*** $\mathbf{d \mid b}$ ***then the congruence*** $\mathbf{ax \equiv b \pmod m}$ ***has exactly d incongruent solutions*** $\mathbf{ax \equiv x_0 + r(m/d) (mod m); r = 0,1,2,....,d-1}$ ***where*** $\mathbf{x_0}$ ***is a solution of*** $\mathbf{ax \equiv b \pmod m}$

**e.g.** Consider $15x \equiv 25 \bmod(35)$

Here $a = 15,\ b = 25,\ m = 35$ so that $d = (a,m) = (15,35) = 5$

Since $d = 5 \mid b = 25$, the congruence has 5 incongruent solutions.

**Note : Imp.** The congruence $ax \equiv b \pmod m$ (1) has unique solution if $(a,m) = 1$

(2) has no solution if $(a,m) \nmid b$.

(3) has $(a,m)$ solutions if $(a,m) \mid b$ and are given by $x \equiv x_0 + t\left(\frac{m}{(a,m)}\right) \pmod m$

where $x_0$ is a solution and $t = 0,1,2,.....,(m-1)$

## 0. 25. INVERSE MODULO *m*

**Definition.** *If* $ab \equiv 1 \pmod m$ *then* $a, b$ *are said to be inverses modulo* $m$. *Also* $'b'$ *is called inverse of* $'a'$ *and* $'a'$ *is called inverse of* $'b'$ *under modulo m.*

**e.g.** $3.2 \equiv 1 \pmod 5 \Rightarrow 3, 2$ are inverses modulo 5.

**Imp.** ***An integer 'a' has an inverse modulo m if and only if*** $\mathbf{(a,m) = 1}$.

**Note :** For an integer $'a'$ if $a^2 \equiv 1 \pmod m$ then inverse of $a$ is itself.

**Ex. 4** : *Solve the linear congruence* $16x \equiv 25 \pmod{19}$ (

**Sol.** Comparing with $ax \equiv b \pmod m$ we have $a = 16, b = 25, m = 19$

Since $(a,m) = (16,19) = 1$, the congruence has unique solution modulo 19.

To solve $16x \equiv 25 \pmod{19}$, we add suitable congruence or congruences and reduce it to the form $x \equiv x_0 \pmod{19}$ which is the required solution.

We have $247 \equiv 0 \pmod{19} \Rightarrow 0 = 247 \pmod{19}$ (Transitive property)

Adding with the given congruence, $16x \equiv 272 \pmod{19} \Rightarrow 16x \equiv 16.17 \pmod{19}$

$\therefore$ $x \equiv 17 \pmod{19}$ (since (16, 19) = 1). $\therefore$ $x \equiv 17 \pmod{19}$ is the unique solution

## EXERCISE 0 ( *d* )

**1.** Find the least positive integer modulo - 11 to which 335 is congruent.

**2.** Does the number 3 have inverse modulo 6 ?

**3.** Find the inverse pairs of $Z_5 = \{0,1,2,3,4\}$

**4.** If $x$ is even integer prove that it satisfies $x \equiv 0 \pmod 2$.

**5.** If $ab \equiv ac \pmod p$ and $a \not\equiv 0 \pmod p$ where $p$ is a prime then prove that $b \equiv c \pmod p$

**6.** List all integers in the range $1 \le x \le 100$ that satisfy $x \equiv 7 \pmod{17}$.

**7.** If $p$ is prime and $a^2 \equiv b^2 \pmod p$ then prove that $p \mid a+b$ or $p \mid a-b$

**8.** Show that $a + x \equiv b \pmod m$ has unique solution.

**9.** Prove that $ab \equiv 0 \pmod 6$ does not always imply either $a \equiv 0 \pmod 6$ or $b \equiv 0 \pmod 6$

**10.** If $ab \equiv 0 \pmod p$ where $p$ is prime. Prove that either $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

**11.** If $f(x)$ is a polynomial of $n^{th}$ degree with integral coefficients and $a \equiv b \pmod m$ prove that $f(a) \equiv f(b) \pmod m$.

**12.** If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}$ and $m = [m_1, m_2]$ then prove that $a \equiv b \pmod m$

**13.** If $a \equiv b \pmod m$ then prove that $(a,m) = (b,m)$

**14.** Solve the following congruences.

(*i*) $3x \equiv 4 \pmod 5$ (*ii*) $6x + 3 \equiv 4 \pmod{10}$ (*iii*) $15x \equiv 12 \pmod{21}$

(*iv*) $13x \equiv 10 \pmod{28}$ ***(N.U. 05)*** (*v*) $135x = \pmod{10}$ ***(S.K.U. 05)***

## ANSWERS

**1.** 5 **2.** No **3.** 2,3 and 4,4 **6.** 7, 24, 41, 58, 75, 92

**14.** (*i*) $x \equiv 3 \pmod 5$ (*ii*) No solution (*iii*) $x = 5 + 4t \pmod{21}$ where $t = 0,1,2$

### 0. 26. EULER $\phi$ - FUNCTION

The least positive residues modulo $m$ that have inverses modulo $m$ are those relatively prime to m. An important function that counts the number of these positive integers is called the Euler $\phi$ - function.

**Definition.** *The Euler $\phi$ - function is the function $\phi : Z^+ \to Z^+$ defined as follows:* (*i*) *For $1 \in Z^+, \phi(1) = 1$ and* (*ii*) *for $n(>1) \in Z^+, \phi(n) =$ the number of positive integers less than $n$ and relatively prime to $n$.*

**Notation :** The Euler $\phi$ function is denoted by $\phi(n)$.

**Note. 1 :** $\phi(1) = 1$.

**2.** For $n > 1, \phi(n) =$ the number of integers $x$ such that $1 \le x < n$ and $(x,n) = 1$. That is, $\phi(n) =$ the number of integers in $Z_n = \{0,1,2,.....,n-1\}$ that are prime to $n$.

**3.** For $n > 1, \phi(n) =$ the number of congruence classes that are prime to $n$.

***e.g.* 1.** Let $n = 2$, then positive integers less than $2 = \{1\}$. Since $(1,2) = 1$; $\phi(2) = 1$

***2.*** Let $n = 3$. Since $(1,3) = 1, (2,3) = 1$, we have $\phi(3) = 2$

**3.** Let $n = 8$. Complete set of residues $\bmod 8 = \{0,1,2,3,4,5,6,7\} = Z_8$

The residues that are relatively prime to $8 = 1,3,5,7$. Therefore, $\phi(8) = 4$.

**Theorem 1.** ***If $(a,b) = 1$ and the numbers $a, 2a, 3a, ....., (b-1)a$ are divided by $b$ then the remainders are $1, 2, 3, ....., b-1$ not necessarily in this order.***

**Proof.** Let $S = \{a, 2a, 3a, ...., (b-1)a\}$

Let $m_1 a, m_2 a \in S$ leave the same remainder $r$, when divided by $b$.

$\therefore\ m_1 a = q_1 b + r$ and $m_2 a = q_2 b + r$ where $q_1, q_2 \in Z$ and $0 < r < b$.

$\therefore\ (m_1 - m_2)a = (q_1 - q_2)b = qb$, where $q = q_1 - q_2$

Since $(a,b) = 1, b \mid (m_1 - m_2)$. This is impossible, as $m_1 < b$ and $m_2 < b$.

$\therefore$ The remainders are different.

Since $(a,b) = 1$, each $ma \in S$ is not a multiple of $b$, and hence no remainder is zero.

Therefore, the remainders are $1,2,3,.....,b-1$ not necessarily in this order.

**Cor.** If $(a,b) = 1, c \in Z$ and the $b$ numbers of the A.P. $c, c+a, c+2a, ....., c+(b-1)a$ are divided by $b$, then, the remainders are $0,1,2,.....,b-1$ not, necessarily in this order.

**Theorem 2.** ***If*** $\mathbf{(m,n) = 1}$, ***then*** $\boldsymbol{\varphi(m.n) = \varphi(m).\varphi(n)}$.

**Cor.** If $n_1, n_2, .....n_r$ are prime to each other, then $\phi(n_1.n_2.....n_r) = \phi(n_1).\phi(n_2)....\phi(n_r)$

**Note.** We have $\phi(4) = 2, \phi(10) = 4, \phi(5) = 4, \phi(8) = 4$ and $\phi(40) = 16$

But $16 = \phi(40) \neq \phi(4).\phi(10) = 8$ since $(4,10) \neq 1$.

While $16 = \phi(40) = \phi(5).\phi(8)$ since $(5,8) = 1$.

Therefore, the formula $\phi(mn) = \phi(m).\phi(n)$ is applicable only when $(m,n) = 1$.

**Theorem 3.** ***If*** $\mathbf{n \in Z^+}$ ***and p is a prime, then*** $\boldsymbol{\varphi(p^n) = p^n - p^{n-1} = p^n(1-(1/p)}$

**Note 1.** $\phi(p) = \phi(p^1) = p^1 - p^0 = p - 1$, if $p$ is a prime.

**2.** $\phi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$, since 2 is a prime.

**3.** If $p$ is a prime then $\phi(p^n) + \phi(p^{n-1}) + .... + \phi(p^2) + \phi(p) + \phi(1) = p^n$

**4.** $n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_m^{\alpha_m}$, where $\alpha_1, \alpha_2, .....\alpha_m$ are positive integers.

Since $p_1, p_2, .....p_m$ are relatively prime to each other,

$$\phi(n) = \phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2}).....\phi(p_m^{\alpha_m}) = p_1^{\alpha_1}(1-(1/p_1)).p_2^{\alpha_2}(1-(1/p_2)).....p_m^{\alpha_m}(1-(1/p_m))$$
$$= n(1-(1/p_1))\ (1-(1/p_2))....(1-(1/p_m))$$

**e.g.** $\phi(6125) = \phi(5^3.7^2) = \phi(5^3).\phi(7^2) = 5^3(1-(1/5)).7^2(1-(1/7)) = 5^2.4.7.6 = 4200.$

**Theorem.4:(Fermat's Theorem):** ***If*** $\mathbf{p}$ ***is a prime and*** $\mathbf{(a,p) = 1}$ ***then*** $\boldsymbol{a^{p-1} \equiv 1 (\text{mod } p)}$

**Proof.** Since $(a, p) = 1$, when the numbers $a, 2a, 3a, ....(p-1)a$ are divided by $p$, the remainders are $1,2,3,...., p-1$; not necessarily in this order.

Let $a \equiv r_1 (\text{mod } p);\ 2a \equiv r_2 (\text{mod}) p; ....., (p-1)a \equiv r_{p-1} (\text{mod } p)$

But $r_1, r_2, .....r_{p-1}$ are the remainders obtained when $a, 2a, ....., (p-1)a$ are divided by $p$.

$\therefore r_1 . r_2 .....r_{p-1} = 1.2.....(p-1)$

Multiplying the above congruent relations : $a.2a.....(p-1)a \equiv r_1.r_2.....r_{p-1} (\text{mod } p)$

$\Rightarrow \{1.2.....(p-1)\}.a^{p-1} \equiv 1.2.....(p-1) (\text{mod } p)$

$\Rightarrow (p-1)!\, a^{p-1} \equiv (p-1)!\, (\text{mod } p) \Rightarrow a^{p-1} \equiv 1 (\text{mod } p)$

($\because p$ is prime and $(p,1) = 1, (p,2) = 1, ....., (p, p-1) = 1$)

**Cor.** If $p$ is a prime and $a \in Z$ then $a^p \equiv a (\text{mod } p)$.

When $(a, p) = 1$; by Fermat's theorem, $a^{p-1} \equiv 1 (\text{mod } p) \Rightarrow a^p \equiv a (\text{mod } p)$

when $(a,p)\neq 1; p\mid a$ and $a\equiv 0\,(\text{mod } p)\Rightarrow 0\equiv a\,(\text{mod } p)$

$a^p\equiv 0\,(\text{mod } p)$ and $0\equiv a\,(\text{mod } p)\Rightarrow a^p\equiv a(\text{mod } p)$.

**Theorem. 5. (Wilson's Theorem) :** *If* **p** *is a prime then* $\mathbf{(p-1)!+1\equiv 0(\text{mod } p)}$.

**Proof. :** For $p=2,(p-1)!+1=2$ and $2\equiv 0\,(\text{mod } 2)\Rightarrow$ the theorem is true.

Let $p>2$ and $a\in Z$ such that $1\le a\le p-1$.

$p$ is prime $\Rightarrow (a,p)=1$ and hence the linear congruence $ax\equiv 1\,(\text{mod } p)$ has unique solution, say, $x_0$. Let $a'\in \bar{x}_0$ and $1\le a'\le p-1$. Then $aa'\equiv 1\,(\text{mod } p)$

$a'=a\Rightarrow a^2\equiv 1\,(\text{mod } p)\Rightarrow p\mid (a^2-1)\Rightarrow p\mid (a-1)$ or $(a+1)$

$p\mid (a-1)$ and $a>0\Rightarrow a+1=p\Rightarrow a=p-1$. $p\mid (a+1)$ and $p>a\Rightarrow a-1=0\Rightarrow a=1$

$\therefore a'=a\Rightarrow$ either $a=1$ or $a=p-1$ and so $a'\neq a\Rightarrow a\in\{2,3,.....,p-2\}$

$\therefore$ the distinct $a,a^1$ belong to the set $\{2,3,.....,(p-2)\}$ containing $(p-3)$ elements.

These $(p-3)$ elements form $(p-3)/2$ pairs, such that the product of each pair $\equiv 1\,(\text{mod } p)$.

Multiplying these $(p-3)/2$ congruences

$2.3.....(p-2)\equiv 1(\text{mod } p)\ \Rightarrow 1.2.3.....(p-2)(p-1)\equiv 1(p-1)\,(\text{mod } p)$

$\Rightarrow (p-1)!\equiv (p-1)\,(\text{mod } p)\Rightarrow (p-1)!+1\equiv p\,(\text{mod } p)\Rightarrow (p-1)!+1\equiv 0\,(\text{mod } p)$

**Note 1. :** The converse of the Wilson's theorem is also true.

That is, $(p-1)!+1\equiv 0\,(\text{mod } p)\Rightarrow p$ is prime.

**2.** $(p-1)!+1\equiv 0\,(\text{mod } p)\Rightarrow p\mid (p-1)!+1\Rightarrow (p-1)!+1=M(p)$

**e.g.** Since 7 is prime, $(7-1)!+1=6!+1$ is divisible by 7.

**Ex. 1 :** *Find the number of positive integers less than 25200 that are prime to 25200.*

**Sol.** $25200=2^4\times 3^2\times 5^2\times 7$

$\therefore \phi(25200)=\phi(2^4\times 3^2\times 5^2\times 7)=\phi(2^4)\times\phi(3^2)\times\phi(5^2)\times\phi(7)$

$=2^4(1-(1/2))\times 3^2(1-(1/3))\times 5^2(1-(1/5))\times 7^1(1-(1/5))$

$=2^4\times 3^2\times 5^2\times 7\times(1/2)(2/3)(4/5)(6/7)=2^6\times 3\times 5\times 6=5760.$

**Ex. 2 :** *If* $n>2$ *prove that* $\phi(n)$ *is even.*

**Sol. :** If $(a,n)=1$ then $(n-a,n)=1$ for $a\in Z^+$.

$\Rightarrow$ Integers coprime to $n$ occur in pairs of the form $a,n-a\Rightarrow\phi(n)$ is even.

$\therefore\phi(n)$ is odd for $n=1$ and $n=2$ only.

**Ex. 3 :** *If p is prime and a, b* $\in$ *z then prove that* $(a+b)^p\equiv a^p+b^p\,(\text{mod } p)$

**Sol.** From the Note of Ferma Theorem;

$a^p\equiv a(\text{mod } p)$, $b^p\equiv p(\text{mod } p)$ and $(a+b)^p\equiv$

$(a+b)\,(\text{mod } p)$ ($\because$ $p$ is prime)

$a^p\equiv a(\text{mod } p)$, $b^p=b(\text{mod } p)\Rightarrow a^p+b^p\equiv a+b(\text{mod } p)$

$\Rightarrow a+b \equiv a^p + b^p \pmod{p}$

$\therefore \quad (a+b)^p \equiv a^p + b^p \pmod{p}$

## EXERCISE 0 ( *e* )

**1.** Find (*i*) $\phi(126)$ (*ii*) $\phi(768)$ (*iii*) $\phi(3600)$
(*iv*) $\phi$ 490 ***(A.U. 05)*** (*v*) $\phi$ (2310)

**2.** Find the smallest integer so that $\phi(n) = 6$

**3.** Proove that $\phi(n) = n-1 \Leftrightarrow n$ is a prime.

**4.** If $p$ is an odd prime prove that $\phi(2p) = \phi(p)$.

**5.** Prove that $\phi(n^2) = n\phi(n)$ for every $n \in Z^+$

**6.** If $(n,17) = 1$ prove that $n^{16} - 1$ is divisible by 17

**7.** If $a,b$ are coprime to prime member $p$ then show that $a^{p-1} - b^{p-1} = M(p).$.
Hence prove that $5^{10} - 3^{10}$ divisible by 11.

**8.** prove that $n^5 - n$ is divisible by 30.

**9.** Prove that $1^{n-1} + 2^{n-1} + \ldots\ldots + (n-1)^{n-1} + 1 = M(n)$

## ANSWERS

**1.**(*i*) 36 (*ii*) $2^8$ (*iii*) 960 (*iv*) 168 (*v*) 480 **2.** 7

# Binary Operation

**1.1.** The use of numbers was there for many centuries and we are familiar with the types of the numbers - integers, rational numbers, real numbers, complex numbers together with certain operations, such as addition and multiplication, defined on them. Addition is basically just such a rule that people learn, enabling them to associate, with two numbers in a given order, some number as answer. Multiplication is also such a rule, but a different rule. But with the use of arbitrary quantities $a, b, c, \ldots, \ldots x, y, z, \ldots$ for numbers the subject, Algebra which is the generalisation of Arithmetic, came into being. For many years mathematicians concentrated on improving the methods to use numbers, and not on the structure of the number system. In the nineteenth century mathematicians came to know that the methods to use numbers are not limited to only sets of numbers but also to other types of sets. A set with a method of combination of the elements of it is called an algebraic structure and we can have many algebraic structures. The study of algebraic structures which have been subjected to an axiomatic development in terms Abstract Algebra.

In what follows we study **Group Theory** i.e. the study of the algebraic structure. **Group**, which is rightly termed the basis of **Abstract Algebra**.

In Group Theory the basic ingredients are sets, relations and mappings. It is expected that the student is very much familiar with them. However, we introduce and discuss some of the aspects connected with them which will be useful to us in our future study.

### 1.2. EQUALITY OF SETS $\mathbf{A}$ AND $\mathbf{B}$ : $\mathbf{A} \subseteq \mathbf{B}$ AND $\mathbf{B} \subseteq \mathbf{A} \Leftrightarrow \mathbf{A} = \mathbf{B}$

### 1.3. UNION AND INTERSECTION OF SETS $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$

$$\mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3 \ldots \cup \mathbf{A}_n = \bigcup_{i=1}^{n} \mathbf{A}_i \text{ and } \mathbf{A}_1 \cap \mathbf{A}_2 \cap \mathbf{A}_3 \ldots \cap \mathbf{A}_n = \bigcap_{i=1}^{n} \mathbf{A}_i .$$

### 1.4. $f$ IS A RELATION FROM A SET $\mathbf{A}$ TO A SET $\mathbf{B}$

$\Leftrightarrow f \subseteq \mathbf{A} \times \mathbf{B}$. $\Leftrightarrow f \subseteq \{(a,b) : a \in \mathrm{A}, b \in \mathrm{B}\}$

We write $(a, b) \in f$ as $afb$ and we say that $a$ is $f$ related to $b$.

Sometimes we write $\sim$ for $f$. In such a case we write $a \sim b$.

If $\mathbf{A} = \mathbf{B}$, then we say that $f$ is a relation in $\mathbf{A}$.

If $f \subseteq \mathbf{A} \times \mathbf{B}$, we write $f^{-1} = \{(b, a) / (a, b) \in f\} \subseteq \mathbf{B} \times \mathbf{A}$ and $f^{-1}$ is called inverse relation of $f$ and it is from $\mathbf{B}$ to $\mathbf{A}$.

The domain of $f$ is equal to the range of $f^{-1}$ and the range of $f$ is equal to the domain of $f^{-1}$. Further $(f^{-1})^{-1} = f$.

$f$ is a relation in $\mathbf{A} \Leftrightarrow f \subseteq \mathbf{A} \times \mathbf{A} \Leftrightarrow f\{(a, b) / a, b \in \mathbf{A}\} \subseteq \mathbf{A} \in \mathbf{A}$.

## 1.5. TYPES OF RELATIONS

$f$ is a relation in a set $\mathbf{A}$.

(i) If $\forall\ x \in \mathbf{A}, (x, x) \in f$ then $f$ is said to be reflexive in $\mathbf{A}$.

(ii) If $\forall\ (x, y) \in f \Rightarrow (y, x) \in f$, then $f$ is said to be symmetric in **A.**

(iii) If $(x, y) \in f$ and $(y, z) \in f \Rightarrow (x, z) \in f$, then $f$ is said to be transitive in **A.**

(iv) If $f$ is reflexive, symmetric and transitive, then $f$ is said to be an equivalence relation.

**e.g. 1.** In the set of triangles in a plane, the relation of similarity is an equivalence relation.

**2.** $\mathbf{A} = \{1, 2, 3\}$ the relation $f = \{(1,1), (2,2), (3,3)\}$ is an equivalence relation in $\mathbf{A}$.

**Partition of a set**

A partition of a set $\mathbf{S}$ is a set of non-empty subsets $\mathbf{S}_i$, with $i$ in some index set $\Delta$, such that : (i) $S = \underset{i \in \Delta}{\cup} S_i$ and (ii) $S_i \cap S_j = \phi$ for $i \neq j$.

That is, a partition of a set $\mathbf{S}$ is a collection of disjoint subsets of $\mathbf{S}$ whose union is the whole set $\mathbf{S}$.

## 1.6. PARTITION OF A SET

$f$ is an equivalence relation in a non-empty set $\mathbf{S}$ and $a$ is an element of $\mathbf{S}$. The subset of elements which are $f$ related to $a$ constitutes an equivalence class of $a$.

The equivalence class of $a$ is denoted by $\bar{a}$ or $[a]$ or $\{a\}$. Thus $\bar{a} = \{x \in \mathbf{S} \mid a\ f\ x\}$ and $\bar{a} \subseteq S$.

Further (i) $a \in \bar{a}$, (ii) $b \in \bar{a} \Rightarrow \bar{b} = \bar{a}$.

For, $b \in \bar{a} \Rightarrow a\ f\ b$ and $x$ is any element of $\bar{b} \Rightarrow b\ f\ x$.

Now $a\ f\ b, b\ f\ x \Rightarrow a\ f\ x \Rightarrow x \in \bar{a} \Rightarrow \bar{b} \subseteq \bar{a}$ ...(1)

Again $y$ is any element of $\bar{a} \Rightarrow a\ f\ y$. Since $f$ symmetric $a\ f\ b \Rightarrow b f\ a$.

Now $b\ f\ a, a\ f\ y \Rightarrow b\ f\ y \Rightarrow y \in \bar{b} \Rightarrow \bar{a} \subseteq \bar{b}$ and hence $\bar{b} = \bar{a}$ using (1).

(iii) $\bar{a} = \bar{b} \Rightarrow a\ f\ b$ For $\bar{a} = \bar{b} \Rightarrow a \in \bar{b} \Rightarrow b\ f\ a \Rightarrow a f\ b$.

(iv) $a\ f\ b \Rightarrow \bar{a} = \bar{b}$

For $x \in \bar{a}, a\ f\ b \Rightarrow a\ f\ x, b\ f\ a \Rightarrow b\ f\ a, a\ f\ x \Rightarrow b\ f\ x \Rightarrow x \in \bar{b} \Rightarrow \bar{a} \subseteq \bar{b}$ ...(2)

Again $y$ is any element of $\bar{b} \Rightarrow b\ f\ y$.

Now $a\ f\ b \Rightarrow a\ f\ y \Rightarrow y \in \bar{a} \Rightarrow \bar{b} \subseteq \bar{a}$. and hence $\bar{a} = \bar{b}$ using (2).

**Theorem 1.** ***If f is an equivalence relation in a non-empty set*** $\mathbf{S}$ ***and a, b are two arbitrary elements of*** $\mathbf{S}$***, then***

(i) $\bar{a} = \bar{b}$ or $\bar{a} \cap \bar{b} = \phi$ (ii) $\bar{a} \cup \bar{b} \cup \bar{c} \cup \ldots = \mathbf{S}$.

**Proof.** (i) If $\bar{a} \cap \bar{b} = \phi$, there is nothing to prove.

Let $\bar{a} \cap \bar{b} = \phi$. Then there exists some element $x$ such that $x \in \bar{a}$ and $x \in \bar{b}$.

$\therefore$ $a\ f\ x$ and $b\ f\ x \Rightarrow a\ f\ x$ and $x\ f\ b \Rightarrow a\ f\ b \Rightarrow \bar{a} = \bar{b}$

Hence we must have either $\bar{a} = \bar{b}$ if $\bar{a} \cap \bar{b} \neq \phi$. or $\bar{a} \neq \bar{b}$ if $\bar{a} \cap \bar{b} = \phi$.

(ii) Let $c$ be any element of $\mathbf{S}$.

If $af\ c$, then $\bar{a} = \bar{c}$ and if $bf\ c$ then $\bar{b} = \bar{c}$. If $\bar{a} \neq \bar{c}$ or $\bar{b} \neq \bar{c}$, then $\bar{a} \cap \bar{b} \cap \bar{c} = \phi$.

$\therefore$ Every element of $\mathbf{S}$ must belong to some equivalence class of $\mathbf{S}$ i.e. all the elements of $\mathbf{S}$ must belong to the disjoint equivalence classes of $\mathbf{S}$ i.e. $\bar{a} \cup \bar{b} \cup \bar{c} \cup \ldots = \mathbf{S}$.

**Note.** If $f$ is an equivalence relation defined in a non-empty set $\mathbf{S}$, the set of equivalence classes related to $f$ is a partition of $\mathbf{S}$.

That is, two equivalence classes related to $f$ are (1) either identical or disjoint and (2) the union of all the disjoint equivalence classes of $f$ is the set $\mathbf{S}$.

**Theorem 2.** ***For any given partition of a set $\mathbf{S}$, there exists an equivalence relation $f$ in $\mathbf{S}$ such that the set of equivalence classes related to $f$ is the given partition.***

**Proof.** Let $\mathbf{P} = \{\mathbf{S}_a, \mathbf{S}_b, \mathbf{S}_c, \ldots\ldots\}$ be any partition of $\mathbf{S}$. Let $p, q \in \mathbf{S}$. Let us define a relation $f$ in $\mathbf{S}$ by $pfq$ if there is a $\mathbf{S}_i$ in the partition such that $p, q \in \mathbf{S}_i$.

(i) Since $\mathbf{S} = \mathbf{S}_a \cup \mathbf{S}_b \cup \mathbf{S}_c \cup \ldots\ldots, \forall\ x \in \mathbf{S}$, there exists $\mathbf{S}_i \in \mathbf{P}$ such that $x \in \mathbf{S}_i$.

Hence $x, x \in \mathbf{S}_i \Rightarrow xfx$ $\quad\therefore\quad$ $f$ is reflexive in $\mathbf{S}$.

(ii) If $xfy$, then there exists $\mathbf{S}_i \in \mathbf{P}$ such that $x, y \in \mathbf{S}_i$.

But $x, y \in \mathbf{S}_i \Rightarrow y, x \in \mathrm{S}_i \Rightarrow yfx$. Hence $xfy \Rightarrow yfx$. $\quad\therefore\quad$ $f$ is symmetric in $\mathbf{S}$.

(iii) Let $xfy$ and $yfz$ then by the definition of $f$, there exist subsets $\mathbf{S}_j$ and $\mathbf{S}_k$ (not necessarily distinct) of $\mathbf{S}$ such that $x, y \in \mathbf{S}_j$ and $y, z \in \mathbf{S}_k$. Since $y \in \mathbf{S}_j$ and also $y \in \mathbf{S}_k$, we have $\mathrm{S}_j \cap \mathrm{S}_k \neq \phi$. But $\mathbf{S}_j, \mathbf{S}_k$ belong to the partition of $\mathbf{S}$.

$\therefore\quad \mathrm{S}_j \cap \mathrm{S}_k \neq \phi \Rightarrow \mathrm{S}_j = \mathrm{S}_k$. Then $x, z \in \mathbf{S}_j$ and hence $xfz$.

Hence $f$ is transitive in $\mathbf{S}$. $\quad\therefore\quad$ $f$ is an equivalence relation in $\mathbf{S}$.

## 1.7. FUNCTIONS OR MAPPINGS

**Definition.** $\mathbf{A}, \mathbf{B}$ are non-empty sets. If $f \subseteq \mathbf{A} \times \mathbf{B}$ such that the following conditions are true, then $f$ is called a function from $\mathbf{A}$ to $\mathbf{B}$.

(i) $\forall\ x \in \mathbf{A}\ \exists\ y \in \mathbf{B}$ such that $(x, y) \in f$. $\qquad$ (ii) $(x, y), (x, z) \in f \Rightarrow y = z$.

If $f$ is a function from $\mathbf{A}$ to $\mathbf{B}$ then we say that $f$ is a mapping from $\mathbf{A}$ to $\mathbf{B}$ and we write $f : \mathbf{A} \to \mathbf{B}$.

Domain of $f$ is $\mathbf{A}$ and range of $f$ is $f(\mathbf{A})$ and $f(\mathbf{A}) \subseteq \mathbf{B}$.

Alternatively if $f$ is a relation which associates every element of $\mathbf{A}$ to an element of $\mathbf{B}$, and if $x = y \Rightarrow f(x) = f(y)$ for $x, y \in \mathbf{A}$, then $f$ is a function from $\mathbf{A}$ to $\mathbf{B}$. In this context we say that **the function is well defined**.

**Transformation.** If $f : \mathbf{A} \to \mathbf{A}$ then the function $f$ is called an operator or transformation on $\mathbf{A}$.

**Equality of Functions.** If $f : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{A} \to \mathbf{B}$ and if $f(x) = g(x)$ for every $x \in \mathbf{A}$ then $f = g$. If $\exists\ x \in \mathbf{A}$ such that $f(x) \neq g(x)$ then we say that $f \neq g$.

## 1.8. TYPES OF FUNCTIONS OR MAPPINGS

(i) If $f : \mathbf{A} \to \mathbf{B}$ is such that there is at least one element in $\mathbf{B}$ which is not the $f$ image of any element in $\mathbf{A}$, then we say that **f is a mapping from $\mathbf{A}$ into $\mathbf{B}$** i.e. $f$ maps $\mathbf{A}$ into $\mathbf{B}$.

(ii) If $f : \mathbf{A} \to \mathbf{B}$ is such that $f(\mathbf{A}) = \mathbf{B}$, then we say that $f$ is a mapping from $\mathbf{A}$ into $\mathbf{B}$. $f$ is also called a **surjection** or a **surjective mapping**.

If $\exists$ some element $b \in \mathbf{B}$ such that $f(a) \neq b$ for some $a \in \mathbf{A}$, then $f$ is not onto.

(iii) If $f : \mathbf{A} \to \mathbf{B}$ is such that for $x, y \in \mathbf{A}$, $f(x) = f(y) \Rightarrow x = y$, then $f$ is said to be a **one-one** or **one-to-one function** or an **injection** or an **injective mapping**. We write $f$ as $1-1$.

If $x, y \in \mathbf{A}$ and $x \neq y \Rightarrow f(x) \neq f(y)$, then $f$ is $1-1$. This is equivalent to the above condition.

If $f(x) = f(y)$ does not imply $x = y$ then we say that $f$ is not $1-1$.

(iv) If $f : \mathbf{A} \to \mathbf{B}$ is $1-1$ and onto, then $f$ is called a bijection. In other words we say that $f$ is a $1-1$ function from $\mathbf{A}$ onto $\mathbf{B}$.

Here $f$ is called a **one-one correspondence between A and B**.

If $\mathbf{A}, \mathbf{B}$ are finite and if $f : \mathbf{A} \to \mathbf{B}$ is a bijection then the number of elements in $\mathbf{A}, \mathbf{B}$ are equal.

(v) If $f : \mathbf{A} \to \mathbf{B}$ is such that every element of $\mathbf{A}$ is mapped into one and only one element of $\mathbf{B}$, then $f$ is called a **constant function**. Here $f(\mathbf{A})$ is a **singleton set**.

(vi) If $f : \mathbf{A} \to \mathbf{A}$ is such that $f(x) = x$ for every $x \in \mathbf{A}$, then $f$ is called the **identity function** on $\mathbf{A}$. It is denoted by $\mathbf{I}_\mathbf{A}$ or simply $\mathbf{I}$. $\mathbf{I}$ is always $1-1$ and onto

(vii) If $f : \mathbf{A} \to \mathbf{B}$ is a bijection then $f^{-1} : \mathbf{B} \to \mathbf{A}$ is unique and is also a bijection.

If $f : \mathbf{A} \to \mathbf{B}$ is one-one and onto, then $f^{-1} : \mathbf{B} \to \mathbf{A}$ where $f^{-1} = \{(b,a) / (a,b) \in f)\}$ is called the inverse mapping of $f$. Here $f(a) = b \Leftrightarrow f^{-1}(b) = a$.

*Only bijections possess inverse mappings.*

## 1.9. PRODUCT OR COMPOSITE OF MAPPINGS AND SOME OF THEIR PROPERTIES

**1.** Let $f : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{B} \to \mathbf{C}$.
Then the composite function of $f$ and $g$, denoted by $gof$ is a mapping from $\mathbf{A}$ to $\mathbf{C}$.
*i.e.* $gof : \mathbf{A} \to \mathbf{C}$ such that $(gof)(x) = g[f(x)], \forall\, x \in \mathbf{A}$.
Here $fog$ cannot be defined. Even if it is possible to define $fog$ and $gof$,
then we may have $fog \neq gof$. Thus composition of mappings is not commutative.

**2.** If $f : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{B} \to \mathbf{C}$ are one-one, then $gof : \mathbf{A} \to \mathbf{C}$ is one-one.
If $f, g$ are onto, then $gof$ is onto.
If $f, g$ are functions such that $gof$ is one-one, then $f$ is one-one.
If $f, g$ are functions such that $gof$ is onto, then $g$ is onto.

**3.** If $f : \mathbf{A} \to \mathbf{B}$ is bijection, then $f^{-1} : \mathbf{B} \to \mathbf{A}$. Also $f^{-1}of = \mathbf{I}_\mathbf{A}$ and $fof^{-1} = \mathbf{I}_\mathbf{B}$.

In particular, if $f : \mathbf{A} \to \mathbf{A}$ is a bijection, then $f^{-1} : \mathbf{A} \to \mathbf{A}$. Also $f^{-1}of = fof^{-1} = \mathbf{I}$.

**4.** If $f : \mathbf{A} \to \mathbf{B}$ then $\mathbf{I}_\mathbf{B} of = f$ and $fo\mathbf{I}_\mathbf{A} = f$.
In particular, if $f : \mathbf{A} \to \mathbf{A}$ then $\mathbf{I}of = fo\mathbf{I} = f$.

**5.** If $f : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{B} \to \mathbf{C}$ are bijections, then $gof : \mathbf{A} \to \mathbf{C}$ is also a bijection.
If $f, g$ are functions such that $gof$ is a bijection then $f$ is one-one and $g$ is onto.
In particular, if $f, g$ are bijections on $\mathbf{A}$, then $gof$ is also a bijection on $\mathbf{A}$.
Also $(gof)^{-1}$ is a bijection and $(gof)^{-1} = f^{-1}og^{-1}$.

**6.** If $f : \mathbf{A} \to \mathbf{B}$, $g : \mathbf{B} \to \mathbf{C}$ and $h : \mathbf{C} \to \mathbf{D}$, then $(hog)of = ho(gof)$
*i.e.* composition of mappings is associative.

**Definition.** $f : \mathbf{A} \to \mathbf{A}$ is a function. $f^n : \mathbf{A} \to \mathbf{A}$ where $n \in \mathbf{Z}$ is defined as follows.

(i) If $n = 0, f^0 = \mathbf{I}$ the identity mapping on $\mathbf{A}$.

(ii) If $n = 1, f^1 = f$ (iii) If $n \geq 2$ and $n \in \mathrm{N}, f^n = fof^{n-1} = f^{n-1}of$.

(iv) If $n$ is a negative integer and $f$ is a bijection then $f^n = (f^{-1})^{-n}$.

**7.** $f^2 = fof, f^3 = fof^2 = fofof$ ……

$f^n = fof^{n-1} = fofof$ …… to $n$ times where $n \in \mathrm{N}$.

**8.** If $n$ is a negative integer and $n = -m$ so that $m$ is a positive integer, then

$$f^n = f^{-m} = (f^{-1})^m = f^{-1}of^{-1}of^{-1}o \ldots\ldots \text{ to } m \text{ times}$$
$$= (fofof \ldots\ldots \text{ to } m \text{ times})^{-1} = (f^m)^{-1}$$

**9.** If $f : \mathbf{A} \to \mathbf{A}$ is a bijection, then $f^n : \mathbf{A} \to \mathbf{A}$ for $n \in \mathbf{Z}$ is also a bijection.

**10.** If $m, n \in \mathbf{Z}$ then $f^m of^n = f^{m+n} = f^{n+m} = f^n of^m$.

## 1.10. BINARY OPERATIONS

Let $\mathbf{R}$ be the set of real numbers and addition $(+)$, multiplication $(\times)$, subtraction $(-)$ be the operations in $\mathbf{R}$. For every pair of numbers $a, b \in \mathbf{R}$, we have unique elements $a + b, a \times b, a - b \in \mathbf{R}$. Thus we can look upon addition, multiplication and subtraction as three mappings of $\mathbf{R} \times \mathbf{R}$ into $\mathbf{R}$, which for each element $(a, b)$ of $\mathbf{R} \times \mathbf{R}$ determine the elements $a + b, a \times b, a - b$ respectively of $\mathbf{R}$. Also one can define many mappings from $\mathbf{R} \times \mathbf{R}$ into $\mathbf{R}$. All these mappings are examples of binary operations on $\mathbf{R}$. The idea of binary operation is not limited only to the sets of numbers. For example, the operations of union $(\cup)$, intersection $(\cap)$ and difference $(-)$ are binary operations in $\mathbf{P}(\mathbf{A})$, the power set of $\mathbf{A}$.

### Binary operation

**Definition.** Let $\mathbf{S}$ be a non-empty set. If $f : \mathbf{S} \times \mathbf{S} \to \mathbf{S}$ is a mapping, then $f$ is called binary operation or binary composition in $\mathbf{S}$ (or on $\mathbf{S}$).

Thus **1.** If a relation in S is such that every pair (distinct or equal) of elements of $\mathbf{S}$ taken in definite order is associated with a unique element of $\mathbf{S}$ then it is called a binary operation is $\mathbf{S}$. Otherwise the relation is not a binary operation in $\mathbf{S}$ and the relation is simply an operation in $\mathbf{S}$.

**2.** $(a, b) \in \mathbf{S} \times \mathbf{S}, \exists$ a unique image $f(a,b) \in \mathrm{S}$.

We observe that addition $(+)$, multiplication $(\times$ or $\cdot)$, subtraction $(-)$ are binary operations in $\mathbf{R}$ and division $(\div)$ is not a binary operation in $\mathbf{R}$.

$(\because$ division by 0 is not defined.)

**Symbolism.** It is customary to denote the binary operation in $\mathbf{S}$ by $o$ (read as circle) or * (read as star) or $\cdot$ or $+$ and to take $a, b, c \in \mathbf{S}$ as arbitrary elements $a, b, c$ of $\mathbf{S}$.

**1.** For $a \in \mathbf{S}, b \in \mathbf{S} \Rightarrow a + b \in \mathbf{S} \Rightarrow +$ is a binary operation in $\mathbf{S}$. Also $+$ is called addition, $+$ is called usual addition if $\mathbf{S} \subseteq \mathbf{C}$ and $a + b$ is called the sum of $a$ and $b$. Addition $(+)$ is to be understood depending upon the set over which the operation is to be taken.

**2.** For $a \in \mathbf{S}, b \in \mathbf{S} \Rightarrow a.b \in \mathbf{S} \Rightarrow .$ is a binary operation in $\mathbf{S}$. Also $\cdot$ is called multiplication, $\cdot$ is called usual multiplication if $\mathbf{S} \subseteq \mathbf{C}$ and $a.b$ is called product of $a, b$. Multiplication $(\cdot)$ is to be understood depending upon the set over which the operation is to be taken.

**3.** For $a \in \mathbf{S}, b \in \mathbf{S} \Rightarrow a\,o\,b \in \mathbf{S} \Rightarrow o$ is a binary operation in $\mathbf{S}$.

**4.** For $a \in \mathbf{S}, b \in \mathbf{S} \Rightarrow a * b \in \mathbf{S} \Rightarrow *$ is a binary operation in $\mathbf{S}$.

This is called **closure law.**

Sometimes we write products $a.b$ or $a * b$ of $a$ and $b$ as $ab$.

If $a, b \in \mathbf{S}$ such that $a \, o \, b \notin \mathbf{S}$ then $o$ is not a binary operation in $\mathbf{S}$. In this case we say that $\mathbf{S}$ is not closed under $o$.

$+$ is a binary operation in the set of natural numbers $\mathbf{N}$ as $(a, b) \in \mathbf{N} \Rightarrow a + b \in \mathbf{N}$.

$-$ is not a binary operation in $\mathbf{N}$ as $(a, b) \in \mathbf{N}$ does not imply $a - b \in \mathbf{N}$.

$o$ is a binary operation in $\mathbf{S}$. The image elements under the mapping $o$ are in $\mathbf{S}$. If $a$ and $b$ are elements of a subset $\mathbf{H}$ of $\mathbf{S}$, it may or may not happen that $ab \in \mathbf{H}$. But if $ab \in \mathbf{H}$ for arbitrary elements $a, b \in \mathbf{H}$ the subset $\mathbf{H}$ is said to be closed under the operation $o$. It may be observed that if $o$ is a binary operation in $\mathbf{S}$, it is implied that $\mathbf{S}$ is closed under the operation $o$.

$o$ is a binary operation in $\mathbf{S}$. If $a, b \in \mathbf{S}$ and $a \neq b$, we know that $(a, b) \neq (b, a)$ and hence, in general, it is not necessary that the images in $\mathbf{S}$ of $(a, b)$ and $(b, a)$ under the binary operation $o$ must be equal. In other words if $o$ is a binary composition in $\mathbf{S}$ it is not necessary that $a, b \in \mathbf{S}$ must hold $a \, o \, b = b \, o \, a$.

$+$ is a binary operation in $\mathbf{R}$. If $a, b, c \in \mathbf{R}$, then $a + b \in \mathbf{R}, b + c \in \mathbf{R}, (a + b) + c \in \mathbf{R}$ and $a + (b + c) \in \mathbf{R}$. We observe that $(a + b) + c = a + (b + c)$. Again $-$ is a binary operation in $\mathbf{R}$. If $a, b, c \in \mathbf{R}$ as above we observe that $(a - b) - c \in \mathbf{R}$ and $a - (b - c) \in \mathbf{R}$. But $(a - b) - c \neq a - (b - c)$.

**Definition.** $o$ is a binary operation in a set $\mathbf{S}$. If for $a, b \in \mathbf{S}, a \, o \, b = b \, o \, a$, then $o$ is said to be commutative in $\mathbf{S}$. This is called **commutative law.** Otherwise, $o$ is said to be not-commutative, in $\mathbf{S}$.

**Definition.** $o$ is a binary operation in a set $\mathbf{S}$. If for $a, b, c \in \mathbf{S}$, $(a \, o \, b) \, o \, c = a \, o \, (b \, o \, c)$ then $o$ is said to be associative in $\mathbf{S}$. This is called **associative law**. Otherwise $o$ is said to be not associative in $\mathbf{S}$.

**Note.** If $o$ is associative in $\mathbf{S}$, then we write $(a \, o \, b) \, o \, c = a \, o \, (b \, o \, c) = a \, o \, b \, o \, c$

*e.g.* $*$ is a commutative binary operation on $\mathbf{N} \Rightarrow a * (b * c) = (b * c) * a = (c * b) * a$

**Definition.** $o, *$ are binary operations in a set $\mathbf{S}$.

If $a, b, c \in \mathbf{S}$, (i) $a \, o \, (b * c) = (a \, o \, b) * (a \, o \, c)$, (ii) $(b * c) \, o \, a = (b \, o \, a) * (c \, o \, a)$, then $o$ is said to be distributive w.r.t. the operation $*$. (i) is called the **left distributive law** and (ii) is called the **right distributive law**. (i) and (ii) are called **distributive laws**.

It is customary in mathematics to omit the words *and only if* from a definition. Definitions are always understood to be *if and only if* statements. *Theorems are not always if and only if statements and no such convention is ever used for theorems.*

**Note.** To prove that a binary operation in $\mathbf{S}$ obeys (follows) a law (commutative law, associative law, etc., ) we must prove that elements of every ordered pair obey the law *i.e.*, the law must be proved by taking arbitrary elements. But to prove that a binary operation in $\mathbf{S}$ does not obey a particular law, it is sufficient if we give a counter example. This method of proving the result is called the **proof by counter example.**

(i) $+$, $.$ are binary operations in $\mathbf{N}$, since for $a, b \in \mathbf{N} \Rightarrow a + b \in \mathbf{N}$ and $ab \in \mathbf{N}$. In other words $\mathbf{N}$ is said to be closed w.r.t. the operation $+$ and $.$.

(ii) $+, .$ are commutative in $\mathbf{N}$ since for $a, b \in \mathbf{N}, a + b = b + a$ and $ab = ba$.

(iii) $+, .$ are associative in $\mathbf{N}$ since for $a, b, c \in \mathbf{N}$.

$$(a + b) + c = a + (b + c) \text{ and } a(bc) = (ab)c.$$

(iv) $.$ is distributive w.r.t. the operation $+$ in $\mathbf{N}$ since for $a, b, c \in \mathbf{N}$.

$$a.(b + c) = a.b + a.c \text{ and } (b + c).a = b.a + c.a.$$

(v) The operations subtraction $(-)$ and division $(\div)$ are not binary operations in $\mathbf{N}$ for $3, 5 \in \mathbf{N}$ does not imply $3 - 5 \in \mathbf{N}$ and $\frac{3}{5} \in \mathbf{N}$.

(vi) Operations $+, -, \bullet$ are binary operations on R but $\div$ is not. However, $\div$ is a binary operation on $\mathrm{R}_* = \mathrm{R} - \{0\}$.

(vii) On $Z^+, \forall a, b \in Z^+$ if $*$ is defined as $a * b = ab$ or $a * b = |a - b|$, then $*$ is a binary operation.

(viii) In N, $o$ is a binary operation defined as $aob =$ L. C. M. for every $a, b \in \mathrm{N}$. Then $7o5 = 35$ and $16o20 = 80$.

**e.g. 2.** $\mathbf{A}$ is the set of even integers.

(i) $+, .$ are binary operations in $\mathbf{A}$ since for $a, b \in \mathrm{A}$, $a + b \in \mathbf{A}$ and $ab \in \mathbf{A}$.

(ii) $+, .$ are commutative in $\mathbf{A}$ since for $a, b \in \mathrm{A}$, $a + b = b + a$ and $ab = ba$.

(iii) $+, .$ are associative in $\mathbf{A}$ since for $a, b, c \in \mathbf{A}$,

$$(a + b) + c = a + (b + c) \text{ and } a(bc) = (ab)c.$$

(iv) is distributive w.r.t. the operation $+$ in $\mathbf{A}$ since for $a, b, c \in \mathbf{A}$,

$$a.(b + c) = a.b + a.c \text{ and } (b + c).a = b.a + c.a.$$

**e.g. 3.** $\mathbf{A}$ is the set of odd integers.

(i) $.$ is a binary operation in $\mathbf{A}$. Also $.$ is associative and commutative in $\mathbf{A}$.

(ii) $+$ is not a binary operation in $\mathbf{A}$ since $3, 5 \in \mathbf{A}$ does not imply $3 + 5 = 8 \in \mathbf{A}$.

**e.g. 4.** $\mathbf{S}$ is the set of all $m \times n$ matrices such that each element of any matrix is a complex number.

Addition of matrices, denoted by $+$, is a binary operation in $\mathbf{S}$. Also $(+)$ is commutative and associative in $\mathbf{S}$.

**e.g. 5.** $\mathbf{S}$ is the set of all vectors.

(i) Addition of vectors, denoted by $+$ is a binary operation in $\mathbf{S}$. Also $+$ is commutative and associative in S.

(ii) Dot product of vectors, denoted $.$, is not a binary operation in $\mathbf{S}$ since for $\bar{a}, \bar{b} \in \mathbf{S}, \bar{a}.\bar{b} \notin \mathbf{S}$.

(iii) Cross product of vectors denoted by $\times$ is a binary operation in $\mathbf{S}$ since for $\bar{a}, \bar{b} \in \mathbf{S}, \bar{a} \times \bar{b} = \bar{c} \in \mathbf{S}$.

**e.g. 6.** In $\mathbf{N}$ the operation $o$ defined by $a\,o\,b = \frac{a + b}{ab}$ is not a binary operation.

**e.g. 7.** '$o$' is a composition in $\mathbf{R}$ such that $a\,o\,b = a + 3b$ for $a, b \in \mathbf{R}$.

(i) Since $a, b \in \mathbf{R}, a + 3b$ is a real number and hence $a + 3b \in \mathbf{R}$ i.e. $a\,o\,b \in \mathbf{R}$. Therefore $o$ is a binary operation in $\mathbf{R}$.

(ii) $a\,o\,b = a + 3b$ and $b\,o\,a = b + 3a$

Since $a\,o\,b \neq b\,o\,a$ for $a, b \in \mathbf{R}$, '$o$' is not commutative in $\mathbf{R}$.

(iii) $(a\,o\,b)\,oc = (a\,o\,b) + 3c = (a + 3b) + 3c$ and $ao\,(b\,o\,c) = a + 3\,(b\,o\,c)$

$= a + 3\,(b + c) = a + 3b + 9c$.

Since $(a\,o\,b)\,oc \neq ao\,(b\,o\,c)$ for $a, b, c \in \mathbf{R}$, $o$ is not associative in $\mathbf{R}$.

**e.g. 8.** On Q define $*$ such that $a*b = ab+1$ for every $a,b \in \mathrm{Q}$.

$(i)$ Since $ab+1 \in \mathrm{Q}$ for every $a,b \in \mathrm{Q}$ then $*$ is a binary operation.

$(ii)$ Since $a*b = ab+1 = ba+1 = b*a$, then $*$ is commutative.

$(iii)$ $\forall a,b,c \in \mathrm{Q}, (a*b)*c = (ab+1)*c = (ab+1)\,c+1 = abc+c+1$

and $a*(b*c) = a*(bc+1) = a\,(bc+1)+1 = abc+a+1$

$\Rightarrow (a*b)*c \neq a*(b*c) \Rightarrow *$ is not associative in Q.

**e.g. 9.** On $\mathrm{R}-\{-1\}$ define o such that $aob = \dfrac{a}{b+1}$ for every $a,b \in \mathrm{R}-\{-1\}$.

$(i)$ Since $\dfrac{a}{b+1} \in \mathrm{R}-\{-1\}$ for every $a,b \in \mathrm{R}-\{-1\}$, then o is a binary operation.

$(ii)$ Since $aob = \dfrac{a}{b+1}$ and $boa = \dfrac{b}{a+1}$ then $aob \neq boa$ and hence o is not commutative.

$(iii)$ $\forall a,b,c \in \mathrm{R}-\{-1\}, (aob)oc = \left(\dfrac{a}{b+1}\right)oc = \dfrac{\frac{a}{b+1}}{c+1} = \dfrac{a}{(b+1)(c+1)}$

and $ao(boc) = ao\left(\dfrac{b}{c+1}\right) = \dfrac{a}{\frac{b}{c+1}+1} = \dfrac{a\,(e+1)}{b+c+1} \Rightarrow (aob)oc \neq ao(boc)$.

$\Rightarrow$ o is not associative $\mathrm{R}-\{-1\}$.

**Composition table for an operation on finite sets (Cayley's composition table)**

Sometimes an operation $o$ on a finite set can conveniently be specified by a table called the composition table. The construction of the table is explained below.

Let $\mathbf{S} = \{a_1, a_2, \ldots a_i, a_j, \ldots a_n\}$ be a finite set with $n$ elements. Let a table with $(n+1)$ rows and $(n+1)$ columns be taken. Let the squares in the first row be filled in with $a, a_1, a_2, \ldots a_n$ and the squares in the first column be filled in with $a, a_1, a_2, \ldots a_n$. Let $a_i (1 \leq i \leq n)$ and $a_j (1 \leq j \leq n)$ be any two elements of $\mathbf{S}$. Let the product $a_i o a_j$ obtained by operating $a_i$ with $a_j$ be placed in the square which is at the intersection of the row headed by $a_i$ and the column headed by $a_j$. Thus the following table be got.

From the composition table we can infer the following laws.

(i) **Closure law.** If all the products formed in the table are the elements of $\mathbf{S}$, the $'o'$ is said to be a binary operation in $\mathbf{S}$ and $\mathbf{S}$ is said to be closed under the composition $'o'$.

| $o$ | $a_1$ | $a_2$ | .... | $a_j$ | .... | $a_n$ |
|---|---|---|---|---|---|---|
| $a_1$ | $a_1oa_1$ | $a_1oa_2$ | .... | $a_1oa_j$ | .... | $a_1oa_n$ |
| $a_2$ | $a_2oa_1$ | $a_2oa_2$ | .... | $a_2oa_j$ | .... | $a_2oa_n$ |
| .... | .... | .... | .... | | .... | .... |
| $a_i$ | $a_ioa_1$ | $a_ioa_2$ | .... | $a_ioa_j$ | .... | $a_ioa_n$ |
| .... | .... | .... | .... | | .... | .... |
| $a_n$ | $a_noa_1$ | $a_noa_2$ | .... | $a_noa_j$ | .... | $a_noa_n$ |

Otherwise, $o$ is not a binary operation in $\mathbf{S}$ and the set $\mathbf{S}$ is not closed under the operation $o$.

(ii) **Commutative law.** If the elements in every row are identical with the corresponding elements in the corresponding column, then the composition $o$ is said to be commutative in $\mathbf{S}$. Otherwise, the binary operation $o$ is not commutative in $\mathbf{S}$.

(iii) **Associative law.** Also we can know from the table whether the binary operation follows associative law or not.

**Note.** The diagonal through $a_1oa_1$ and $a_noa_n$ is called the leading diagonal in the table. If the elements in the table are symmetric about the leading diagonal, then we infer that $o$ is commutative in $\mathbf{S}$.

**Identity element. Definition.**

Let $o$ be a binary operation on a non-empty set S. If there exists an element $e \in S$ such that $aoe = a = eoa \; \forall \; a \in A$, then e is called **Identity of S** w.r.t. the operation o. If e is an identity of S w.r.t. o, then it can be proved to be unique.

**e.g.1.** In Z, 0 is the identity w.r.t. $'+'$ since $a+0=a=0+a, \forall a \in Z$. But in N, 0 is not the idntity w.r.t. + since $0 \notin N$ and 1 is the identity w.r.t. as $'\cdot' \; a \cdot 1 = a = 1 \cdot a \; \forall \; a \in N$.

**e.g. 2.** In R, 0 is the identity w.r.t. + since $a+0=a=0+a, \forall a \in R$.

In R, 1 is the identity w.r.t. $'\cdot'$ since $a \cdot 1 = a = 1 \cdot a, \forall a \in R$.

**Note :** Operations $(-),(\div)$ are not binary operations in N. But $+,-,\bullet$ are binaryy operations in R and $\div$ is a binary operation in $R_*$ (non-zero real number set). Also o is the identity in R w.r.t. +, 1 is the identity in R (w.r.t. $'\bullet'$ where as $'-'$ and $'\div'$ do not have identity element in R.)

**Invertible element. Definition.**

Let $e$ be the identity element in S w.r.t. the binary operation o. An element $a \in S$ is said to be invertible w.r.t. o, if there is an element $b$ in S such that $aob = e = boa$ and $b$ is called inverse of $a$.

If o is associative in S, then inverse of $a$ is unique in S and is denoted by $a^{-1}$ or sometimes as $1/a$ if the operation is $\bullet$ and by $-$ if the operation is $+\bullet$.

**Note : 1.** $aoa^{-1} = a^{-1}oa = e$ and $e^{-1}oe = eoe^{-1} = e$. Also $(a^{-1})^{-1} = a$.

**2.** In R, $-a$ is the inverse w.r.t. '$+$' and $1/a\ (a \neq 0)$ is the inverse w.r.t. '$\cdot$' of $a$.

For : $a + (-a) = 0 = (-a) + a$ and $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a\ (a \neq 0)$

**3.** $-a$ is not the inverse of $a$ in N w.r.t. $+$ and $a^{-1}$ is not the inverse of $a$ in N w.r.t. $+$.

Also $a^{-1}$ is the inverse of $a$ in $R_*$ w.r.t. '$\cdot$' and $-a$ is the inverse of $a$ w.r.t. '$+$' in R.

**e.g. 1.** $\mathbf{S} = \{1, -1, i, -i\}$ and usual multiplication is the operation in **S**. Then we have the following composition table. We can clearly see that is a binary operation in **N** following commutative law and associative law.

| $\bullet$ | 1 | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| 1 | 1 | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | 1 | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | 1 |
| $-i$ | $-i$ | $i$ | 1 | $-1$ |

**e.g. 2.** Consider the binary operation on the set $\{1,2,3,4,5\}$ defined by $aob = \min\{a,b\}$. Composition table is :

| $o$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 2 | 2 | 2 |
| 3 | 1 | 2 | 3 | 3 | 3 |
| 4 | 1 | 2 | 3 | 4 | 4 |
| 5 | 1 | 2 | 3 | 4 | 5 |

**e.g. 3.** Define a binary operation $*$ on the set $A = \{0,1,2,3,4,5\}$ as

$a * b = \begin{cases} a+b, \text{if } a+b<6 \\ a+b-6, \text{if } a+b \geq 6 \end{cases}$. o is the identity w.r.t. $*$ and each element $(a \neq 0)$ of the set is invertible with $6-a$ being the inverse of $a$.

For : Composition table is :

| $*$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

(*i*) $*$ is binary since every entry belongs to A.

(*ii*) Every row is same as the corresponding column $\Rightarrow *$ is commutative.

(*iii*) Since every element of the first row = every corresponding element of the top row, identity element exists and it is 0.

since $0*0=0, 0*1=1, \ldots, 0*5=5$ and $0*0, 1*0=1, 2*0=2, \ldots, 5*0=5$.

(*iv*) Since $1*5=0=5*1, 1^{-1}=5$ and $5^{-1}=1$;

Since $2*4=0=4*2, 2^{-1}=4$ and $4^{-1}=2$; Since $3*3=0, 3^{-1}=3$. Also $0^{-1}=0$.

**Ex. 1.** *Show that the operation $o$ given by $aob = a^b$ is a binary operation on the set of natural numbers $\mathbf{N}$. Is this operation associative and commutative in $\mathbf{N}$?*

***(O. U. A12)***

**Sol.** $\mathbf{N}$ is the set of natural numbers and $o$ is operation defined in $\mathbf{N}$ such that $aob = a^b$ for $a, b \in \mathbf{N}$ When $a, b \in \mathbf{N}, a^b = a \times a \times \ldots b$ times is also a natural number and hence $a^b \in \mathbf{N}$.

$\therefore$ $o$ is binary operation in $\mathbf{N}$. Let $a, b, c \in \mathbf{N}$.

$\therefore$ $(aob)oc = (aob)^c = (a^b)^c = a^{bc}$ and $ao(boc) = aob^c = a^{b^c}$

$\therefore$ $(aob)oc \neq ao(boc)$ and $o$ is not associative in $\mathbf{N}$.

Since $a^b \neq b^a$ i.e. '$o$' is not commutative in $\mathbf{N}$.

**Ex. 2.** *Let $\mathbf{S}$ be a non-empty set and $o$ be an operation on $\mathbf{S}$ defined by $aob = a$ for $a, b \in \mathbf{S}$. Determine whether $o$ is commutative and associative in $\mathbf{S}$.*

**Sol.** Since $aob = a$ for $a, b \in \mathbf{S}$ and $boa = b$ for $a, b \in \mathbf{S}$, $aob \neq boa$.

$\therefore$ $o$ is not commutative in $\mathbf{S}$.

Since $\left.\begin{matrix}(aob)oc = aoc = a \\ ao(boc) = aob = a\end{matrix}\right\}$ for $a, b, c \in \mathbf{S}$.

$\therefore$ $o$ is associative in $\mathbf{S}$.

**Ex. 3.** *$o$ is operation defined on $\mathbf{Z}$ such that $aob = a + b - ab$ for $a, b \in \mathbf{Z}$. Is the operation, $o$ a binary operation in $\mathbf{Z}$? If so, is it associative and commutative in $\mathbf{Z}$?*

**Sol.** If $a, b \in \mathbf{Z}$ we have $a + b \in \mathbf{Z}, ab \in \mathbf{Z}$

$a + b - ab \in \mathbf{Z}$.

$\therefore \quad aob = a + b - ab \in \mathbf{Z}$ $\quad\therefore\quad$ $o$ is a binary operation in $\mathbf{Z}$.

Since $aob = a + b - ab = b + a - ba = boa$, '$o$' is commutative in $\mathbf{Z}$.

Now $(aob)\,oc = (aob) + c - (aob)\,c$

$= a + b - ab + c - (a + b - ab)\,c \quad = a + b - ab + c - ac - bc + abc$

and $ao\,(boc) = a + (boc) - a\,(boc)$

$= a + b + c - bc - a\,(b + c - bc)$

$= a + b + c - bc - ab - ac + abc \quad = a + b - ab + c - ac - bc + abc$

$\therefore\ (aob)\,oc = ao\,(boc)$ and hence $o$ is associative in $\mathbf{Z}$.

**Ex. 4.** $\mathbf{S} = \{a, b, c\}$ *and* $o$ *is an operation on* $\mathbf{S}$ *for which the following composition table is formed. Is the operation* $o$ *a binary operation in* $\mathbf{S}$*? Is the operation* $o$ *in* $\mathbf{S}$ *commutative and associative* ?

| $o$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

**Sol.** All the products formed are the elements of $\mathbf{S}$.

$\therefore$ $o$ is a binary operation in $\mathbf{S}$ and hence $\mathbf{S}$ is closed under the operation $o$.

Since the elements in every row are identical with corresponding elements in the corresponding column, $o$ is commutative in $\mathbf{S}$.

Since $(aob)\,oc = boc = a = aoa = ao\,(boc)$,

$(boa)\,oc = boc = bo\,(aoc)$ etc., $o$ is associative in $\mathbf{S}$.

**Ex. 5.** *Fill in the blanks in the following composition table so that* $o$ *is associative in* $\mathbf{S} = \{a, b, c, d\}$

| $o$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $a$ | $c$ | $d$ |
| $c$ | $c$ | $d$ | $c$ | $d$ |
| $d$ | | | | |

Using associative law and by trial and error :

Since $do\,(aoa) = doa$ and $(doa)\,oa = do\,(aoa) = doa, doa$ must be equal to $d$ only.

Since $do\,(boa) = dob$ and $(dob)\,oa = do\,(boa), dob$ must be equal to $d$ only.

Since $do\,(coa) = doc$ and $(doc)\,oa = do\,(coa), doc$ must be equal to $a$ only.

Since $do\,(doa) = dod$ and $do\,(doa) = (dod)\,oa, dod$ must be equal to $a$.

Thus $d, d, a, a$ are respectively the four products.

**Ex. 6.** *Let* $\mathbf{P}(\mathbf{S})$ *be the power set of a non-empty set* $\mathbf{S}$. *Let* '$\cap$' *be an operation in* $\mathbf{P}(\mathbf{S})$. *Prove that associative law and commutative law are true for the operation* $\cap$ *in* $\mathbf{P}(\mathbf{S})$.

**Sol.** $\mathbf{P}(\mathbf{S})$ = Set of all possible subsets of $\mathbf{S}$.

Let $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbf{P}(\mathbf{S})$. Since $\mathbf{A} \subseteq \mathbf{S}, \mathbf{B} \subseteq \mathbf{S} \Rightarrow \mathbf{A} \cap \mathbf{B} \subseteq \mathbf{S} \Rightarrow \mathbf{A} \cap \mathbf{B} \in \mathbf{P}(\mathbf{S})$

Also $\mathbf{B} \cap \mathbf{A} \subseteq \mathbf{S} \Rightarrow \mathbf{B} \cap \mathbf{A} \in \mathbf{P}(\mathbf{S})$. $\therefore \cap$ is a binary operation in $\mathbf{P}(\mathbf{S})$.

Also $\mathbf{A} \cap \mathbf{B} = \mathbf{B} \cap \mathbf{A}$. $\therefore \cap$ is commutative in $\mathbf{P}(\mathbf{S})$.

Again $\mathbf{A} \cap \mathbf{B}, \mathbf{B} \cap \mathbf{C}, (\mathbf{A} \cap \mathbf{B}) \cap \mathbf{C}$

and $\mathbf{A} \cap (\mathbf{B} \cap \mathbf{C})$ are subsets of $\mathbf{S}$.

$\therefore (\mathbf{A} \cap \mathbf{B}) \cap \mathbf{C}, \mathbf{A} \cap (\mathbf{B} \cap \mathbf{C}) \in \mathbf{P}(\mathbf{S})$.

Since $(\mathbf{A} \cap \mathbf{B}) \cap \mathbf{C} = \mathbf{A} \cap (\mathbf{B} \cap \mathbf{C})$, $\cap$ is associative in $\mathbf{P}(\mathbf{S})$.

**Ex. 7.** $\mathbf{A} = \{a, b\}$. *Consider the set* $\mathbf{S}$ *of all mappings from* $\mathbf{A} \to \mathbf{A}$. *Is the composition of mappings denoted by* $o$ *is a binary composition in* $\mathbf{S}$.

**Sol.** Total number of possible mappings from $\mathbf{A} \to \mathbf{A}$ is 4.

Let them be $\mathbf{I} : \mathbf{A} \to \mathbf{A} = \{(a, a), (b, b)\}$

$f_1 : \mathbf{A} \to \mathbf{A} = \{(a, b), (b, a)\}$

$f_2 : \mathbf{A} \to \mathbf{A} = \{(a, a), (b, a)\}$

$f_3 : \mathbf{A} \to \mathbf{A} = \{(a, a), (b, b)\}$

$\therefore \mathbf{S} = \{\mathbf{I}, f_1, f_2, f_3\}$. Let the composition of mappings be denoted by $o$.

Composition table is :

| $o$ | I | $f_1$ | $f_2$ | $f_3$ |
|---|---|---|---|---|
| I | I | $f_1$ | $f_2$ | $f_3$ |
| $f_1$ | $f_1$ | I | $f_2$ | $f_3$ |
| $f_2$ | $f_2$ | $f_3$ | $f_3$ | $f_3$ |
| $f_3$ | $f_3$ | $f_2$ | $f_2$ | $f_3$ |

Clearly (i) $o$ is binary operation in $\mathbf{S}$,

(ii) $o$ is not commutative in $\mathbf{S}$ and

(iii) $o$ is not associative in $\mathbf{S}$. $\sin a\ (f_2 o f_3) o f_1 \neq f_2 o (f_3 o f_1)$

## EXERCISE 1

**1.** Are the following operations binary on the indicated sets.

(i) The usual addition on $\mathbf{Q}$.

(ii) The usual multiplication on $\mathbf{C}$.

(iii) $o$ is an operation on $\mathbf{Z} - \{0\}$ defined by $aob$ = *l.c.m.* of $a$ and $b$ for $a, b \in \mathbf{Z} - \{0\}$.

(iv) The usual addition in the set of negative integers.

(v) The usual multiplication in the set of negative integers.

(vi) $o$ is an operation in $\mathbf{R}$ defined by $aob = 3a + 2b$ for $a, b \in \mathbf{R}$.

(vii) $\cup$ is an operation in $\mathbf{S}$ and $\mathbf{S} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}\}$ where $\mathbf{A} = \{a_1, a_2\}$, $\mathbf{B} = \{a_2, a_4\}, \mathbf{C} = \{a_4, a_3, a_5\}, \mathbf{D} = \{a_5\}$

**2.** In the following, a set is given and a binary operation is defined on it. Find whether the binary operation is commutative or associative or both in.

(i) $\mathbf{Z} : aob = a + b + ab \ \forall \ a, b \in \mathbf{Z}$.

(ii) $\mathbf{Z} : aob = a + b + 1 \ \forall \ a, b \in \mathbf{Z}$.

(iii) $\mathbf{S} = \{a + b\sqrt{2} / a, b \in \mathbf{R}\}$, usual multiplication.

(iv) $\mathbf{S}$ is the set of even integers : $aob = 3ab, \ \forall \ a, b \in \mathbf{S}$

(v) $\mathbf{Z} : aob = a - b$ (***O.U.M. 05***)

**ANSWERS**

**1.** (*i*) Yes (*ii*) Yes (*iii*) Yes (*iv*) Yes
(*v*) No (*vi*) Yes (*vii*) No

**2.** (*i*) Commutative, associative (*ii*) Commutative, associative
(*iii*) Commutative, associative (*iv*) Commutative, associative
(*v*) Neither associative not commutative

# Groups

## 2.1. ALGEBRAIC STRUCTURE

**Definition.** A non-empty set $\mathbf{G}$ equipped with one or more binary operations is called an **algebraic structure** or an **algebraic system**.

If $o$ is a binary operation on $\mathbf{G}$, then the algebraic structure is written as $(\mathbf{G}, o)$.

**e.g.** $(\mathbf{N}, +), (\mathbf{Q}, -), (\mathbf{R}, +)$ are algebraic structure.

## 2.2. SEMI GROUP

An algebraic structure $(\mathbf{S}, o)$ is called a semi group if the binary operation $o$ is associative in $\mathbf{S}$.

**e.g. 1.** $(\mathbf{N}, +)$ is a semi group. For, $a, b \in \mathbf{N} \Rightarrow a + b \in \mathbf{N}$ and $a, b, c \in \mathbf{N}$

$\Rightarrow (a + b) + c = a + (b + c)$.

**e.g. 2.** $(\mathbf{Q}, -)$ is not a semi group. For, $5, \frac{3}{2}, 1 \in \mathbf{Q}$ does not imply

$\left(5 - \frac{3}{2}\right) - 1 = 5 - \left(\frac{3}{2} - 1\right)$.

**e.g. 3.** $(\mathbf{R}, +)$ is a semi group. For $a, b \in \mathbf{R} \Rightarrow a + b \in \mathbf{R}$ and

$a, b, c \in \mathrm{R} \Rightarrow (a + b) + c = a + (b + c)$

**e.g. 4.** $(\mathbf{S}, o)$ is a semi group. (vide Ex. 2. Art. 1.10.)

**e.g. 5.** $(\mathbf{Z}, o)$ is a semi group. (vide Ex. 3 Art. 1.10.)

**e.g. 6.** $(\mathbf{P}(\mathbf{S}), \cap)$ is a semi group where $\mathbf{P}(\mathbf{S})$ is the power set of non-empty set $\mathbf{S}$.

**e.g. 7.** $(\mathbf{P}(\mathbf{S}), \cup)$ is a semi group where $\mathbf{P}(\mathbf{S})$ is the power set of a non-empty set $\mathbf{S}$.

**e.g. 8.** $(\mathbf{S}, o)$ is a semi group (vide Ex. 7, Art 1.10.)

**e.g. 9.** $\mathbf{Q}$ is the set of rational numbers. $o$ is a binary operation defined on $\mathbf{Q}$ such that $aob = a - b + ab$ for $a, b \in \mathbf{Q}$.

$(\mathbf{Q}, o)$ is not a semi group.

For $a, b, c \in \mathbf{Q}$,

$$(aob)oc = (aob) - c + (aob)c = a - b + ab - c + (a - b + ab)c$$
$$= a - b + ab - c + ac - bc + abc$$
$$ao(boc) = a - (boc) + a(boc) = a - (b - c + bc) + a(b - c + bc)$$
$$= a - b + c - bc + ab - ac + abc$$

and $(aob)oc \neq ao(boc)$.

**e.g. 10.** $\mathbf{Q}$ is the set of rational numbers. $o$ is a binary operation defined on $\mathbf{Q}$ such that for $a, b \in \mathbf{Q}, aob = a + b - ab$

$(\mathbf{Q}, o)$ is a semi group.

For $a, b, c \in \mathbf{Q}$,

$$(aob)\,oc = (aob) + c - (aob)\,c$$
$$= a + b - ab + c - (a + b - ab)\,c \quad = a + b + c - bc - ab - ac + abc$$
$$= a + b + c - bc - a\,(b + c - bc) = a + (boc) - a\,(boc)$$
$$= ao\,(boc)$$

**e.g. 11.** The set $\mathbf{Q}$ under the binary operation $o$ defined by $aob = \dfrac{a+b}{2}$ is not a semigroup. For $(a\,o\,b)\,o\,c \neq a\,o\,(b\,o\,c)$.

## 2.3. IDENTITY ELEMENT

**Definition.** Let $\mathbf{S}$ be a non-empty set and $o$ be a binary operation on $\mathbf{S}$.

(i) If there exists an element $e_1 \in \mathbf{S}$ such that $e_1oa = a$ for $a \in \mathbf{S}$ then $e_1$ is called a left identity of $\mathbf{S}$ w.r.t. the operation $o$.

(ii) If there exists an element $e_2 \in \mathbf{S}$ such that $aoe_2 = a$ for $a \in \mathbf{S}$ then $e_2$ is called a right identity of $\mathbf{S}$ w.r.t. the operation $o$.

(iii) If there exists an element $e \in \mathbf{S}$ such that $e$ is both a left and a right identity of $\mathbf{S}$ w.r.t. $o$, then $e$ is called an identity of $\mathbf{S}$.

**e.g. 1.** In the algebraic system $(\mathbf{Z}, +)$, the number 0 is an identity element.

**e.g. 2.** In the algebraic system $(\mathbf{R}, .)$ the number 1 is an identity element.

**e.g. 3.** Let $(\mathbf{S}, o)$ be an algebraic structure such that $\mathbf{S}$ contains at least two elements and $o$ be the operation such that $aob = b$ for $a, b \in \mathbf{S}$. Then each element of $\mathbf{S}$ is a left identity of $(\mathbf{S}, o)$ but $(\mathbf{S}, o)$ has no right identity.

Let $(\mathbf{S}, o)$ be an algebraic structure such that $\mathbf{S}$ contains at least two elements and $o$ be the operation such that $aob = a$ for $a, b \in \mathbf{S}$. Then each element of $\mathbf{S}$ is a right identity of $(\mathbf{S}, o)$ but $(\mathbf{S}, o)$ has no left identity.

**e.g. 4.** Let $(\mathbf{S}, .)$ be an algebraic structure such that $\mathbf{S}$ is the set of all even integers. It has neither a left identity nor a right identity.

**Note.** In an algebraic structure $(\mathbf{S}, o)$,

(i) a left identity may exist and a right identity may not exist.

(ii) a right identity may exist and a left identity may not exist.

(iii) The identity may not exist.

**Theorem 1.** ***Let*** $(\mathbf{S}, o)$ ***be an algebraic structure. If*** $e_1$ ***and*** $e_2$ ***be respectively left and right identities of*** $\mathbf{S}$ ***w.r.t.*** $o$***, then*** $e_1 = e_2$.

**Proof.** Since $e_1, e_2 \in \mathbf{S}$ and $e_1$ is a left identity in $\mathbf{S}$ w.r.t. $o$, we have $e_1oe_2 = e_2$.

Since $e_1, e_2 \in \mathbf{S}$ and $e_2$ is a right identity in $\mathbf{S}$ w.r.t. $o$, we have $e_1oe_2 = e_1$.

$\therefore$ From (1) and (2), $e_1 = e_2$.

**Theorem 2.** *Let* $(\mathbf{S}, o)$ *be an algebraic structure and if* $e$ *is an identity of* $\mathbf{S}$ *w.r.t.* $o$*, then it is unique.*

**Proof.** If possible, let $e, e'$ be identities of $\mathbf{S}$.

$\therefore \quad eoe' = e'$ (taking $e$ left identity)

and $eoe' = e$ (taking $e'$ as right identity)

$\therefore \quad e' = e$ and hence identity in $\mathbf{S}$ with respect to $o$ is unique.

This identity in $\mathbf{S}$ is called the identity element in $\mathbf{S}$ w.r.t. the operation $o$.

**Note 1.** If $\mathbf{S}$ is the set of even integers, then the algebraic structure $(\mathbf{S}, .)$ has no identity element.

**2.** The algebraic structure $(\mathbf{Q}, .)$ has 1 as the identity element whereas the structure $(\mathbf{Q}, +)$ has 0 as the identity element.

**e.g.** If $\mathbf{S}$ is the set of all mappings from a finite set $\mathbf{A}$ into $\mathbf{A}$ and $o$ is the composition of mapping in $\mathbf{S}$, the identity mapping $\mathbf{I} \in \mathbf{S}$ is the identity element in $\mathbf{S}$ w.r.t. $o$.

**3.** If multiplicative notation is used for a binary composition then the identity element w.r.t. the operation, if exists, is often denoted by 1. 1 is called the multiplicative identity or unit element.

If additive notation is used then identity element, if exists, is often denoted by 0. 0 is called the additive identity or zero element.

The elements 1 and 0 should not be confused with integers, although in special cases they may actually be integers.

## 2. 4. MONOID

**Definition.** A semi group $(\mathbf{S}, o)$ with the identity element w.r.t. $o$ is known as a monoid. i.e. $(\mathbf{S}, o)$ is a monoid if $\mathbf{S}$ is a non-empty set and $o$ a binary operation in $\mathbf{S}$ such that $o$ is associative and there exists an identity element w.r.t. $o$.

**e.g.1.** $(\mathbf{Z}, +)$ is a monoid and the identity is 0.

**e.g. 2.** $(\mathbf{Z}, .)$ is monoid and the identity element is 1.

**e.g. 3.** $\mathbf{S}$ is the set of all mappings from a finite set $\mathbf{A}$ to itself and $o$ is the composition of mappings in $\mathbf{S}$. Then $(\mathbf{S}, o)$ is monoid with the identity element 1 (identity mapping).

**e.g. 4.** Let $\mathbf{S}$ be the set of all $2 \times 2$ matrices such that each element in $\mathbf{S}$ are rational numbers. If matrix multiplication $(.)$ is the binary operation on $\mathbf{S}$ then $(\mathbf{S}, .)$ is a monoid and unit matrix $\mathbf{I}_2$ is the identity element in $\mathbf{S}$.

Similarly if matrix addition $(+)$ is the binary operation on $\mathbf{S}$, then $(\mathbf{S}, +)$ is a monoid and null matrix $\mathbf{O}_2$ is the identity element in $\mathbf{S}$.

**e.g. 5.** $\mathbf{S}$ is the set of all odd integers and $.$ is the usual multiplication in $\mathbf{S}$. Then $(\mathbf{S}, .)$ is a monoid with integer 1 as the identity element in $\mathbf{S}$.

**Note. Existence of identity** : If $\mathbf{S}$ is a finite set and $o$ is a binary operation in $\mathbf{S}$, we observe from the Caley's Composition table the following :

If the row (column) headed by an element $a_i$ coincides with the first row (first column), then we say that identity exists in $(\mathbf{S}, o)$ and $a_i$ is the identity in $(\mathbf{S}, o)$.

## 2. 5. INVERTIBLE ELEMENT

**Definition.** Let $(\mathbf{S}, o)$ be an algebraic structure with the identity element $e$ in $\mathbf{S}$ w.r.t. $o$. An element $a \in \mathbf{S}$ is said to be left invertible or left regular if there exists an element $x \in \mathbf{S}$ such that $xoa = e$. $x$ is called a left inverse of $a$, w.r.t. $o$.

An element $a \in \mathbf{S}$ is said to be right invertible or right regular if there exists an element $y \in \mathbf{S}$ such that $aoy = e$. $y$ is called a right inverse of $a$, w.r.t. $o$.

An element $x$ which is both a left inverse and a right inverse of $a$ is called an **inverse** of $a$ and $a$ is said to be **invertible** or **regular**.

Thus : $a$ is invertible or regular w.r.t. $o \Leftrightarrow a$ is left invertible or left regular w.r.t. $o$, and $a$ is right invertible or right regular w.r.t. $o$.

**Theorem 3.** *Let $(\mathbf{S}, o)$ be a monoid and $a \in \mathbf{S}$. If $b$ and $c$ are left and right inverses respectively of $a$ then $b = c$.*

**Proof.** Let $e$ be the identity in $\mathbf{S}$ w.r.t. $o$.

Now $ba = e, ac = e$.

$\therefore \quad b = be = b(ac) = (ba)c = ec = c$.

**Theorem 4.** *Let $(\mathbf{S}, o)$ be a monoid. If $a \in \mathbf{S}$ and $a$ is invertible w.r.t. $o$, then inverse of $a$ w.r.t. $o$ is unique.*

**Proof.** Let $e$ be the identity element of $\mathbf{S}$ w.r.t. $o$. Since $a$ is invertible, it has an inverse w.r.t. $o$. If possible, let $b \in \mathbf{S}$ and $c \in \mathbf{S}$ be two inverses of $a$ w.r.t. $o$ in $\mathbf{S}$.

$\therefore \quad aob = e = boa$ and $aoc = e = coa$.

Now $co(aob) = coe = c$ …(1)

and $co(aob) = (coa)ob = eob = b$ …(2)

$\therefore$ From (1) and (2), $c = b$.

$\therefore$ Inverse of $a$ is unique.

The unique inverse of $a$ is denoted by $a^{-1}$. If the operation is taken multiplicatively and by $-a$ if the operation is taken additively.

**Note 1.** The inverse of the identity element $e$ is $e$.

$[\because \; eoe = e$ i.e., $e^{-1} = e$ or, $e + (-e) = e$ i.e., $= -e]$

**2.** $aoa^{-1} = a^{-1}oa = e, a + (-a) = (-a) + a = e$

**3.** $a^{-1}oa = aoa^{-1} = e \Rightarrow (a^{-1})^{-1} = a$ and

$a + (-a) = (-a) + a = e \Rightarrow -(-a) = a$.

i.e. the inverse of the inverse of $a$ is $a$.

## 2.6. CANCELLATION LAWS

Let $\mathbf{S}$ be non-empty set and $o$ be a binary operation on $\mathbf{S}$.

For $a, b, c \in \mathbf{S}$.

(i) $aob = aoc \Rightarrow b = c$, (ii) $boa = coa \Rightarrow b = c$.

(i) is called **left cancellation law**. (ii) is called **right cancellation law** and (i), (ii) are called **cancellation laws**.

**e.g. 1.** In $(\mathbf{N}, .)$, $3x = 3y \Rightarrow x = y$

**e.g. 2.** In $(\mathbf{R}, +), x + 2\sqrt{3} = y + 2\sqrt{3} \Rightarrow x = y$

## 2. 7. GENERALISED ASSOCIATIVE LAWS

Let $\mathbf{S} = \{a_1, a_2, \ldots\ldots a_n\}$. Let $(\mathbf{S}, .)$ be an algebraic structure in which $.$ is associative. We define their product inductively :

$$\prod_{k=1}^{n} a_k = a_1 . a_2 \ldots\ldots a_n = (a_1 \ldots\ldots a_{n-1}) a_n,$$

Then we have the following by induction :

$$\prod_{p=1}^{m} a_p . \prod_{q=1}^{n-m} a_{m+q} = \prod_{r=1}^{n} a_r \quad i.e., \quad (a_1 \ldots a_m)\,(a_{m+i} \ldots a_n) = a_1 . a_2 \ldots\ldots a_n$$

Also if $a \in$ S, we can have $(a.a.a.a)(a.a)(a.a.a) \ldots = a.a.a.a.a \ldots$

## 2.8. GROUP

**Definition.** If $\mathbf{G}$ is a non-empty set and $o$ is a binary operation defined on $\mathbf{G}$ such that the following three laws are satisfied then $(\mathbf{G}, o)$ is a group.

$\mathbf{G}_1$. **Associative law**. For $a, b, c \in \mathbf{G}, (aob)oc = ao(boc)$

$\mathbf{G}_2$. **Identity law**. $\exists e \in \mathbf{G}$ such that $aoe = a = eoa$ for every $a \in \mathbf{G}$ is called an identity element in $\mathbf{G}$.

$\mathbf{G}_3$. **Inverse law**. For each $a \in \mathbf{G} \exists$ an element $b \in \mathbf{G}$ such that $aob = boa = e.$ $b$ is called an inverse of $a$.

**Note 1.** A group is an algebraic structure. It can also be written as $<\mathbf{G}, o>$.

**2.** A semigroup $(\mathbf{G}, o)$ is a group if $\mathbf{G}_2$ and $\mathbf{G}_3$ are satisfied.

**3.** A monoid $(\mathbf{G}, o)$ is a group if $\mathbf{G}_3$ is satisfied.

**4.** $\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3$ are called group axioms or group postulates.

**5.** It is possible to define more than one binary composition on $\mathbf{G}$. Thus we can have over $\mathbf{G}$ different groups depending on binary compositions defined on $\mathbf{G}$.

For example, $\mathbf{Z}$ is a group with infinitely many operations defined by $aob = a + b + n$, $n = 1, 2, 3, \ldots\ldots$. If in a group there is no likelihood of any confusion regarding the binary composition, we shall simply refer to the set $\mathbf{G}$ as a group.

**6.** It is possible to define the same operation on different sets so that each may form a group for the operation. For example, $(\mathbf{Z}, +), (\mathbf{Q}, +), (\mathbf{R}, +), (\mathbf{C}, +)$ are all groups.

**Abelian or Commutative group**

**Definition.** $\mathbf{G}_4$ : For the group $a, b \in \mathbf{G}, aob = boa$. If $\mathbf{G}_4$ is satisfied, then $(\mathbf{G}, o)$ is called an abelian or a commutative group.

Otherwise (if $\mathbf{G}_4$ is not satisfied) $(\mathbf{G}, o)$ is said to be a non-abelian group.

It is possible that $aob = boa$ for certain elements $a, b$ of a non-abelian group and in such cases we say that these particular elements commute.

**Note.** $\mathbf{G}_4$ is called commutative axiom or commutative postulate of the group.

**Finite and Infinite groups**

**Definition.** If the set $\mathbf{G}$ contains a finite number of elements then the group $(\mathbf{G}, o)$ is called a finite group.

Otherwise the group $(\mathbf{G}, o)$ is called an infinite group.

**Note. Existence of inverse**. If $\mathbf{S}$ is a finite set and $o$ is a binary composition in $\mathbf{S}$, we observe from the Caley's composition table the following :

If the identity element in $(\mathbf{S}, o)$ is found at the intersection of the row headed by $a_i$ and the column headed by $a_j$ then $a_i$ and $a_j$ are said to be the inverses of each other in $(\mathbf{S}, o)$.

## 2. 9. ORDER OF A GROUP

**Definition.** The number of elements in a group $(\mathbf{G}, o)$ (finite or infinite) is called the *order* of the group $\mathbf{G}$ and is denoted by $o(\mathbf{G})$ or $|\mathbf{G}|$. If $\mathbf{G}$ is infinite, then we say that the order of $\mathbf{G}$ is infinite.

Thus : (i) If the number of elements in a group $\mathbf{G}$ is $n$, then $o(\mathbf{G}) = |\mathbf{G}| = n$.

In general, for a finite set S, $|\mathbf{S}|$ is the number of elements in S.

(ii) If $o(\mathbf{G}) = 2n, n \in \mathbf{N}$, we say that the group is of even order.

(iii) If $o(\mathbf{G}) = 2n - 1, n \in \mathbf{N}$ we say that the group is of odd order

**Theorem 5.** ***In a group*** $\mathbf{G}$, ***identity element is unique.***

**Proof.** If possible let $e_1, e_2$ be two identity elements in the group $(\mathbf{G}, o)$

$\therefore$ $e_1 e_2 = e_2 e_1 = e_2$ is an identity in $\mathbf{G}$.

and $e_2 e_1 = e_1 e_2 = e_1$ is an identity in $\mathbf{G}$.

$\therefore$ $e_1 = e_2$.

**Theorem 6.** ***In a group*** $\mathbf{G}$, ***inverse of any element is unique.***

**Proof.** Let $e$ be the identity element in the group $(\mathbf{G}, .)$.

If $a \in \mathbf{G}$ then $a$ will have an inverse.

If possible, let $b \in \mathbf{G}$ and $c \in \mathbf{G}$ be two inverses of $a$ in $\mathbf{G}$.

$\therefore$ $ab = ba = e$ and $ac = ca = e$.

$\therefore$ $c(ab) = ce = c$ …(1)

and $c(ab) = (ca)b = e.b = b$ …(2)

$\therefore$ From (1) and (2), $b = c$.

**Note 1.** We denote the inverse of $a$ as $a^{-1}$ or $-a$ depending on the operation.

**2.** Since $a^{-1}a = aa^{-1} = e$, we have $(a^{-1})^{-1} = a$. i.e. the *inverse of the inverse of an element in a group is itself.*

**3.** Since $ee = e$, the inverse of the identity element in a group is itself. *i.e.* $e^{-1} = e$.

**e.g. 1.** The set $\mathbf{Z}$ of integers is a group w.r.t. usual addition.

For (i) For $a, b \in \mathbf{Z}, a + b \in \mathbf{Z}$.

(ii) For $a, b, c \in \mathbf{Z}, (a + b) + c = a + (b + c)$

(iii) $0 \in \mathbf{Z}$ such that $0 + a = a + 0 = a$ for each $a \in \mathbf{Z}$

$\therefore$ 0 is the identity element in $\mathbf{Z}$.

(iv) For $a \in \mathbf{Z}$ $\exists -a \in \mathbf{Z}$ such that $a + (-a) = (-a) + a = 0$

$\therefore$ $-a$ is the inverse of --.

$\therefore$ $(\mathbf{Z}, +)$ is a group.

Also $a, b \in \mathbf{Z} \Rightarrow a + b = b + a$.

$\therefore$ $(\mathbf{Z}, +)$ is an abelian group.

**e.g. 2.** The set $\mathbf{N}$ of natural numbers w.r.t. usual multiplication is not a group.

For (i) For $a, b \in \mathbf{N}, ab \in \mathbf{N}$.

(ii) For $a, b, c \in \mathbf{N}, a(bc) = (ab)c$.

(iii) $1 \in \mathbf{N}$ such that $1a = a$ for $a \in \mathbf{N}$.

(iv) There is no $n \in \mathbf{N}$ such that $an = 1$ for $a \in \mathbf{N}$.

$\therefore$ Inverse law is not true.

$\therefore$ The algebraic structure $(\mathbf{N}, .)$ is not a group.

**Note.** Even if one of the laws $\mathbf{G}_1$ to $\mathbf{G}_3$ is not true, $\mathbf{G}$ is not a group. Hence to prove that $\mathbf{G}$ is not a group it is sufficient if one law is proved to be not true.

**e.g. 3.** $(\mathbf{Z}, o)$ is not a group since $3 \in \mathbf{Z}$ has no inverse in $\mathbf{Z}$ (Inverse law $\mathbf{G}_3$ is not true).

**e.g. 4.** $(\mathbf{Q}, +)$ is an abelian group with 0 as the identity element and $-a$ is the inverse of $a$.

**e.g. 5.** $(\mathbf{Q}, .)$ is not a group since $0 \in \mathbf{Q}$ has no inverse.

**e.g. 6.** $(\mathbf{Q} - \{0\}, .)$ is an abelian group with 1 as the identity element and $\frac{1}{a}$ is the inverse of $a$.

**e.g. 7.** $(\mathbf{R} - \{0\}, .)$ is an abelian group with 1 as the identity element and $\frac{1}{a}$ as the inverse of $a$.

**e.g. 8.** $\mathbf{S}$ is the set of all odd integers. Then $(\mathbf{S}, .)$ is not a group since $5 \in \mathbf{S}$ has no inverse in $\mathbf{S}$.

**e.g. 9.** $\mathbf{S}$ is any non-empty set $(\mathbf{P}(\mathbf{S}), \cup)$ is not a group although $\phi$ is the identity element w.r.t. $\cup$ since for any non-empty subset of $\mathbf{S}$, there is no inverse in $\mathbf{P}(\mathbf{S})$.

**e.g. 10.** $\mathbf{S}$ is any non-empty set. $(\mathbf{P}(\mathbf{S}), \cap)$ is not a group although $\mathbf{S}$ is the identity element w.r.t. $\cap$ since for any non-empty subset of $\mathbf{S}$ there is no inverse in $\mathbf{P}(\mathbf{S})$.

**e.g. 11.** Let $\mathbf{V}$ be the set of all position vectors in a plane containing the origin of reference. It is an abelian group under vector addition with $\bar{o}$ as the identity element and $-\bar{a}$ as the inverse $a \in \mathbf{V}$.

**e.g. 12.** For any fixed positive integer $n$, the set $\mathbf{R}_n$ of all $n \times n$ matrices over the real numbers from an abelian group under matrix addition as binary composition. $\mathbf{O}_{n \times n}$ is the additive identity and for $\mathbf{A} \in \mathbf{R}_n$, $-\mathbf{A}$ is the inverse.

**e.g. 13.** (i) $\mathbf{G} = \{0\}$ (number 0) is a group w.r.t. usual addition.

(ii) $\mathbf{G} = \{0\}$ (number 0) is a group w.r.t. usual multiplication.

For : Closure, Associative laws are satisfied.

For $0 \in \mathbf{G}, \exists 0 \in \mathbf{G}$ such that $0.0 = 0$.

$\therefore$ 0 is the identity.

For $0 \in \mathbf{G}, \exists 0 \in \mathbf{G}$ such that $0.0 = 0$

$\therefore$ 0 is the inverse of 0.

**Note 1.** $\mathbf{G} = \{0\}$ is the only set which is a group both w.r.t. usual addition and usual multiplication.

**2.** In general, if $\mathbf{G}$ is a group w.r.t. usual addition, then it cannot be a group w.r.t. usual multiplication since the multiplicative inverse does not exist for the additive identity 0. Similarly a multiplicative group cannot be an additive group.

**e.g. 14.** If $\mathbf{G} = \{a\}$ and $\cdot$ is a binary composition on $\mathbf{G}$, then $(\mathbf{G}, \cdot)$ is group. $a$ is the identity and $a$ is the inverse of $a$ in $\mathbf{G}$.

**e.g. 15.** $\mathbf{G} = \{-1, 0, 1\}$, under usual addition, is not a group since closure law is not true. $(1 + 1 = 2 \notin \mathbf{G})$.

**e.g. 16.** $\mathbf{G} = \{-1, 0, 1\}$, under usual multiplication is not a group since $0 \in \mathbf{G}$ has no inverse.

## SOLVED PROBLEMS

**Ex. 1.** *If* $\mathbf{G}$ *is the set of even integers i.e.* $\mathbf{G} = \{\ldots -4, -2, 0, 2, 4 \ldots\}$, *then prove that* $\mathbf{G}$ *is an abelian group with usual addition as the operation.*

**Sol.** Let $a, b, c \in \mathbf{G}$. $\therefore$ We can take $a = 2x, b = 2y, c = 2z$, where $x, y, z \in \mathbf{Z}$.

(i) **Closure.** $a, b \in \mathrm{G} \Rightarrow a + b \in \mathrm{G}$.

since $a + b = 2x + 2y = 2(x + y) \in \mathbf{G}$.

(ii) **Associativity.** $a, b, c \in \mathbf{G} \Rightarrow a + (b + c) = (a + b) + c$

since $a + (b + c) = 2x + (2y + 2z) = 2[x + (y + z)]$

$= 2[(x + y) + z] = (2x + 2y) + 2z$

$= (a + b) + c$.

(iii) **Existence of identity.** $a \in \mathbf{G}$. $\exists 0 \in \mathbf{G}$ such that

$a + 0 = 0 + a = a$.

since $a + 0 = 2x + 0 = 2x = a$ and $0 + a = 0 + 2x = 2x = a$

$\therefore$ 0 is the identity element in $\mathbf{G}$.

(iv) **Existence of inverse.** $a \in \mathbf{G}$. $\exists -a \in \mathbf{G}$ such that $a + (-a) = -a + a = 0$.

since $a + (-a) = 2x + (-2x) = 0$ and

$(-a) + a = (-2x) + 2x = 0$

$\therefore$ $(\mathbf{G}, +)$ is a group.

(v) **Commutativity.** $a \in \mathbf{G}, b \in \mathbf{G} \Rightarrow a + b = b + a$ since

$a + b = 2x + 2y = 2(x + y) = 2(y + x) = 2y + 2x = b + a$

$\therefore$ $(\mathbf{G}, +)$ is an abelian group.

**Note.** 0 is the unique identity element and $-a$ is the unique inverse of $a$.

Also cancellation laws hold.

Further $-(a + b) = -a + (-b) = (-b) + (-a)$

i.e. the additive inverse of $(a + b)$ is equal to the additive inverse of $b +$ the additive inverse of $a$.

**Ex. 2.** *Show that set* $\mathbf{Q}_+$ *of all +ve rational numbers forms an abelian group under the composition defined by* $o$ *such that* $aob = (ab)/3$ *for* $a, b \in \mathbf{Q}_+$.

**Sol.** $\mathbf{Q}_+$ is the set of all +ve rational numbers and for $a, b \in \mathbf{Q}_+$, we have the operation $o$ such that $aob = \frac{ab}{3}$.

**Closure.** $a, b \in \mathbf{Q}_+ \Rightarrow aob \in \mathbf{Q}_+$. since $a, b \in \mathbf{Q}_+$ and so $\frac{ab}{3} \in \mathbf{Q}_+$.

**Associativity**. $a, b, c \in \mathbf{Q}_+ \Rightarrow (aob)oc = ao(boc)$

since $(aob)\,oc = \left(\frac{ab}{3}\right)oc = \left\{\frac{ab}{3}.c\right\}\Big/3 \qquad = \frac{a}{3}\left\{\frac{bc}{3}\right\} = \frac{a}{3}(boc) = ao(boc)$

**Existence of identity**. Let $a \in \mathbf{Q}_+$. Let $e \in \mathbf{Q}_+$ such that $eoa = a$ i.e., $\frac{ea}{3} = a$

i.e. $ea - 3a = 0$ i.e. $a(e-3) = 0$

i.e. $e - 3 = 0 \quad (\because a \neq 0)$ i.e. $e = 3$.

clearly $aoe = \frac{ea}{3} = \frac{a}{3} \times 3 = a$

$\therefore$ $e$ is an element in $\mathbf{Q}_+$ such that $eoa = aoe = a$.

i.e. $e = 3$ is the identity element in $\mathbf{Q}_+$

**Existence of inverse.** Let $a \in \mathbf{Q}_+$. Let $b \in \mathbf{Q}_+$ such that $aob = e$ i.e., $\frac{ab}{3} = 3$

i.e. $b = \frac{9}{a} \quad (\because a \neq 0)$

$\therefore$ For every $a \in \mathbf{Q}_+$ $\exists \frac{9}{a} \in \mathbf{Q}_+$ such that $ao\frac{9}{a} = \frac{9}{a}oa = e$.

**Commutativity.** $a, b \in \mathbf{Q}_+ \Rightarrow aob = boa$. Since $aob = \frac{ab}{3} = \frac{ba}{3} = boa$.

$\therefore$ $(\mathbf{Q}_+, .)$ is an infinite abelian group.

**Ex. 3.** *Show that the set* $\mathbf{G} = \{x / x = 2^a 3^b$ *and* $a, b \in \mathbf{Z}\}$ *is a group under multiplication.*

**Sol.** Let $x, y, z \in \mathbf{G}$. Let $x = 2^p 3^q$, $y = 2^r 3^s$, $z = 2^l 3^m$ where $p, q, r, s, l, m \in \mathbf{Z}$.

We know that (i) $p + r, q + s \in \mathbf{Z}$

(ii) $(p + r) + l = p + (r + l), (q + s) + m = q + (s + m)$

**Closure**. $x, y \in \mathbf{G} \Rightarrow xy \in \mathbf{G}$, since $xy = 2^p 3^q 2^r 3^s = 2^{p+r} 3^{q+s} \in \mathbf{G}$.

**Associativity.** $x, y, z \in \mathbf{G} \Rightarrow (xy)\,z = x(yz)$,

since $(xy)\,z = (2^p 3^q 2^r 3^s)\,2^l 3^m = 2^{p+(r+l)} 3^{q+(s+m)}$

$= 2^p 3^q (2^{r+l} 3^{s+m}) = 2^p 3^q (2^r 3^s 2^l 3^m) = x(yz)$.

**Existence of identity**. Let $x \in \mathbf{G}$. We know that $e = 2^0 3^0 \in \mathbf{G}$ since $0 \in \mathbf{Z}$.

$\therefore$ $xe = 2^p 3^q 2^0 3^0 = 2^{p+0} 3^{q+0} = 2^p 3^q = x$

and $ex = 2^0 3^0 2^p 3^q = 2^p 3^q = e$.

$\therefore$ $e \in \mathbf{G}$ such that $xe = ex = x$.

$\therefore$ $e = 2^0 3^0$ is the identity element in $\mathbf{G}$.

**Existence of inverse**. Let $x \in \mathbf{G}$.

Now $y = 2^{-p} 3^{-q} \in \mathbf{G}$ exists since $-p, -q \in \mathbf{Z}$ such that

$xy = 2^p 3^q 2^{-p} 3^{-q} = 2^0 3^0 = e$

and $yx = 2^{-p} 3^{-q} 2^p 3^q = 2^0 3^0 = e$

$\therefore$ For every $x = 2^p 3^q \in \mathbf{G}$ there exists $y = 2^{-p} 3^{-q} \in \mathbf{G}$ such that $xy = yx = e$.

$\therefore$ $\mathbf{G}$ is a group under multiplication.

**Ex. 4.** *Prove that the set of martices* $\mathbf{A}_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ $\alpha \in \mathbf{R}$ *forms a group w.r.t. matrix multiplication if* $\cos\theta = \cos\phi \Rightarrow \theta = \phi$.

**Sol.** Let $\alpha, \beta, \gamma \in \mathbf{R}$ and $\mathbf{G} = \{\mathbf{A}_\alpha / \alpha \in \mathbf{R}\}$. (

**Closure.** $\mathbf{A}_\beta \mathbf{A}_\alpha \in \mathbf{G} \Rightarrow \mathbf{A}_\alpha \mathbf{A}_\beta \in \mathbf{G}$

since $\mathbf{A}_\alpha \mathbf{A}_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} \in \mathbf{G}$

**Associativity.** $\mathbf{A}_\alpha, \mathbf{A}_\beta, \mathbf{A}_\gamma \in \mathbf{G} \Rightarrow (\mathbf{A}_\alpha \mathbf{A}_\beta)\mathbf{A}_\gamma = \mathbf{A}_\alpha(\mathbf{A}_\beta \mathbf{A}_\gamma)$

(Matrix multiplication is associative)

since $(\mathbf{A}_\alpha \mathbf{A}_\beta)\mathbf{A}_\gamma = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} \begin{bmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{bmatrix}$

$= \begin{bmatrix} \cos(\alpha+\beta+\gamma) & -\sin(\alpha+\beta+\gamma) \\ \sin(\alpha+\beta+\gamma) & \cos(\alpha+\beta+\gamma) \end{bmatrix}$

and $\mathbf{A}_\alpha(\mathbf{A}_\beta \mathbf{A}_\gamma) = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos(\beta+\gamma) & -\sin(\beta+\gamma) \\ \sin(\beta+\gamma) & \cos(\beta+\gamma) \end{bmatrix}$

$= \begin{bmatrix} \cos(\alpha+\beta+\gamma) & -\sin(\alpha+\beta+\gamma) \\ \sin(\alpha+\beta+\gamma) & \cos(\alpha+\beta+\gamma) \end{bmatrix}$

**Existence of identity.** $A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathrm{I} \in \mathrm{G}$

Clearly $\mathbf{A}_\alpha \mathbf{A}_0 = \mathbf{A}_0 \mathbf{A}_\alpha = \mathbf{A}_\alpha$ $\therefore$ $\mathbf{A}_0 = \mathbf{I}$ is the identity element in $\mathbf{G}$.

**Existence of inverse.**

Since $|\mathbf{A}_\alpha| = \sin^2\alpha + \cos^2\alpha = 1$, $\mathbf{A}_\alpha$ is non-singular.

$\therefore$ Inverse of $\mathbf{A}_\alpha$ exists in $\mathbf{G}$ and it is $\mathbf{A}_\alpha^{-1} = \dfrac{1}{|\mathbf{A}_\alpha|}(adj.\mathbf{A}_\alpha)$

$= \dfrac{1}{1}\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = \mathbf{A}_{-\alpha}$

$\therefore$ $\mathbf{A}_{-\alpha} \in \mathbf{G}$ such that $\mathbf{A}_\alpha \mathbf{A}_{-\alpha} = \mathbf{A}_{-\alpha}\mathbf{A}_\alpha = \mathbf{A}_0$

$\therefore$ $\mathbf{G}$ is a group under matrix multiplication.

**Ex. 5.** *Prove that the set-Z of all integers form an abelian group w.r.t. the operations defined by* $a * b = a + b + 2$, *for all* $a, b \in Z$.

**Sol.** Let $a, b, c \in \mathrm{Z}$ and $*$ is the operation defined on $Z$ as $a * b = a + b + 2$.

**1. Closure.** $a, b \in \mathrm{Z} \Rightarrow a * b = a + b + 2 \in \mathrm{Z}$

**2. Associativity :** $a,b,c \in Z$

$(a*b)*c = (a+b+2)*c = a+b+2+c+2 = a+(b+c+2)+2$

$= a*(b+c+2) = a*(b*c)$ .

**3. Existence of Identity :** $a,e \in Z$

$a*e = a \Rightarrow a+e+2 = a \Rightarrow e = -2$ and $e*a = a \Rightarrow e+a+2 = a \Rightarrow e = -2$

So $\exists e \in Z$ such that $a*e = e*a = a$. $\therefore$ $e$ is the identity in $Z$. Here $e = -2$.

**4. Existence of Inverse :** Let $a,b \in Z$

Now $a*b = e \Rightarrow a + b + 2 = -2 \Rightarrow b = -4 - a$ and

$b*a = e \Rightarrow b + a + 2 = -2 \Rightarrow b = -4 - a$

So $a*b = b*a = e$. $\therefore -4 - a \in Z$ is the inverse of $a$.

**5. Commutativity :** Let $a, b \in Z$.

$a*b = a + b + 2 = b + a + 2 = b*a$.

$\therefore$ $(Z, *)$ is an abelian group.

**Ex.6.** *Prove that the set G of rational (real) numbers other than* 1, *with operation* $\oplus$ *such that* $a \oplus b = a + b - ab$ *for* $a, b \in G$ *is an abelian group. Hence show that* $x = 3/2$ *is a solution of the equation* $4 \oplus 5 \oplus x = 7$ .

**Sol.** G is the set of rational (real) numbers other than 1.

$\oplus$ is the operation considered on G as $a \oplus b = a + b - ab$ *for* $a, b \in$ G.

Let $a,b,c \in G$ and so $a \neq 1, b \neq 1, c \neq 1$ .

**1. Closure :** $a \oplus b = a + b - ab \in$ G.

**2. Associativity :** $(a \oplus b) \oplus c = (a + b - ab) \oplus c$.

$= a + b - ab + c - (a + b - ab)c = a + b - ab + c - ac - bc + abc$

$= a + b + c - bc - ab - ac - abc = a + b + c - bc - a(b+c - bc)$

$= a \oplus (b + c - bc) = a \oplus (b \oplus c)$

**3. Existence of Identity :** $e \in$ G

$e \oplus a = a \Rightarrow e + a - ea = a \Rightarrow e(1 - a) = 0 \Rightarrow e = 0 \ (\because a \neq 1)$

$\therefore$ Identity exists and $e = 0$ is the identity.

**4. Existence of Inverse :** $b \in$ G

$a \oplus b = e \Rightarrow a+b-ab = 0 \Rightarrow b(1-a) = -a \Rightarrow b = \dfrac{a}{a-1} \ (\because a \neq 1)$

Also $b \oplus a = e \Rightarrow b+a-ba = 0 \Rightarrow b = \dfrac{a}{a-1} \ (\because a \neq 1)$

$\therefore$ $a \oplus b = 0 = b \oplus a \Rightarrow$ Inverse of $a$ exists and it is $\dfrac{a}{a-1}$ .

**5. Commutativity :** Also $a \oplus b = a+b-ab = b+a-ba = b \oplus a$

Hence $(G, \oplus)$ is an abelian group.

Hence $4 \oplus 5 \oplus x = 7 \Rightarrow (4 \oplus 5) \oplus x = 7 \Rightarrow (4+5-4\times5) \oplus x = 7$

$\Rightarrow -11 \oplus x = 7 \Rightarrow -11 + x + 11x = 7 \Rightarrow x = 3/2$ .

**Theorem 7.** *Let* $\mathbf{G}$ *be a group. For* $a, b \in \mathbf{G}, (ab)^{-1} = b^{-1}a^{-1}$. *(A.N.U.03, S.K.U.05,11)*

**Proof.** $\mathbf{G}$ is a group. Let $e$ be the identity in $\mathbf{G}$.

$\therefore \quad a, b \in \mathbf{G} \Rightarrow ab \in \mathbf{G}, a^{-1} \in \mathbf{G}, b^{-1} \in \mathbf{G} \Rightarrow ab \in \mathbf{G}, b^{-1}a^{-1} \in \mathbf{G}$

Now $(ab)(b^{-1}a^{-1}) = a[b(b^{-1}a^{-1})] = a[(bb^{-1})a^{-1}] = a[ea^{-1}] = aa^{-1} = e$.

Also $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)] = b^{-1}[(a^{-1}a)b] = b^{-1}[eb] = b^{-1}b = e$.

$\therefore \quad (ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$. $\therefore \quad (ab)^{-1} = b^{-1}a^{-1}$.

**Note 1.** $(b^{-1}a^{-1})^{-1} = ab$. **2.** $(abc)^{-1} = [(ab)c]^{-1} = c^{-1}(ab)^{-1} = c^{-1}b^{-1}a^{-1}$

**3.** $(\mathbf{G}, +)$ is a group, then $-(a+b) = (-b) + (-a)$.

**4.** $-(a+b+c) = -c - (a+b) = -c - b - a$.

**Theorem 8.** *Cancellation laws hold in a group.*
*Let* $\mathbf{G}$ *be a group. Then for* $a, b, c \in \mathbf{G}$, $ab = ac \Rightarrow b = c$ *(Left cancellation law) and* $ba = ca \Rightarrow b = c$ *(Right cancellation law)*

**Proof.** $\mathbf{G}$ is a group. Let $e$ be the identity in $\mathbf{G}$.

For $a, b, c \in \mathbf{G}, ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec \Rightarrow b = c$.

Similarly $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1} \Rightarrow b(aa^{-1}) = c(aa^{-1}) \Rightarrow be = ce \Rightarrow b = c$.

**Note 1.** If $\mathbf{G}$ is an additive group $a + b = a + c \Rightarrow b = c$ and $b + a = c + a \Rightarrow b = c$

**2.** In a semi group cancellation laws may not hold. Let $\mathbf{S}$ be the set of all $2 \times 2$ matrices over integers and let matrix multiplication be the binary operation defined on $\mathbf{S}$. Then $\mathbf{S}$ is a semi group of the above operation.

If $\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

then $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbf{S}$ and $\mathbf{AB} = \mathbf{AC}$. We observe that $\mathbf{B} \neq \mathbf{C}$ asserting that left cancellation law is not true in the semi group.

**3.** $(\mathbf{N}, +)$ is a semi group.

For $a, b, c \in \mathbf{N}$, $a + b = a + c \Rightarrow b = c$ and $b + a = c + a \Rightarrow b = c$

But $(\mathbf{N}, +)$ is not a group.

$\therefore$ In a semi group even if cancellation law holds the semi-group is not a group.

**Theorem 9.** *In a group* $\mathbf{G}\,(\neq \phi)$, *for* $a, b, x, y \in \mathbf{G}$, *the equation* $ax = b$ *and* $ya = b$ *have unique solutions.*

**Proof .** $\mathbf{G}$ is a group. $a \in \mathbf{G}, b \in \mathbf{G} \Rightarrow a^{-1} \in \mathbf{G}, b \in \mathbf{G} \Rightarrow a^{-1}b \in \mathbf{G}$.

Let $e$ be the identity element of $\mathbf{G}$.

$\therefore \quad ax = b \Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow (a^{-1}a)x = a^{-1}b \Rightarrow ex = a^{-1}b \Rightarrow x = a^{-1}b$

But if $x = a^{-1}b$ then $ax = a(a^{-1}b) = (aa^{-1})b = eb = b$

$\therefore \quad x = a^{-1}b$ is a solution of the equation $ax = b$.

If possible, let $x_1, x_2$ be two solutions of the equation $ax = b$.

$\therefore$ $ax_1 = b$ and $ax_2 = b$

$\therefore$ $ax_1 = ax_2 \Rightarrow x_1 = x_2$ (Left cancellation law)

$\therefore$ Solution of the equation $ax = b$ is unique and it is $a^{-1}b$.

Similarly if $y = ba^{-1}$ then $ya = (ba^{-1})\,a = b\,(a^{-1}a) = be = b$.

$\therefore$ $y = ba^{-1}$ is a solution of the equation $ya = b$.

If possible, let $y_1, y_2$ be two solutions of the equation $ya = b$.

$\therefore$ $y_1a = b$ and $y_2a = b$

$\therefore$ $y_1a = y_2a \Rightarrow y_1 = y_2$ (Right cancellation law)

$\therefore$ Solution of the equation $ya = b$ is unique and it is $ba^{-1}$.

**Note.** If $(\mathbf{G}, +)$ is a group, then the equation $a + x = b$ and $y + a = b$ have unique solutions.

**Commutator of the ordered pair $(a, b)$ where $(\mathbf{G}, .)$ a group.**

**Definition.** Let $(\mathbf{G}, .)$ be a group and $a, b \in \mathbf{G}$. The element $ab\,a^{-1}b^{-1}$ is called the **commutator** of the ordered pair $(a, b)$ in group $\mathbf{G}$.

**Ex.** If the commutator of every two elements of the group $(\mathbf{G}, .)$ is the identity element of $\mathbf{G}$, then $\mathbf{G}$ is abelian.

For $a, b \in \mathbf{G}$ and $ab\,a^{-1}b^{-1} = e \Rightarrow ab\,a^{-1}b^{-1}b = eb$.

$\Rightarrow aba^{-1} = b \Rightarrow ab\,a^{-1}a = ba \Rightarrow abe = ba \Rightarrow ab = ba \Rightarrow \mathbf{G}$ is abelian.

**Theorem 10.** *$\mathbf{G}$ is a non-empty set. If . is a binary operation in $\mathbf{G}$ such that the following three conditions are satisfied, then $(\mathbf{G}, .)$ is a group.*

(i) $a, b, c \in \mathbf{G} \Rightarrow (ab)\,c = a\,(bc)$ (ii) $a \in \mathbf{G}, \exists\, e \in \mathbf{G}$ *such that* $ea = a$ *and*

(iii) $a \in \mathbf{G}, \exists\, a^{-1} \in \mathbf{G}$ *such that* $a^{-1}a = e$.

**Proof. Part 1.** First we shall prove the left cancellation law in $\mathbf{G}$.

$e$ is left identity and $a^{-1}$ is left inverse of $a$ in $\mathbf{G}$.

For $a, b, c \in \mathbf{G}$, $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)\,b = (a^{-1}a)\,c \Rightarrow eb = ec \quad \Rightarrow b = c$

**Part 2.** Now we prove that $ae = a$.

$a \in \mathbf{G} \Rightarrow a^{-1} \in \mathbf{G}$ such that $a^{-1}a = e$.

$\therefore$ $a^{-1}(ae) = (a^{-1}a)\,e = ee = e = a^{-1}a$

$\therefore$ $a^{-1}(ae) = a^{-1}a \Rightarrow ae = a$

$\therefore$ $e$ is also right identity.

$\therefore$ $ea = ae = a\ \forall\ a \in \mathbf{G}$.

**Part 3.** Further we prove that $aa^{-1} = e$.

$a \in \mathbf{G} \Rightarrow a^{-1} \in \mathbf{G}$ such that $a^{-1}a = e$.

$\therefore$ $a^{-1}(aa^{-1}) = (a^{-1}a)\,a^{-1} = ea^{-1} = a^{-1} = a^{-1}e$.

$\therefore$ $a^{-1}(aa^{-1}) = a^{-1}e \Rightarrow aa^{-1} = e$.

$\therefore$ $a^{-1}$ is also right inverse of $a$ in $\mathbf{G}$.

$\therefore$ $a^{-1}a = aa^{-1} = e \Rightarrow$ every element in $\mathbf{G}$ has inverse.

$\therefore$ All the conditions of a group are satisfied and hence $\mathbf{G}$ is a group.

Thus : We can say that a semi - group $(\mathbf{G}, .)$ in which left axioms are satisfied is a group.

**Note 1. Theorem.** ***The left identity in a group is also the right identity if conditions*** (i), (ii), (iii) ***are satisfied in*** $(\mathbf{G}, .)$.

Proof of the theorem follows from parts 1 and 2 of the above theorem.

**2. Theorem.** ***The left inverse of an element in a group is also its right inverse if conditions*** (i), (ii), (iii) ***are satisfied in*** $(\mathbf{G}, .)$.

Proof of the theorem follows from parts 1, 2 and 3 of the above theorem.

**3.** We can also prove that $\mathbf{G}$ is a group w.r.t. binary operation even if conditions

(i) $a, b, c \in \mathbf{G} \Rightarrow (ab)\,c = a\,(bc)$, (ii) for $a \in \mathbf{G}, \exists\, e \in \mathbf{G}$ such that $ae = a$ and

(iii) for $a \in \mathbf{G}, \exists\, a^{-1} \in \mathbf{G}$ such that $aa^{-1} = e$ are given.

**4.** The above theorem can be stated as follows :

If a semi-group G statisfies the following conditions

(i) For $a \in$ G, $\exists e \in$ G such that $ea = a$ and

(ii) $a \in$ G, $\exists a^{-1} \in$ G such that $a^{-1}a = e$ then G is a group. ***(K.U.0.98, O.U.A. 01, S.K.U.0 03)***

**5.** $\mathbf{G}$ is a semi group. If $\exists\, e \in \mathbf{G}$ such that $ae = a, \forall a \in \mathbf{G}$ and $\exists\, a' \in \mathbf{G}$ such that $aa' = e, \forall a \in \mathbf{G}$, then $\mathbf{G}$ is a group.

**6.** However, we cannot prove that $\mathbf{G}$ is a group if closure, associativity, existence of left (right) identity and existence of right (left) inverse are given to be true.

**Theorem 11.** $(\mathbf{G} \neq \phi, \bullet)$ ***is an algebraic structure. Then*** $(\mathbf{G}, .)$ ***is a group iff*** (i) $a, b, c \in \mathbf{G} \Rightarrow (ab)\,c = a\,(bc)$ (ii) $ax = b$, $ya = b$ ***have unique solutions in*** $\mathbf{G}$ ***for every*** $a, b \in \mathbf{G}$.

**Proof. Necessary conditions.**

Given that $\mathbf{G}$ is a group we prove the condition (i) and (ii). Since $\mathbf{G}$ is a group (i) is true and (ii) is also true (vide theorem 9 and write the proof).

**Sufficient conditions.**

Given that the condition (i) and (ii) are true, we prove that $\mathbf{G}$ is a group.

Closure in $\mathbf{G}$ is true since $(\mathbf{G}, .)$ is an algebraic structure. Associativity in $\mathbf{G}$ is true by condition (i).

**Existence of left identity :** The equation $ya = b$ has a unique solution in $\mathbf{G}$ for $a, b \in \mathbf{G}$.

$\therefore$ If $a \in \mathbf{G}$, then taking $b = a$,

we see that there exists an element $e \in \mathbf{G}$ such that $e \cdot a = a$ .... (1)

Let $b \in \mathbf{G}$. Now $ax = b \Rightarrow e\,(ax) = eb.$ .... (2)

Also $e\,(ax) = (ea)\,x = ax$ (using (1)) $= b$ .... (3)

$\therefore$ From (2), (3), we have $eb = b$ for any element $b$ in $\mathbf{G}$. $\therefore$ $e$ is the left identity in $\mathbf{G}$.

**Existence of left inverse :** $a \in \mathbf{G}$. Since $e \in \mathbf{G}$, the equation $ya = e$ must have a unique solution in $\mathbf{G}$. Let it be $c$. $\therefore$ $ca = e$ which implies that the left inverse of $a$ is $c$.

$\therefore$ Left inverse exists for every element in $\mathbf{G}$.

$\therefore$ $\mathbf{G}$ is a group if (i) and (ii) are true.

**Note.** A semi-group $(\mathbf{G}, .)$ is a group if the equation $ax = b, ya = b$ have unique solutions in $\mathbf{G}$ for $a, b \in \mathbf{G}$. (This is Theorem 11 only)

Thus we have : **Another definition of a group.**

$(\mathbf{G}, \cdot)$ is an algebraic structure. If . is associative in $\mathbf{G}$ and the equations $ax = b, ya = b$ have unique solutions in $\mathbf{G}$ for every $a, b \in \mathbf{G}$ then $\mathbf{G}$ is a group.

In other words a semi-group $(\mathbf{G}, \cdot)$ is a group if the equations $ax = b, ya = b$ have unique solutions in $\mathbf{G}$ for every $a, b \in \mathbf{G}$.

***Theorem 12. A finite semi-group*** $(\mathbf{G}, .)$ ***satisfying the cancellation laws is a group.***

**OR**

***A finite set*** $\mathbf{G}$ ***with a binary composition is a group if*** . ***is associative and the cancellation laws hold in*** $\mathbf{G}$.

**Proof.** Let $\mathbf{G} = \{a_1, a_2, \ldots a_n\}$ be a set with $n$ distinct elements and $(\mathbf{G}, .)$ be a semi-group satisfying the cancellation laws.

Let $a \in \mathbf{G}$. Since . is a binary operation in $\mathbf{G}$, each of the products $aa_1, aa_2, \ldots aa_n$ are $n$ elements of $\mathbf{G}$.

For $i \neq j, aa_i = aa_j \Rightarrow a_i = a_j$ (by left cancellation law) which is a contradiction.

$\therefore$ All the $n$ products $aa_1, aa_2, \ldots aa_n$ are $n$ distinct elements of $\mathbf{G}$, of course in some order.

Now let $b \in \mathbf{G}$.

$\therefore \exists$ unique $a_i \in \mathbf{G}$ such that $aa_i = b$ i.e. the equation $ax = b$ has a unique solution in $\mathbf{G}$.

Again considering the products $a_1a, a_2a, \ldots a_na$ and proceeding as above we conclude that the equation $ya = b$ has a unique solution.

$\therefore$ By the definition of a group (Th. 11), $(\mathbf{G}, .)$ is a group.

**Note.** Consider the set $\mathbf{N}$ under +, we know that $\mathbf{N}$ is a semi - group under + in which cancellation laws hold. But $(\mathbf{N}, +)$ is not a group.

In view of this fact, the above theorem cannot be proved for infinite semi-group.

**Theorem 13.** ***In the composition table for a finite group any element of the group occurs in one and only one place in a row (or in a column).***

**Proof.** Let $(\mathbf{G}, .)$ be a finite group. Let $\mathbf{G} = \{a_1, a_2, \ldots a_n\}$. Prepare a table with $(n + 1)$ rows and $(n + 1)$ columns. Take . in the pivot's place. Fill the other squares in the first row successively by $a_1, a_2, \ldots a_n$ and the other square in the first column successively by $a_1, a_2, \ldots a_n$. Then we will be left with $n \times n$ blank squares. Take $a_1$ (2nd element in the first column) and write the equation $a_1x = a_k$ ($\because$ $\mathbf{G}$ is closed under .) where $k = 1, 2, \ldots n$ in $\mathbf{G}$. If $a_1$ and $a_k$ are fixed, then $x$ is unique since the equation has a unique solution in $\mathbf{G}$. Suppose $x = a_i (1 \leq i \leq n)$. Write $a_k$ as the product of $a_1$ and $a_i$ in the $i^{th}$ square of the $1^{st}$ row. Thus all the $n$ squares of the $1^{st}$ row (in $n \times n$ blank squares) are filled in. Now it is

clear that no element of **G** can be repeated in $n$ squares of the first row (of the $n \times n$ blank square).

Similarly all other remaining squares in the $2^{nd}$, $3^{rd}$, … rows can be filled.

We can also fill the $n \times n$ blank squares using the equation $ya = b$.

Hence no element occurs in the composition table of a finite group more than once in any row (or column)

**Ex. 7.** *Show that the sets of all ordered pairs* $(a, b)$ *of real numbers for which* $a \neq 0$ *w.r.t. the operations* $\times$ *defined by* $(a, b) \times (c, d) = (ac, bc + d)$ *is a group. Is the group commutative?*

**Sol. Closure :** $(a, b), (c, d) \in \mathbf{S} \Rightarrow (ac, bc + d) \in \mathbf{S}$ since $a \neq 0, c \neq 0 \Rightarrow ac \neq 0$.

**Associativity :** $(a, b), (c, d), (f, g) \in \mathbf{S} \Rightarrow \{(a, b) \times (c, d)\} \times (f, g) \in \mathbf{S}$

$$= (ac, bc + d) \times (f, g)$$

$$= (acf, \overline{bc + d} f + g) = (acf, bcf + df + g)$$

$$= (a, b) \times (cf, df + g) = (a, b) \times \{(c, d) \times (f, g)\}$$

**Existence of left identity :**

Let $(a, b) \in \mathbf{S}$. Let $(x, y) \in \mathbf{S}$ such that $(x, y) \times (a, b) = (a, b)$

$\therefore$ $(xa, ya + b) = (a, b) \Rightarrow xa = a, ya + b = b$

$\Rightarrow x = 1 \quad (\because a \neq 0)$ and $ya = 0$.

$\Rightarrow x = 1$ and $y = 0 \quad (\because a \neq 0)$.

$(1, 0) \in \mathbf{S}$ such that $(1, 0) \times (a, b) = (a, b)$.

$\therefore$ Left identity in **S** exists and it is $(1, 0)$.

**Existence of left inverse.** Let $(a, b) \in \mathbf{S}$. Let $(x, y) \in \mathbf{S}$ such that $(x, y) \times (a, b) = (1, 0)$.

$\therefore$ $(xa, ya + b) = (1, 0) \Rightarrow xa = 1, ya + b = 0$

$\Rightarrow x = \left(\frac{1}{a}\right), y = -\frac{b}{a} \quad (\because a \neq 0)$

$\therefore$ Left inverse of $(a, b)$ exists and it is $\left(\frac{1}{a}, -\frac{b}{a}\right)$

**Commutativity :** Let $(a, b), (c, d) \in \mathbf{S}$.

$\therefore$ $(a,b) \times (c,d) = (ac, bc + d)$ and $(c, d) \times (a, b) = (ca, da + b)$

Clearly $(a, b) \times (c, d) \neq (c, d) \times (a, b)$

$\therefore$ **S** is a group but not a commutative group w.r.t. $\times$.

**Ex. 8.** *Prove that the set of* $n^{th}$ *roots of unity under multiplication form a finite group.*

**Sol.** $1^{1/n} = (\cos\theta + i \sin\theta)^{1/n}$

$$= \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}, k = 0, 1, 2, \ldots n - 1.$$

$$= e^{2k\pi i/n} \text{ by Euler's theorem.}$$

Let $G = \{e^{2k\pi i/n}, k = 0, 1, 2, \ldots n-1\}$ and complex multiplication "."be the operation on **G**.

(i) **Closure :** Let $a, b \in \mathbf{G}$ then $a^n = 1$ and $b^n = 1$.

$\therefore \quad (ab)^n = a^n b^n = 1.1 = 1 \Rightarrow a, b \in \mathbf{G}$.

(ii) **Associativity :** Since the elements of $\mathbf{G}$ are complex numbers '.' is associative in $\mathbf{G}$.

(iii) **Existence of right identity :**

We know that $1 = e^{2\pi i/n \,.\, 0} \in \mathrm{G}$. If $a \in \mathbf{G}$ then $a.1 = a$.

Right identity element exists in $\mathbf{G}$ and is equal to 1.

(iv) **Existence of right inverse :**

Let $e^{(2r\pi i/n)} \in \mathbf{G}$. Then $0 \le r \le n-1$ *i.e.* either $r = 0$ or $0 < r \le n-1$.

$\therefore\ e^{(2\pi.0/n)\,i} \in \mathbf{G}$ or $e^{2\pi(n-r)\,i/n} \in \mathbf{G}$ when $0 < r \le n-1$.

Now $e^{2\pi.0/n} . e^{2\pi.0/n} = 1$ or $e^{2r\pi i/n} . e^{2\pi(n-r)i/n} = e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$

when $0 < r \le n-1$.

$\therefore$ The right inverse of $e^{2\pi.0i/n}$ is $e^{2\pi.0i/n} (= 1)$ and

the right inverse of $e^{2r\pi i/n}$ is $e^{2\pi(n-r)i/n}$ when $0 < r \le n-1$.

Thus every element of $\mathbf{G}$ is invertible.

(v) **Commutativity :**

Since the elements of $\mathbf{G}$ are complex numbers, . is commutative in $\mathbf{G}$.

$\therefore$ $\mathbf{G}$ is a finite abelian group under multiplication.

**Ex. 9.** *Show that the fourth roots of unity form an abelian group w.r.t. multiplication.*

**Sol.** Fourth roots of unity are $1, -1, i, -i$.

Let $\mathbf{G} = \{1, -1, i, -i\}$. The composition table for multiplication is

| $\cdot$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

We can observe (i) Closure (ii) Associativity (iii) Existence of identity (identity element = 1) (iv) Existence of inverse (v) commutativity to be true.

$$(1)^{-1} = 1, (-1)^{-1} = -1, (i)^{-1} = -i, (-i)^{-1} = i\,.$$

$\therefore$ $(\mathbf{G}, .)$ is an abelian group (of order 4).

**Ex. 10.** *If every element of a group* $(\mathbf{G}, .)$ *is its own inverse, show that* $(\mathbf{G}, .)$ *is an abelian group.*

**Sol.** Let $a, b \in \mathbf{G}$. By hypothesis $a^{-1} = a, b^{-1} = b$.

Then $ab \in \mathbf{G}$ and hence $(ab)^{-1} = ab$.

Now $(ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab \Rightarrow ba = ab \Rightarrow (\mathbf{G}, .)$ is an abelian group.

**Ex. 11.** All groups of order 4 and less are commutative.

**Sol. Group of order 1.**

Let $(\mathbf{G}, .)$ be a group such that $\mathbf{O}(\mathbf{G}) = 1$.

Then $\mathbf{G} = \{e\}$ where $e$ is the identity element.

Now $e.e = e$. $\therefore$ $\mathbf{G}$ is commutative.

**Group of order 2.**

Let $(\mathbf{G}, .)$ be a group such that $\mathbf{O}(\mathbf{G}) = 2$.

Let $\mathbf{G} = \{e, a\}$ where $e$ is the identity element.

Then $e.e = e, e.a = a.e = a$ and $a.a = e$.

$\therefore$ The composition table is :

| . | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

Clearly $\mathbf{G}$ is abelian.

**Group of order 3.**

Let $(\mathbf{G}, .)$ be a group such that $\mathbf{O}(\mathbf{G}) = 3$

Let $\mathbf{G} = \{e, a, b\}$ where $e$ is the identity element.

We have (i) $e.e = e, e.a = a$ and $e.b = b$

(ii) $ae = a, ab = e$

($\because$ $ab = b \Rightarrow ab = eb \Rightarrow a = e$ which is absurd) and $aa = b$.

(iii) $be = b, ba = e$

($\because$ $ba = a \Rightarrow ba = ea \Rightarrow b = e$ which is absurd) and $bb = a$.

$\therefore$ The composition table is :

| • | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

Clearly $\mathbf{G}$ is abelian.

**Group of order 4.**

Let $(\mathbf{G}, .)$ be a group such that $\mathbf{O}(\mathbf{G}) = 4$.

Let $\mathbf{G} = \{e, a, b, c\}$ where $e$ is the identity element.

Since $e = e^{-1}$ if $a = a^{-1}$ two causes arise.

**I.** $b = c^{-1}$ and $c = b^{-1}$ **II.** $b = b^{-1}$ and $c = c^{-1}$

**Case I. We have** :

(i) $ee = e, ea = a, eb = b$ and $ec = c$.

(ii) $ae = a, aa = e, ab = c$

[$\because$ $ab = b \Rightarrow ab = eb \Rightarrow a = e$ which is absurd].

(iii) $be = b, bc = e, ba = c$

[$\because$ $ba = a \Rightarrow ba = ea \Rightarrow b = e$ which is absurd].

(iv) $ce = c, cb = e, ca = b$

[$\because$ $ca = a \Rightarrow ca = ea \Rightarrow c = e$ which is absurd].

$\therefore$ The composition table in this case is :

| • | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $a$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $a$ |

**Case II. We have** :

(i) $ee = e, ea = a, eb = b$ , $ec = c$ .

(ii) $ae = a, aa = e$

[$\because$ $ab = b \Rightarrow ab = eb \Rightarrow a = e$ which is absurd] $ab = c, ac = b$ .

(iii) $be = b, bb = e, ba = c$

[$\because$ $ba = a \Rightarrow ba = ea \Rightarrow b = e$ which is absurd] and $bc = a$ .

(iv) $ce = c, cc = e, cb = a$

[$\because$ $cb = b \Rightarrow cb = eb \Rightarrow c = e$ which is absurd] and $ca = b$ .

| . | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

$\therefore$ The composition table in this case is :

Clearly $\mathbf{G}$ is commutative in either case.

**Note.** The algebraic structure shown in case II is called Klein-4-group. In this group $\forall\, a \in \mathbf{G}$, we have $aa = e$ i.e. $a^2 = e$ by defining $aa = a^2$.

**Ex. 12.** $\mathbf{A}$ *is any non-empty set.* $\mathbf{S}$ *is the set of all bijections (one-one and onto mappings) from* $\mathbf{A}$ *to* $\mathbf{A}$ *. Then show that* $\mathbf{S}$ *is a group w.r.t. composition of mappings as binary operation.*

**Sol.** Let $\mathbf{S}$ be the set of all bijections from $\mathbf{A}$ to $\mathbf{A}$. Let $g, f \in \mathbf{S}$ .

By the definition of composition of mappings, for $x \in \mathbf{A}, (gf)(x) = g(f(x))$ .

**Closure.** Let $g, f \in \mathbf{S}$ are bijections on $\mathbf{A}$ .

Let $a, b \in \mathrm{A}. (gf)(a) = (gf)(b) \Rightarrow g(f(a)) = g(f(b))$

$\Rightarrow f(a) = f(b)$ ($\because$ $g$ is $1-1$) $\Rightarrow a = b$ ($\because$ $f$ is $1-1$) $\Rightarrow gf$ is $1-1$

Since $g$ is onto on $\mathbf{A}, \exists\, b \in \mathbf{A}$ such that $g(b) = c$ for $c \in \mathbf{A}$ .

Since $f$ is onto on $\mathbf{A}, \exists\, a \in \mathbf{A}$ such that $f(a) = b$ for $b \in \mathbf{A}$ .

$\therefore$ $g(b) = c \Rightarrow g(f(a)) = c \Rightarrow (gf)(a) = c \Rightarrow gf$ is onto.

$\therefore$ $gf$ is a bijection defined over $\mathbf{A}$ and hence $gf \in \mathrm{S}$ .

$\therefore$ . follows closure law in $\mathbf{S}$ .

**Associativity.** $h, g, f \in \mathbf{S} \Rightarrow h(gf) = (hg)f$

Since for $x \in \mathrm{A}, (h(gf))(x) = h[(gf)(x)] = h[g(f(x))]$

$= (hg)[f(x)] = [(hg)f](x) \Rightarrow h(gf) = (hg)f$ .

**Existence of identity.** Let $e$ be the identity mapping from $\mathbf{A}$ to $\mathbf{A}$ .

$\therefore$ For $x \in \mathbf{A}, e(x) = x$ . Also $e$ is a bijection $\therefore$ $e \in \mathbf{S}$ .

$\therefore$ $f \in \mathbf{S} \Rightarrow ef = fe = f$ since

$(ef)(x) = e(f(x)) = f(x) \Rightarrow ef = f$ and $(fe)(x) = f(e(x)) = f(x) \Rightarrow fe = f$

$\therefore$ Identity element in $\mathbf{S}$ exists and it is $e$ .

**Existence of Inverse.** Let $f \in \mathbf{S}$ . $\therefore$ $f : \mathbf{A} \to \mathbf{A}$ is a bijection.

$\therefore$ $f^{-1} : \mathbf{A} \to \mathbf{A}$ is a bijection . $\therefore$ $f^{-1} \in \mathbf{S}$ .

Now for $x \in \mathbf{A}, (f^{-1}f)(x) = f^{-1}(f(x)) = x = e(x) \Rightarrow f^{-1}f = e$

and $(ff^{-1})(x) = f[f^{-1}(x)] = x = e(x) \Rightarrow ff^{-1} = e$ . $\therefore$ $f^{-1}f = ff^{-1} = e$

$\therefore$ Every element of $\mathbf{S}$ is invertible and $f^{-1}$ is the inverse of $f$.

$\therefore$ $\mathbf{S}$ is a group w.r.t. the composition of mappings as the binary operation.

**Commutativity.** If $\mathbf{A}$ has only one element then $\mathbf{S}$ has only one element and every group of order 1 is abelian. If $\mathbf{A}$ has only two elements, then $\mathbf{S}$ has only two elements and every group of order 2 is abelian. But if $\mathbf{A}$ has more than 2 elements then we shall show that $\mathbf{S}$ is non-abelian.

Let $\mathbf{A} = \{a, b, c\}$. Define $f : \mathbf{A} \to \mathbf{A}$ such that

$f(a) = b, f(b) = c$ and $f(c) = a$ and $g : \mathbf{A} \to \mathbf{A}$ such that

$g(a) = b, g(b) = a; g(c) = c$. Clearly $f$ and $g$ are bijections in $\mathbf{A}$.

$\therefore$ $f, g \in \mathbf{S}$.

Now $(gf)(a) = g(f(a)) = g(b) = a$ and $(fg)(a) = f[g(a)] = f(b) = c$

$\therefore$ $(gf)(a) \neq (fg)(a)$ i.e. $gf \neq fg$.

In this case $\mathbf{S}$ consists of six elements and $\mathbf{S}$ is a non-abelian group.

**Ex. 13.** *Show that the set of six transformations* $f_1, f_2, f_3, f_4, f_5, f_6$ *on the set* $\mathbf{A} = \mathbf{C} - \{0, 1\}$ *defined by*

$$f_1(\mathbf{Z}) = \mathbf{Z},\ f_2(\mathbf{Z}) = \frac{1}{\mathbf{Z}},\ f_3(\mathbf{Z}) = 1 - \mathbf{Z},\ f_4(\mathbf{Z}) = \frac{\mathbf{Z}}{\mathbf{Z}-1},\ f_5(\mathbf{Z}) = \frac{1}{1-\mathbf{Z}},\ f_6(\mathbf{Z}) = \frac{\mathbf{Z}-1}{\mathbf{Z}}$$

*forms a finite non-abelian group of order six w.r.t. composition of functions as the composition.*

**Sol.** If $f : \mathbf{A} \to \mathbf{A}$ then $f$ is a transformation on $\mathbf{A} = \mathbf{C} - \{0, 1\}$

Let $\mathbf{G} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$. Each $f_i$ is a transformation since $f_i : \mathbf{A} \to \mathbf{A}$.

Since $\forall\, \mathbf{Z} \in \mathbf{A}, f_1(\mathbf{Z}) = \mathbf{Z}$, $f_1$ is the identity function.

$\therefore$ $f_1 f_1 = f_1, f_1 f_2 = f_2 = f_2 f_1, f_1 f_3 = f_3 f_1$ etc.

Now : $(f_2 f_2)(\mathbf{Z}) = f_2[f_2(\mathbf{Z})] = f_2\left(\frac{1}{\mathbf{Z}}\right) = \left(\frac{1}{1/\mathbf{Z}}\right) = \mathbf{Z} = f_1(\mathbf{Z}) \Rightarrow f_2 f_2 = f_1$.

$(f_2 f_3)(\mathbf{Z}) = f_2[f_3(\mathbf{Z})] = f_2(1 - \mathbf{Z}) = \frac{1}{1-\mathbf{Z}} = f_5(\mathbf{Z}) \Rightarrow f_2 f_3 = f_5$.

$(f_2 f_4)(\mathbf{Z}) = f_2[f_4(\mathbf{Z})] = f_2\left(\frac{\mathbf{Z}}{\mathbf{Z}-1}\right) = \frac{1}{\mathbf{Z}/(\mathbf{Z}-1)} = \frac{\mathbf{Z}-1}{\mathbf{Z}} = f_6(\mathbf{Z}) \Rightarrow f_2 f_4 = f_6$.

$(f_2 f_5)(\mathbf{Z}) = f_2[f_5(\mathbf{Z})] = f_2\left(\frac{1}{\mathbf{Z}-1}\right) = 1 - \mathbf{Z} = f_3(\mathbf{Z}) \Rightarrow f_2 f_5 = f_3$.

$(f_2 f_6)(\mathbf{Z}) = f_2[f_6(\mathbf{Z})] = f_2\left(\frac{\mathbf{Z}-1}{\mathbf{Z}}\right) = f_4(\mathbf{Z}) \Rightarrow f_2 f_6 = f_4$ etc.

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_5$ | $f_6$ | $f_3$ | $f_4$ |
| $f_3$ | $f_3$ | $f_6$ | $f_1$ | $f_5$ | $f_4$ | $f_2$ |
| $f_4$ | $f_4$ | $f_5$ | $f_6$ | $f_1$ | $f_2$ | $f_3$ |
| $f_5$ | $f_5$ | $f_4$ | $f_2$ | $f_3$ | $f_6$ | $f_1$ |
| $f_6$ | $f_6$ | $f_3$ | $f_4$ | $f_2$ | $f_1$ | $f_5$ |

Clearly $\mathbf{G}$ is a group w.r.t. the composition of mappings as composition.

But it is non-abelian since $f_3 f_4 = f_5$ and $f_4 f_3 = f_6$.

**Ex. 14.** *Real quaternion group. Let* $\mathbf{T} = \{a_0 + a_1 i + a_2 j + a_3 k / a_0, a_1, a_2, a_3 \in \mathbf{R}\}$ *where* $i, j, k$ *are such that* $i^2 = j^2 = k^2 = -1$.

$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$ *and* $ijk = -1$.

*Also* $a_0 + a_1 i + a_2 j + a_3 k = b_0 + b_1 i + b_2 j + b_3 k \Leftrightarrow a_0 = b_0, a_1 = b_1, a_2 = b_2, a_3 = b_3$

*Define an operation* $\oplus : \mathbf{T} \times \mathbf{T} \to \mathbf{T}$ *as follows :*

$$(a_0 + a_1 i + a_2 j + a_3 k) \oplus (b_0 + b_1 i + b_2 j + b_3 k)$$
$$= (a_0 + b_0) + (a_1 + b_1) i + (a_2 + b_2) j + (a_3 + b_3) k$$

*Show that* $(\mathbf{T}, \oplus)$ *is an abelian group.*

**Sol.** Clearly the operation $\oplus$ is well defined.

Let $x = a_0 + a_1 i + a_2 j + a_3 k,\ y = b_0 + b_1 i + b_2 j + b_3 k$

$z = c_0 + c_1 i + c_2 j + c_3 k$.

**Closure.** $x, y \in \mathbf{T} \Rightarrow x \oplus y \in \mathbf{T}$

since $a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3 \in \mathbf{R}$ etc.

**Associativity.** $x, y, z \in \mathbf{T} \Rightarrow (x \oplus y) \oplus z = x \oplus (y \oplus z)$

since $(a_0 + b_0) + c_0 = a_0 + (b_0 + c_0)$ etc.

**Commutativity.** $x, y \in \mathbf{T} \Rightarrow x \oplus y = y \oplus x$.

**Existence of identity.** $e = 0 + 0i + 0j + 0k \in \mathbf{T}$ is the identiry element.

**Existence of inverse.** Let $x \in \mathbf{T}$. Then $-x \in \mathbf{T}$ such that $x + (-x) = (-x) + x = e$.

$\therefore$ $(\mathbf{T}, \oplus)$ is an abelian group.

## EXERCISE 2 ( *a* )

**1.** Prove that the set $\mathbf{Q}_0$ of all non-zero rational numbers forms a group under usual multiplication.

**2.** $\mathbf{G} = \{x / x$ is a rational number and $0 < x \leq 1\}$. Show that $(\mathbf{G}, .)$ is not a group. ($.$ is usual multiplication).

**3.** Prove that the set $\mathbf{C}$ of all complex numbers forms an abelian group w.r.t. ordinary addition.

[**Hint.** Let $a, b, c \in \mathbf{C}$. Take $a = p_1 + iq_1, b = p_2 + iq_2, c = p_3 + iq_3$

where $p_1, q_1, p_2, q_2, p_3, q_3 \in \mathbf{R}$ ]

**4.** Prove the set $\mathbf{C}_0$ of all non-zero complex numbers forms an infinite abelian group w.r.t. multiplication.

**5.** Show that the set $G = mz = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$ is an abelian group w.r.t. usual addition, $m$ being a fixed integer.

[**Hint.** Let $a, b, c \in \mathbf{G}$. Take $a = pm, b = qm, c = rm$ where $p, q, r \in \mathbf{Z}$ ]

**6.** Show that the set $\mathbf{G} = \{\ldots, 2^{-3}, 2^{-2}, 1, 0, 2, 2^2, 2^3, \ldots\}$ is an abelian group under usual multiplication.

[**Hint.** Let $a, b, c \in \mathbf{G}$. Take $a = 2^p, b = 2^q, c = 2^r$ where $p, q, r \in \mathbf{Z}$ ]

**7.** (a) Prove that the set of integers $\mathbf{Z}$ is an abelian group for the operation $\oplus$ defined by $a \oplus b = a + b + 1 \; \forall \quad a, b \in \mathbf{Z}$.

[**Hint.** $e \in \mathbf{Z}$. $e \oplus a = a \Rightarrow e + a + 1 = a \Rightarrow e = -1$

$b \in \mathbf{Z}$. $a \oplus b = e \Rightarrow a + b + 1 = -1 \Rightarrow b = -a - 2$ ]

(b) Prove that the set $\mathbf{Z}$ of all integers forms an abelian group w.r.t. the operation defined by $a * b = a + b + 2$, for all $a, b \in \mathbf{Z}$.

**8.** Prove that the set $\mathbf{G} = \{a + b\sqrt{2} \,/\, a, b \in \mathbf{Q}\}$ is a commutative group w.r.t. addition.

[**Hint.** Let $x, y, z \in \mathbf{G}$. Take $x = a + b\sqrt{2}, y = c + d\sqrt{2}, z = p + q\sqrt{2}$ .

Identity element = 0. Inverse of $x$ is $-x$ ]

**9.** Show that the set of all positive rational numbers forms an abelian group under the composition $o$ defined by

(i) $aob = (ab)/2$ ***(K. U. 10, O. U. 12)*** (ii) $aob = (ab)/4$

**10.** Prove that the set $\mathbf{C} = \{z = x + iy \,/\, x, y \in \mathbf{R}$ and $|z| = 1\}$ forms an infinite abelian group under multiplication.

[**Hint.** $z_1, z_2 \in \mathbf{C}$. Then $|z_1| = 1, |z_2| = 1, |z_1|\,|z_2| = 1$

Multiplication of complex numbers is associative.

Identity element $= 1 + 0i = 1$. $|z|\,|\frac{1}{z}| = 1$ since $|\frac{1}{z}| = \frac{1}{|z|} = 1$].

**11.** $(\mathbf{G}, *)$ is an arbitrary group. Define a new binary operation $o$ on the set G by the formula $aob = b * a$. Prove that $(\mathbf{G}, o)$ is also a group.

[**Note.** $(\mathbf{G}, o)$ is called the **opposite group** of $(\mathbf{G}, *)$ ]

**12.** Show that the set $\mathbf{R}$ of real numbers other that $-1$ is an abelian group w.r.t. the operation $\oplus$ defined by $a \oplus b = a + b + ab$. Show that the solution of the equation $2 \oplus x \oplus 3 = 7$ in $\mathbf{R} - \{-1\}$ is $-1/3$.

**13.** Prove that the set $\mathbf{G}$ of $2 \times 2$ non singular matrices whose elements are real numbers is a non-abelian group w.r.t. matrix multiplication.

**14.** Prove that the set of all $m \times n$ matrices whose elements are numbers (integers, real or complex) form an infinite abelian group w.r.t. matrix addition.

**15.** Prove that the set of all $n \times n$ non-singular matrices having their elements as rational (real or complex) numbers is an infinite non-abelian group w.r.t. matrix multiplication.

**16.** In a group $\mathbf{G}$ (*i*) if $b^{-1}a^{-1}ba = e$ ($e$ is the identity in $\mathbf{G}$) $\forall\ a, b \in \mathbf{G}$, prove that $\mathbf{G}$ is abelian. (*ii*) let $a, b \in \mathbf{G}$. Show that $(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow ab = ba$.

**Ex. 15.** *Show that the set* $\mathbf{P}_3$ *of all bijections on three symbols* $a, b, c$ *(some take them as 1, 2, 3) is a finite non-abelian group of order 6 w.r.t. composition of mappings.* )

**Sol.** Let $\mathbf{S} = \{a, b, c\}$ and let $\mathbf{P}_3$ be the set $= \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where $f_i (i = 1 \text{ to } 6)$ is a bijection over $\mathbf{S}$.

Let $f_1 = \{(a,a),(b,b),(c,c)\}, f_2 = \{(a,b),(b,a),(c,c)\}$
$f_3 = \{(a,a),(b,c),(c,b)\}, f_4 = \{(a,c),(b,b),(c,a)\}$
$f_5 = \{(a,b),(b,c),(c,a)\}, f_6 = \{(a,c),(b,a),(c,b)\}$

Let $o$ be the composition of mappings in $\mathbf{P}_3$.

Let $g, f \in \mathbf{P}_3$.

Then $gof \Rightarrow$ perform first $f$ and then perform $g$.

The composition table for $\mathbf{P}_3$ is given below.

$f_2 of_3 = \{(a,b),(b,a),(c,c)\}\ o\ \{(a,a),(b,c),(c,b)\}$
$= \{(a,b),(b,c),(c,a)\} = f_5$

$f_5 of_4 = \{(a,b),(b,c),(c,a)\} o \{(a,c),(b,b),(c,a)\}$
$= \{(a,a),(b,c),(c,b)\} = f_3$

and so on.

| 0 | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_5$ | $f_6$ | $f_3$ | $f_4$ |
| $f_3$ | $f_3$ | $f_6$ | $f_1$ | $f_5$ | $f_4$ | $f_2$ |
| $f_4$ | $f_4$ | $f_5$ | $f_6$ | $f_1$ | $f_2$ | $f_3$ |
| $f_5$ | $f_5$ | $f_4$ | $f_2$ | $f_2$ | $f_6$ | $f_1$ |
| $f_6$ | $f_6$ | $f_3$ | $f_4$ | $f_2$ | $f_1$ | $f_5$ |

Since all the products in the table are elements of $\mathbf{P}_3$, closure is true. Composition of mappings is associative. Identity element is $f_1$.

Also $f_1^{-1} = f_1, f_2^{-1} = f_2, f_3^{-1} = f_3, f_4^{-1} = f_4, f_5^{-1} = f_6, f_6^{-1} = f_5$.

The composition is not commutative since $f_3 of_5 \neq f_5 of_3$.

$\therefore$ $\mathbf{P}_3$ is a finite non-abelian group of order 6.

**Note.** If $\mathbf{A}_3 = \{f_1, f_5, f_6\}$, the composition table w.r.t. the composition of mappings as composition is :

Clearly $\mathbf{A}_3$ **is a commutative group on** $\mathbf{S}$.

Identity is $f_1 . f_5^{-1} = f_6, f_6^{-1} = f_5$.

Similarly $\mathbf{H} = \{f_1, f_2\}$ **is an abelian group** w.r.t. composition of mappings.

| 0 | $f_1$ | $f_5$ | $f_6$ |
|---|---|---|---|
| $f_1$ | $f_1$ | $f_5$ | $f_6$ |
| $f_5$ | $f_5$ | $f_6$ | $f_1$ |
| $f_6$ | $f_6$ | $f_1$ | $f_5$ |

**Ex. 16.** *The symmetries of an equilateral triangle.*

Let **ABC** be an equilateral triangle with medians $p, q, r$ and centroid **O**.

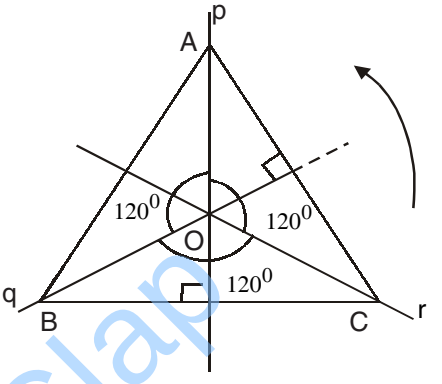
$\therefore \quad \angle \mathbf{AOB} = \mathbf{BOC} = \angle \mathbf{COA} = 120°$

We form by rotations and reflections the following 6 distinct symmetries.

(1) Anti clock-wise rotations about **O** in its plane through $0°, 120°, 240°$ are represented respectively by

$$r_0 = \{(\mathbf{A}, \mathbf{A}), (\mathbf{B}, \mathbf{B}), (\mathbf{C}, \mathbf{C})\}$$
$$r_1 = \{(\mathbf{A}, \mathbf{B}), (\mathbf{B}, \mathbf{C}), (\mathbf{C}, \mathbf{A})\}$$
and $$r_2 = \{(\mathbf{A}, \mathbf{C}), (\mathbf{B}, \mathbf{A}), (\mathbf{C}, \mathbf{B})\}$$

Clearly $r_0, r_1, r_2$ are bijections over the set of vertices $\{\mathbf{A}, \mathbf{B}, \mathbf{C}\}$.

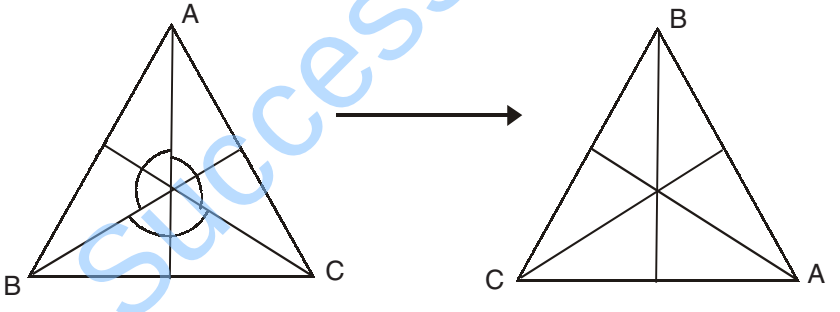



(2) Reflections in the medians $p, q, r$ are represented by

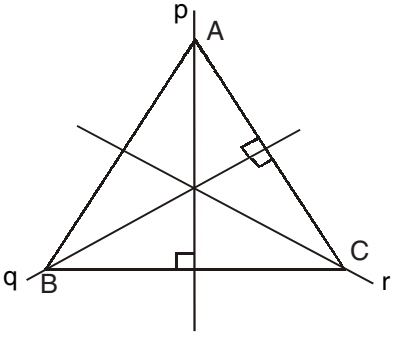
$$f_1 = \{(\mathbf{A}, \mathbf{A}), (\mathbf{B}, \mathbf{C}), (\mathbf{C}, \mathbf{B})\}$$
$$f_2 = \{(\mathbf{A}, \mathbf{C}), (\mathbf{B}, \mathbf{B}), (\mathbf{C}, \mathbf{A})\}$$
and $$f_3 = \{(\mathbf{A}, \mathbf{B}), (\mathbf{B}, \mathbf{A}), (\mathbf{C}, \mathbf{C})\}$$

Clearly $f_1, f_2, f_3$ are bijections over the set of vertices $\{\mathbf{A}, \mathbf{B}, \mathbf{C}\}$. We shall explain the above motions by taking one rotation from (1) and one reflection from (2).

Consider $r_2 = \{(\mathbf{A}, \mathbf{C}), (\mathbf{B}, \mathbf{A}), (\mathbf{C}, \mathbf{B})\}$.




Consider $f_2 = \{(\mathbf{A}, \mathbf{C}), (\mathbf{B}, \mathbf{B}), (\mathbf{C}, \mathbf{A})\}$. $f_2$ is the position obtained by the reflection in the median $q$. Imagine $q$ as a mirror. Then reflection of **A** in $q$ is **C** and the reflection of **C** in $q$ is **A**. Also reflection of **B** in $q$ is **B**.



We denote the set of these bijections by $\mathbf{G} = \{r_0, r_1, r_2, f_1, f_2, f_3\}$.

Let $o$ is be the binary operation (composition of mappings) on $\mathbf{G}$ such that for $a, b \in \mathbf{G}$.

$aob$ = perform first $b$ and then perform $a$ and the resulting position of the vertices is the result.

$\therefore$ We have the following composition table.

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | $r_0$ | $r_1$ | $r_2$ | $f_1$ | $f_2$ | $f_3$ |
| $r_0$ | $r_0$ | $r_1$ | $r_2$ | $f_1$ | $f_2$ | $f_3$ |
| $r_1$ | $r_1$ | $r_2$ | $r_0$ | $f_3$ | $f_1$ | $f_2$ |
| $r_2$ | $r_2$ | $r_0$ | $r_1$ | $f_2$ | $f_3$ | $f_1$ |
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $r_0$ | $r_1$ | $r_2$ |
| $f_2$ | $f_2$ | $f_3$ | $f_1$ | $r_2$ | $r_0$ | $r_1$ |
| $f_3$ | $f_3$ | $f_1$ | $f_2$ | $r_1$ | $r_2$ | $r_0$ |

Clearly $\mathbf{G}$ is a group with identity $r_0$.

Also $r_0^{-1} = r_0, r_1^{-1} = r_2, r_2^{-1} = r_1, f_1^{-1} = f_1, f_2^{-1} = f_2, f_3^{-1} = f_3$

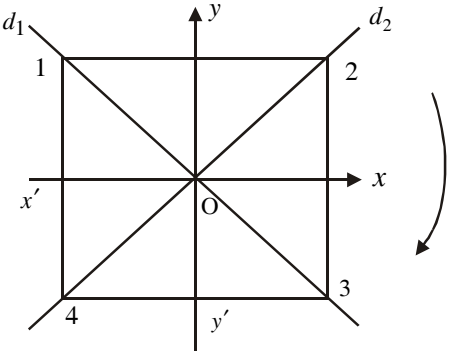
Further $r_1 o f_2 = f_1$ and $f_2 o r_1 = f_3$ i.e. $r_1 o f_2 \neq f_2 o r_1$.

$\therefore$ $\mathbf{G}$ is not an abelian group w.r.t. $o$.

**Ex. 17.** *Dihedral groups - symmetries of a square.*

Consider a square (say, a card board square) on a rectangular Cartesian plane of two dimensions with its centre at the origin. (So that the square may move freely).

Let the vertices of the square be numbered as 1, 2, 3, 4 as shown in the figure.




If the following one or more rotational motions are applied on the square, it remains in its original place. The motion of the square is identified by its final position which is indicated by the numbered vertices. Further two motions of the square are said to be equal if they leave the square in the same final position.

Rotational motions of the square are symbolised as follows :

1. Clockwise rotation about -- in its plane through $90° \ldots r_{90}$.
2. " " " " " " $180° \ldots r_{180}$.
3. " " " " " " $270° \ldots r_{270}$.
4. " " " " " " $360° \ldots r_{360}$.
5. Reflexion in the x – axis (inspace) i.e. flips out of the plane about x – axis and back into the plane $\Big\} - x$

6. $\left.\begin{matrix} \ldots\ldots\ldots \text{ y – axis } \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots \text{ y – axis } \ldots\ldots\ldots\ldots \end{matrix}\right\} - y$

7. $\left.\begin{matrix} \ldots\ldots\ldots \text{ diagonal } d_1 \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots \text{ diagonal } d_1 \ldots\ldots\ldots\ldots \end{matrix}\right\} - d_1$

8. $\left.\begin{matrix} \ldots\ldots\ldots \text{ diagonal } d_2 \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots \text{ diagonal } d_2 \ldots\ldots\ldots\ldots \end{matrix}\right\} - d_2$

Clearly $r_{90}, r_{180}, \ldots\ldots, d_2$ are all bijections over the set of vertices {1, 2, 3, 4} and $r_{90} = \{(1,4),(2,1),(3,2),(4,3)\}, r_{180} = \{(1,3),(2,4),(3,1),(4,2)\} \ldots, d_2 = \{(1,3),(2,2),(3,1),(4,4)\}$.

Now we have the following composition table on $\mathbf{D}_4 = \{r_{90}, r_{180}, r_{270}, r_{360}, x, y, d_1, d_2\}$ w.r.t. the composition of mappings $o$.

If $g, f \in \mathbf{D}_4$, then $gof \Rightarrow$ perform the motion $f$ first and then perform motion $g$.

| $o$ | $r_{90}$ | $r_{180}$ | $r_{270}$ | $r_{360}$ | $x$ | $y$ | $d_1$ | $d_2$ |
|---|---|---|---|---|---|---|---|---|
| $r_{90}$ | $r_{180}$ | $r_{270}$ | $r_{360}$ | $r_{90}$ | $d_1$ | $d_2$ | $y$ | $x$ |
| $r_{180}$ | $r_{270}$ | $r_{360}$ | $r_{90}$ | $r_{180}$ | $y$ | $x$ | $d_2$ | $d_1$ |
| $r_{270}$ | $r_{360}$ | $r_{90}$ | $r_{180}$ | $r_{270}$ | $d_2$ | $d_1$ | $x$ | $y$ |
| $r_{360}$ | $r_{90}$ | $r_{180}$ | $r_{270}$ | $r_{360}$ | $x$ | $y$ | $d_1$ | $d_2$ |
| $x$ | $d_2$ | $y$ | $d_1$ | $x$ | $r_{360}$ | $r_{180}$ | $r_{270}$ | $r_{90}$ |
| $y$ | $d_1$ | $x$ | $d_2$ | $y$ | $r_{180}$ | $r_{360}$ | $r_{90}$ | $r_{270}$ |
| $d_1$ | $x$ | $d_2$ | $y$ | $d_1$ | $r_{90}$ | $r_{270}$ | $r_{360}$ | $r_{180}$ |
| $d_2$ | $y$ | $d_1$ | $x$ | $d_2$ | $r_{270}$ | $r_{90}$ | $r_{180}$ | $r_{360}$ |

Clearly $\mathbf{D}_4$ is a group with identity $r_{360}$.

Also each of $r_{180}, r_{360}, x, y, d_1, d_2$ is its own inverse and $(r_{90})^{-1} = r_{270}, (r_{270})^{-1} = r_{90}$.

Since $r_{270} o x = d_2$ and $x o r_{270} = d_1$.

$r_{270} o x \neq x o r_{270}$

$\mathbf{D}_4$ is not an abelian group.

**Note.** $(\mathbf{D}_4, o)$ is a dihedral group which is an octic group. It is an example for a finite non-abelian group.

**Ex. 18.** *Consider three mutually rectangular coordinate axes ($\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ axes) in space. The set of rotations of a line about the x-axis in the anticlockwise direction through angles $0°, 90°, 180°, 270°$ in the $\mathbf{XY}$ planes. We denote the rotations through angles $0°, 90°, 180°, 270°$ respectively by $r_0, r_1, r_2, r_3$. Let $\mathbf{G} = \{r_0, r_1, r_2, r_3\}$. Clearly $r_0, r_1, r_2, r_3$ are all bijections over the set of positions of the line in the $\mathbf{XY}$ plane.*

Let $o$ is be the binary composition (composition of mappings) defined on $\mathbf{G}$.

Now we have the following composition table :

| 0 | $r_0$ | $r_1$ | $r_2$ | $r_3$ |
|---|---|---|---|---|
| $r_0$ | $r_0$ | $r_1$ | $r_2$ | $r_3$ |
| $r_1$ | $r_1$ | $r_2$ | $r_3$ | $r_0$ |
| $r_2$ | $r_2$ | $r_3$ | $r_0$ | $r_1$ |
| $r_3$ | $r_3$ | $r_0$ | $r_1$ | $r_2$ |

Clearly **G** is a finite commutative group with identity $r_0$.

Also $r_0^{-1} = r_0, r_1^{-1} = r_3, r_2^{-1} = r_2, r_3^{-1} = r_1$.

**Ex. 19.** *In a group* (**G**, .) *for* $a \in \mathbf{G}$, *is idempotent* $\Leftrightarrow a = e$. ***(A.U. M12)***

**Sol.** (**G**, .) is a group. Let $a \in \mathbf{G}$, $a$ is idempotent.

$\Leftrightarrow a \,.\, a = a \Leftrightarrow a \,.\, a = ae \Leftrightarrow a = e$.

**Note.** If $a$ is an element in a group (**G**, .) such that $a \,.\, a = a$, then $a$ is called an **idempotent element**.

**Ex. 20.** *If* $a, b$ *are any two elements of a group* (**G**, .) *which commute show that* (i) $a^{-1}$ *and* $b$ *commute,* (ii) $b^{-1}$ *and* $a$ *commute and* (iii) $a^{-1}$ *and* $b^{-1}$ *commute.*

**Sol.** (**G**, .) is a group and such that $ab = ba$.

(i) $ab = ba \Rightarrow a^{-1}(ab) = a^{-1}(ba)$

$\Rightarrow (a^{-1}a)\, b = a^{-1}(ba) \Rightarrow eb = (a^{-1}b)\, a \Rightarrow b = (a^{-1}b)\, a$

$\Rightarrow ba^{-1} = [(a^{-1}b)\, a]\, a^{-1} = (a^{-1}b)\,(aa^{-1}) = (a^{-1}b)\, e = a^{-1}b$

$\Rightarrow$ $a^{-1}$ and $b$ commute.

Similarly (ii) can be proved.

(iii) $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1} \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}$

$\Rightarrow$ $a^{-1}$ and $b^{-1}$ commute.

## 2.10. ADDITION MODULO $m$

**Definition.** Let $a, b \in \mathbf{Z}$ and $m$ be a fixed positive integer. If $r$ is the remainder $(0 \le r < m)$ when $a + b$ (ordinary sum of $a, b$) is divided by $m$, we define $'a +_m b' = r$ and we read $'a +_m b'$ as a 'addition modulo $m$' $b$.

**e.g. 1.** $20 +_6 5 = 1$ since $20 + 5 = 4(6)+1$ i.e. 1 is the remainder when 20 + 5 is divided by 6.

**e.g. 2.** $24 +_5 4 = 3$.

**e.g. 3.** $2 +_7 3 = 5$.

**e.g. 4.** $-32 +_4 5 = 1$ since $-32 + 5 = (-7)(4) + 1$.

**e.g. 5.** $(-9) +_2 (-18) = 1$ since $-9 - 18 = (-14)(2) + 1$.

**e.g. 6.** $0 +_5 (-3) = 2$ since $0 +_5 (-3) = 0 - 3 = (-1)5 + 2$.

**Note.** $a +_m b = b +_m a$.

## 2.11. CONGRUENCES

**Definition.** Let $a, b \in \mathbf{Z}$ and $m$ be any fixed positive integer. If $a - b$ is divisible by $m$ we say that $a$ is congruent to $b$ modulo $m$ and we write it as $a \equiv b \pmod m$. This relation between integers $a$ and $b$ is called congruence modulo $m$.

Thus : $a \equiv b \pmod m \Leftrightarrow m/(a - b)$ or $m/(b - a)$ or $a - b = qm$ for $q \in \mathbf{Z}$ and

$a \not\equiv b \pmod m \Leftrightarrow m$ does not divide $(a - b)$ or $a - b \ne km$ for $k \in \mathbf{Z}$.

**Note 1.** If $a \equiv b \pmod m$, then we get the same remainder if $a$ and $b$ are separately divided by $m$.

**e.g. 1.** If $22 \equiv 13 \pmod 3$, then 1 is the remainder when 22 and 13 are separately divided by 3.

**e.g. 2.** If $-7 \equiv 17 \pmod 6$ then 5 is the remainder when $-7$ and 17 are separately divided by 6.

**2.** Since $a + b \equiv r \pmod m$, we have $a +_m b = a + b \pmod m$.

**e.g.** $12 +_4 7 = 12 + 7 \pmod 4$

Since $12 +_4 7 = 3$ and $3 \equiv 19 \pmod 4$.

**3.** If $a \equiv b \pmod m$, then $a +_m c = b +_m c$.

For : $a \equiv b \pmod m \Rightarrow m/(a-b) \Rightarrow m/(a+c)-(b+c)$

$\Rightarrow a + c \equiv b + c \pmod m$ for $c \in \mathbf{Z}$.

$\Rightarrow a +_m c = b +_m c$.

**2.12.** The operation congruence modulo '$m$' is an equivalence relation, in the set of integers. So the operation 'congruence modulo $m$' partitions $\mathbf{Z}$ into disjoint equivalence classes called residue classes modulo $m$ or congruence classes modulo $m$.

If $a \in \mathbf{Z}$ then the residue class of $a$ is $\bar{a}$ or $|\bar{a}|$ or $|a|$ where $a = \{x | \in \mathbf{Z}$ and $x - a$ is divisible by $m\}$.

Similarly if $b \in \mathbf{Z}$ then $\bar{b} = \{x | \ x \in Z$ and $x - b$ is divisible by $m\}$.

Clearly $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod m$ or $m/(a-b)$.

**Definition.** $\mathbf{Z}_m = \{0, 1, 2, 3, \ldots (m-1)\}$ is called the complete set of least positive residues modulo $m$ or simply set of residues modulo $m$.

**Definition.** Let $m \in \mathbf{N}$ and $r \in \mathbf{Z}$.

Let $\bar{r} = \{x | \ x \in \mathbf{Z}, x \equiv r \pmod m\}$. Then the set $\overline{\mathbf{Z}_m} = \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{m-1}\}$ is called the complete set of least positive residue classes modulo $m$ or simply set of residue classes modulo $m$.

Here $\bar{r} = \{\ldots, -2m + r, -m + r, r, m + r, 2m + r, \ldots\}$.

**e.g.** If $m = 6$, the set of least positive residues modulo $m = \{0, 1, 2, 3, 4, 5\}$ and the set of residue classes modulo $m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ where

$\bar{0} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}, \bar{1} = \{\ldots, -11, -5, 1, 7, 13, \ldots\},$

$\bar{2} = \{\ldots, -10, -4, 2, 8, 14, \ldots\}, \bar{3} = \{\ldots, -9, -3, 3, 9, 15, \ldots\},$

$\bar{4} = \{\ldots, -8, -2, 4, 10, 16, \ldots\}, \bar{5} = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$.

We observe that $\bar{a} = \overline{a + m} = \overline{a + 2m} = \ldots$

Thus for the above example, $\bar{0} = \bar{6} = \overline{12} = \ldots$,

$\bar{1} = \bar{7} = \overline{13} = \ldots, \bar{2} = \bar{8} = \overline{14} = \ldots$, etc.

Also $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ are all disjoint.

**Note 1.** The elements $\bar{0}, \bar{1}, \bar{2}, \ldots \overline{m-1}$ of $\overline{\mathbf{Z}_m}$ are distinct.

**2.** It $a \in \mathbf{Z}$ and if $r$ is the remainder when $a$ is divided by $m$, then $\bar{a} = \bar{r}$.

For : By division algorithm, $a = qm + r, q \in \mathbf{Z}$ and $r$ is the remainder such that $o \le r \le m - 1$.

$\therefore a - r = qm \Rightarrow a - r$ is divisible by $m$.

$\Rightarrow a \equiv r \pmod m \Rightarrow \bar{a} = \bar{r}$

**3.** The residue class $\bar{0}$ is called the zero residue class. We have $\bar{a} = \bar{o} \Leftrightarrow m/a$.

**Addition of residue classes**

**Definition.** For $a, b \in \overline{\mathbf{Z}_m}$ we define addition of residue classes, denoted by +, as $\bar{a} + \bar{b} = \overline{a + b}$.

**Note 1.** + on the R.H.S. is ordinary addition.

**2.** If $r$ is the remainder $(o \le r < m)$ when $a+b$ is divided by $m$, then $\overline{a+b} = \bar{r}$ *i.e.* $\bar{a} + \bar{b} = \bar{r}$.

## 2. 13. ADDITION GROUP OF INTEGERS MODULO $m$

**Theorem 14.** *The set* $\mathbf{G} = \{0, 1, 2, \ldots (m-1)\}$ *of first* $m$ *non-negative integers is an abelian group w.r.t. the operation addition modulo* $m$.

**Proof.** If $a, b \in \mathbf{Z}$ and $m$ is a +ve integer, then $a +_m b = r$ where $r$ is the remainder when $a+b$ is divided by $m$.

Clearly $0 \le r \le m-1$.

**Closure.** $a, b \in \mathbf{G} \Rightarrow a +_m b \in \mathbf{G}$.

Since $a +_m b = r, 0 \le r \le m-1$.

**Associativity.** $a, b, c \in \mathbf{G} \Rightarrow a +_m (b +_m c) = (a +_m b) +_m c$ since

$a +_m (b +_m c) = a +_m (b + c) \pmod m$ $[\because b +_m c \equiv (b + c) \pmod m$

= remainder when $a + (b + c)$ is divided by $m$.

= remainder when $(a + b) + c$ is divided by $m$.

$= (a+b) +_m c = (a +_m b) +_m c$.

**Existence of identity.** Let $a \in \mathbf{G}, \exists\, 0 \in \mathbf{G}$ such that $0 +_m a = a +_m 0$.

$\therefore$ 0 is the identity element in $\mathbf{G}$.

**Existence of inverse.** Since $0 +_m 0 = 0$, the inverse of 0 is 0 itself.

If $r (\ne 0) \in \mathbf{G}$, then $m - r \in \mathbf{G}$.

$\therefore$ $(m-r) +_m r$ = remainder when $(m - r + r)$ is divisible by $m = 0$

$= r +_m (m - r)$

$\therefore$ $m - r$ is the inverse of $r$.

$\therefore$ Every element in $\mathbf{G}$ is invertible.

**Commutativity.** $a, b \in \mathbf{G} \Rightarrow a +_m b = b +_m a$.

Since $a +_m b$ = remainder when $a + b$ is divided by $m$.

= remainder when $b + a$ is divided by $m$.

$= b +_m a$.

$\therefore$ $(\mathbf{G}, +_m)$ is an abelian group $\mathbf{O}(\mathbf{G}) = m$.

**Note. 1.** Here we denote $\mathbf{G}$ by $\mathbf{Z}_m$. **2.** $(\mathbf{G} - \{0\}, +_m)$ is not a group.

**Ex. 21.** *Prove that the set* $\mathbf{G} = \{0, 1, 2, 3, 4\}$ *is an abelian group of order 5 w.r.t. addition modulo* 5.

**Sol.** The composition table for $\mathbf{G}$ w.r.t. $+_5$ is given :

| $+_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

Now we can prove all the axioms of an abelian group.

$\therefore$ $(\mathbf{G}, +_5)$ is a finite abelian group of order 5.

**Additive group of residue classes modulo $m$**

***Theorem 15. The set of residue classes modulo $m$ is an abelian group of order $m$ w.r.t. addition of residue classes.***

**OR**

***$(\overline{\mathbf{Z}_m}, \oplus)$ is an abelian group.***

**Proof.** The set of residue classes modulo $m =$

$$\overline{\mathbf{Z}_m} = \{\bar{0},\ \bar{1},\ \bar{2},\ \ldots,\ \overline{m-1}\} = \{\bar{r} \mid 0 \le r \le m-1\}.$$

Addition of residue classes $\bar{a}$ and $\bar{b}$ denoted by +, is defined as follows :

For $a, b \in \overline{\mathbf{Z}_m} \Rightarrow \bar{a} + \bar{b} = \overline{a+b}$. The operation + is well defined.

For this we have to show that if $\bar{a} = \bar{c}$ and $\bar{b} = \bar{d}$ in $\overline{\mathbf{Z}_m}$ then $\bar{a} + \bar{b} = \bar{c} + \bar{d}$.

We have $\bar{a} = \bar{c} \Rightarrow m \mid (a-c)$ and $\bar{b} = \bar{d} \Rightarrow m \mid (b-d)$.

Now $m \mid (a-c)$ and $m \mid (b-d) \Rightarrow m \mid \{a-c+b-d\}$

$\Rightarrow m \mid \{(a+b)-(c+d)\} \Rightarrow a+b \equiv c+d \pmod m$

$\Rightarrow \overline{a+b} = \overline{c+d} \Rightarrow \bar{a} + \bar{b} = \bar{c} + \bar{d}$ $\quad\therefore$ + is well defined.

**Closure.** $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_m} \Rightarrow \bar{a} + \bar{b} \in \overline{\mathbf{Z}_m}$.

Since $\bar{a} + \bar{b} = \overline{a+b} = \bar{r}, 0 \le r \le m-1$ where $r$ is the remainder when $a+b$ is divided by $m$.

**Associativity.** $\bar{a}, \bar{b}, \bar{c} \in \overline{\mathbf{Z}_m}$. $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$, since $(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c}$

$= \overline{(a+b)+c} \quad = \overline{a+(b+c)} \quad = \bar{a} + (\bar{b} + \bar{c})$

**Commutativity.** $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_m} \Rightarrow \bar{a} + \bar{b} = \bar{b} + \bar{a}$ since $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$.

**Existence of identity.** Let $\bar{a} \in \overline{\mathbf{Z}_m}$. $\exists\ \bar{0} \in \overline{\mathbf{Z}_m}$ such that

$$\bar{0} + \bar{a} = \overline{0+a} = \bar{a} = \overline{a+0} = \bar{a} + \bar{0}.$$

$\therefore$ Identity in $\overline{\mathbf{Z}_m}$ exists and it is $\bar{0}$.

**Existence of inverse.** $\bar{0} + \bar{0} = \bar{0} \Rightarrow \bar{0}$ is the inverse of $\bar{0}$.

If $\bar{r} \in \overline{\mathbf{Z}_m}$ such that $1 \le r \le m-1$, then $\overline{m-r} \in \overline{\mathbf{Z}_m}$.

Further $\overline{m-r} + \bar{r} = \overline{m-r+r} = \bar{m} = \bar{0}$ and $\bar{r} + \overline{m-r} = \overline{r+m-r} = \bar{m} = \bar{0}$

$\therefore$ $\overline{m-r} + \bar{r} = \bar{r} + \overline{m-r} = \bar{0}$

$\therefore$ $\overline{m-r}$ is the inverse of $\bar{r}$ for $1 \le r \le m-1$.

$\therefore$ Every element in $\overline{\mathbf{Z}_m}$ is invertible.

$\therefore$ $(\overline{\mathbf{Z}_m}, +)$ is an abelian group of order $m$.

## 2. 14. MULTIPLICATION MODULO $p$

**Definition.** If $a$ and $b$ are integers and $p$ is a fixed positive integer and if $ab$ (ordinary product of $a$ and $b$) is divided by $p$ such that $r$ is the remainder $(0 \le r < p)$, we define $a \times_p b = r$. We read $a \times_p b$ as $a$ "multiplication modulo $p$" $b$.

**e.g. 1.** $20 \times_6 5 = 4$ since $20 \times_5 = 100 = 16\ (6) + 4$ *i.e.* 4 is the remainder when $20 \times_5$ is divided by 6.

**e.g. 2.** $24 \times_5 4 = 1$ **e.g. 3.** $2 \times_7 3 = 6$

**e.g. 4.** $(-32)\times_4 5 = 0$ since $(-32)\times 5 = -160 = (-40)\,4 + 0$

**e.g. 5.** $(-28)\times_4 (-11) = 2$ since $(-28)\times(-11) = 308 = 102\,(3) + 2$

**e.g. 6.** $0\times_5 (-3) = 0$ since $0\times(-3) = 0 = 0\,(5) + 0$

**Note 1.** $a\times_p b \equiv ab \pmod p$

**e.g.** $7\times_5 3 \equiv 21 \pmod 5$ since $7\times_5 3 = 1$ and $1 - 21 = (-4)\,5$

**2.** If $a\times_m b = b\times_m a$. **e.g.** $3\times_7 6 = 6\times_7 3$

**3.** If $a \equiv b \pmod p$ then $a\times_p c = b\times_p c$

**e.g. 1.** If $3 \equiv 23 \pmod 5$ then $3\times_5 4 = 23\times_5 4$ since $3\times_5 4 = 2$ and $23\times_5 4 = 2$

**e.g. 2.** If $-4 \equiv -25 \pmod 7$ then $(-4)\times_7 5 = (-25)\times_7 5$

since $-4\times_7 5 = 1$ and $(-25)\times_7 5 = 1$

**Prime integer**

**Definition.** An integer $p$ is said to be a prime integer if $p \neq 0$, $p \neq \pm 1$ and the only divisors of $p$ are $\pm 1, \pm p$.

**e.g.** $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$ are prime integers.

**Note.** If $p$ is a prime integer and $a, b$ are two integers such that $p \mid ab$, then we have $p \mid a$ or $p \mid b$.

**Multiplication group of integers modulo $p$ where $p$ is prime.**

**Theorem 16.** ***The set of G of $(p-1)$ integers $1, 2, 3, \ldots, p-1, p$ being prime, form a finite abelian group of order $p-1$ w.r.t. multiplication modulo $p$.***

**Proof.** Let $\mathbf{G} = \{1, 2, 3, \ldots, (p-1)\}$, $p$ being prime and the operation $\times_p$ be the multiplication modulo $p$.

**Closure.** Let $a, b \in \mathbf{G}$. $\therefore$ $1 \le a \le (p-1)$ and $1 \le b \le (p-1)$.

Now $a\times_p b = r$ where $r$ is the remainder when the ordinary product is divided by $p$.

Since $p$ is prime, $ab$ is not divisible by $p$.

$\therefore$ $r$ cannot be zero and we shall have $1 \le r \le (p-1)$ *i.e.* $r \in \mathbf{G}$.

$\therefore$ $a, b \in \mathbf{G} \Rightarrow a\times_p b \in$ G.

**Associativity.** $a, b, c \in \mathbf{G} \Rightarrow (a\times_p b)\times_p c = a\times_p (b\times_p c)$

Since $(a\times_p b)\times_p c = (ab)\times_p c$ [$\because a\times_p b \equiv ab \pmod p$]

= remainder when $ab\,(c)$ is divided by $p$

= remainder when $a\,(bc)$ is divided by $p$.

$= a\times_p (bc)$ $= a\times_p (b\times_p c)$

**Existence of identity.** Let $a \in \mathbf{G}, \exists 1 \in \mathbf{G}$ such that $1\times_p a = a$.

$\therefore$ Left identity in $\mathbf{G}$ exists and it is 1.

**Existence of inverse.** Let $s \in \mathbf{G}$. $\therefore$ $1 \le s \le (p-1)$

Consider the following $(p-1)$ products :

$1\times_p s,\ 2\times_p s,\ 3\times_p s, \ldots (p-1)\times_p s$

All these are elements of $\mathbf{G}$ by closure law.

Also these elements are distinct for the following reasoning.

Let $i, j$ be two integers such that $1 \le i \le (p-1)$, $1 \le j \le (p-1)$ and $i > j$.

$\therefore$ $1 \le (i - j) < (p-1)$.

Now $i\times_p s = j\times_p s \Rightarrow is$ and $js$ leave the same remainder when each is divided by $p$.

$\Rightarrow is - js$ is divisible by $p$. $\Rightarrow (i-j)s$ is divisible by $p$.

$\Rightarrow p \mid (i-j)$ or $p \mid s$ which is absurd.

$\therefore\ i\times_p s \neq j\times_p s$ and hence all the elements $1\times_p s,\ 2\times_p s,\ 3\times_p s,\ldots,\ (p-1)\times_p s$ are distinct.

$\therefore$ One of these elements must be 1. Let $s'\times_p s = 1$

$\therefore\ s'$ is the left inverse of $s$.

**Commutativity.** $a, b \in G \Rightarrow a\times_p b = b\times_p a$

Since $a\times_p b$ = remainder when $ab$ is divided by $p$.

= remainder when $ba$ is divided by $p$. $= b\times_p a$.

$\therefore\ (G, \times_p)$ is a finite abelian group of order $(p-1)$.

**Note 1.** In the above theorem if $p$ is not prime, then $p$ must be composite. Then $\exists$ two integers $a$ and $b$ such that $1 \le a \le (p-1), 1 \le b \le (p-1)$ and $ab = p$. (Suppose $p = 8$ and $a = 2, b = 4$. Then $1 \le a \le 7,\ 1 \le b \le 7$ and $ab = 8$).

$\therefore\ a\times_p b = 0$ and $0 \notin \mathbf{G}$ *i.e.* $\mathbf{G}$ is not closed w.r.t. $\times_p$.

Thus $\mathbf{G}$ is not a group for the operation $\times_p$.

**2.** Even if 0 is included as an element of $\mathbf{G}$, the inverse of 0 w.r.t. $\times_p$ does not exist. Thus $\mathbf{G}$ is not a group w.r.t. $\times_p$ even if 0 is included in $\mathbf{G}$.

**Ex. 22.** *Prove that the set* $\mathbf{G} = \{1, 2, 3, 4, 5, 6\}$ *is a finite abelian group of order 6 w.r.t.* $\times_7$.

**Sol.** The composition table is

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

Clearly $(\mathbf{G}, \times_7)$ is a finite abelian group of order 6.

## 2.15. MULTIPLICATIVE GROUP OF NON-ZERO RESIDUE CLASSES MODULO A PRIME INTEGER $p$.

**Theorem 17.** ***The set of non-zero residue classes modulo a prime integer*** $p$ ***forms an abelian group of order*** $(p-1)$ ***w.r.t. multiplication of residue classes.***

**Proof.** The set of non-zero residue classes modulo $p$.

$= \mathbf{Z}_p = \{\overline{1},\ \overline{2},\ \overline{3},\ldots,\ \overline{p-1}\}$ i.e. $\mathbf{Z}_p = \{\overline{r} / r \in Z$ and $1 \le r \le (p-1)\}$

Also no element of $\bar{r}$ is divisible by $p$.

Now we shall show that the elements of $\overline{\mathbf{Z}_p}$ are distinct.

Let $1 \le i \le (p-1), 1 \le j \le (p-1)$ and $i > j$.

Then $\bar{i} = \bar{j} \Rightarrow i \equiv j \pmod{p} \Rightarrow (i-j)$ is divisible by $p$ which is absurd since $i - j < p$.

Hence $i \ne j$ and all the elements of $\overline{\mathbf{Z}_p}$ are distinct.

Multiplication of residue classes $\bar{a}$ and $\bar{b}$, denoted by $\cdot$ is defined as follows :

For $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_p}, \bar{a} \cdot \bar{b} = \overline{ab}$.

The multiplicative operation is well defined.

For this we have to show that if $\bar{a} = \bar{c}$ and $\bar{b} = \bar{d}$ in $\overline{\mathbf{Z}_p}$ then $\overline{ab} = \overline{cd}$.

We have $\bar{a} = \bar{c} \Rightarrow p \mid (a-c)$ and $\bar{b} = \bar{d} \Rightarrow p \mid (b-d)$.

Now $p \mid (a-c) \Rightarrow p \mid b(a-c)$ and $p \mid (b-d) \Rightarrow p \mid c(b-d)$

$p \mid b(a-c) + c(b-d)$ i.e. $p \mid (ab - cd)$

i.e. $ab \equiv cd \pmod{p}$ i.e. $\overline{ab} = \overline{cd}$ i.e. $\bar{a}\bar{b} = \bar{c}\bar{d}$

$\therefore$ Multiplication of residue classes is well defined.

**Closure.** Let $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_p}$. $\therefore$ $p \mathbf{X} a$ and $p \mathbf{X} b$ *i.e.* $p \mathbf{X} ab$, since $p$ is prime.

By def. $\bar{a}\bar{b} = \overline{ab}$. Since $ab$ is not divisible by $p$.

$\overline{ab} = \bar{r}$ where $1 \le r \le (p-1)$ $\therefore$ $ab \in \overline{\mathbf{Z}_p}$.

$\therefore$ $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_p} \Rightarrow \overline{ab} \in \overline{\mathbf{Z}_p}$

**Associativity.** $a, b, c \in \overline{\mathbf{Z}_p} \Rightarrow (\bar{a}\bar{b})\,\bar{c} = \bar{a}(\bar{b}\bar{c})$ since

$(\bar{a}\bar{b})\,\bar{c} = \overline{(ab)}\,\bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a}\overline{(bc)} = \bar{a}(\bar{b}\bar{c})$

**Commutativity.** $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_p} \Rightarrow \bar{a}\bar{b} = \bar{b}\bar{a}$ since $\bar{a}\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\bar{a}$.

**Existence of identity.** $\bar{a} \in \overline{\mathbf{Z}_p}$, $\exists\ \bar{1} \in \overline{\mathbf{Z}_p}$ such that $\bar{1}\bar{a} = \overline{1a} = a = \overline{a1} = \bar{a}\bar{1}$.

$\therefore$ Identity element in $\overline{\mathbf{Z}_p}$ exists and it is $\bar{1}$.

**Existence of inverse.** Let $\bar{a} \in \overline{\mathbf{Z}_p}$.

$\therefore$ $a$ is any non-zero residue class. Then $p$ does not divide $a$.

Consider the products $1\bar{a}, 2\bar{a}, 3\bar{a}, \ldots, p-1\bar{a}$.

By closure law, all these products are elements of $\overline{\mathbf{Z}_p}$.

We claim that all these are distinct elements of $\overline{\mathbf{Z}_p}$ for the following reasoning.

Let $i$ and $j$ be two integers such that

$1 \le i \le (p-1), 1 \le j \le (p-1)$ and $\bar{i} > \bar{j}$.

Then $\bar{i}\bar{a} = \bar{j}\bar{a} \Rightarrow \overline{ia} = \overline{ja}$

$\Rightarrow$ $ia - ja$ is divisible by $p$ $\Rightarrow$ $(i-j)a$ divisible by $p$

$\Rightarrow$ $p \not| (i-j)$ or $p \not| a$ which is absurd since

$0 \le i - j < p - 1$ and $p$ doe not divide $a$.

Hence $\bar{i}\bar{a} = \bar{j}\bar{a}$, and the elements $1\bar{a}, 2\bar{a}, \ldots, p-1\bar{a}$ are the $(p-1)$ distinct elements of $\overline{\mathbf{Z}_p}$ in some order.

$\therefore$ One of these elements must be $\bar{1}$.

Let $\bar{b}\bar{a} = \bar{1} = \overline{ab}$. $\therefore$ $\bar{b}$ is the inverse of $\bar{a}$.

$\therefore$ Every element of $\overline{\mathbf{Z}_p}$ is invertible.

$\therefore$ $\overline{\mathbf{Z}_p}$ is a finite abelian group of order $(p-1)$ w.r.t. multiplication of residue classes.

**Theorem 18.** ***The set of non-zero residue classes modulo a composite positive integer $m$ is not a group w.r.t. multiplication of residue classes.***

**Proof.** Let $\overline{\mathbf{Z}_m}$ be the set of non-zero residue classes modulo a composite positive integer $m$.

Let $m = ab$ where $1 < a < m$ and $1 < b < m$.

$\therefore$ $m \mathbf{X} a \Rightarrow \bar{a} \neq \bar{0}$ and $m \mathbf{X} b \Rightarrow \bar{b} \neq \bar{0}$. $\therefore$ $\bar{a}, \bar{b} \in \overline{\mathbf{Z}_m}$.

Now $ab = m \Rightarrow \overline{ab} = \bar{m}$

$\Rightarrow \overline{ab} = \bar{0}$ since $\bar{m} = \bar{0}$ $\Rightarrow ab \notin \overline{\mathbf{Z}_m}$. $\therefore$ $a, b \in \overline{\mathbf{Z}_m} \Rightarrow \overline{ab} \notin \overline{\mathbf{Z}_m}$

Since $\overline{\mathbf{Z}_m}$ is not closed w.r.t. multiplication of residue classes, $\overline{\mathbf{Z}_m}$ is not a group w.r.t. multiplication or residue classes.

## EXERCISE 2 ( *b* )

**1.** Prove that $\{1, -1\}$ form an abelian group under multiplication.

**2.** Prove that $\{1, \omega, \omega^2\}$ where $\omega$, $\omega^2$ are the complex cube roots of unity form a commutative group under multiplication.

**3.** Show that $\mathbf{G} = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6\}$ form an abelian group w.r.t. the operation $a_i o a_j = a_{i+j}$ for $i + j < 7$ and $a_i o a_j = a_{i+j-7}$ for $i + j \geq 7$.

**4.** Show that the matrices $\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{C} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $\mathbf{D} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ form an abelian group under matrix multiplication.

**5.** Show that the functions $f_1, f_2$ on $\mathbf{R}$ into $\mathbf{R}$ given by $f_1(x) = x$, $f_2(x) = 1 - x$ for all $x \in \mathbf{R}$ from an abelian group w.r.t. the operation composition of mappings.

**6.** Show that the bijective transformations $f_1, f_2, f_3, f_4$ of $\mathbf{R} - \{0\}$ given by $f_1(x) = x$, $f_2(x) = 1/x$, $f_3(x) = -x$, $f_4(x) = -1/x$ w.r.t. the operation composition of mappings is an abelian group.

**7.** Prove that the set of all rational numbers of the form $\frac{q}{2^p}$ $(q, p \in \mathbf{Z})$ is not a group under multiplication.

**8.** Prove that the set $\mathbf{G} = \{m^p / m$ is a non-zero integer and $p \in \mathbf{Z}\}$ is a group under usual multiplication.

**9.** Prove that the set $\mathbf{Z}$ form an abelian group with operation defined by $a * b = a + b + 2 \; \forall \; a, b \in \mathbf{Z}$

**10.** Prove that the set of all numbers $\cos\theta + i \sin\theta$ where $\theta \in \mathbf{Q}$ will form an infinite multiplicative abelian group.

**11.** Prove that the set of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ where $a, b$ are real numbers not both equal to zero form a group w.r.t. matrix multiplication.

**12.** Show that the set of $2\times 2$ matrices $\left\{\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \Big/ x(\neq 0) \in \mathbf{R}\right\}$ is an abelian group under matrix multiplication

**13.** Prove that the set $\mathbf{G} = \{0, 1, 2, 3, 4, 5\}$ is an abelian group w.r.t. $+_6$.

**14.** Prove that the set $\mathbf{G} = \{1, 2, 3, 4\}$ is an abelian group of order 4 w.r.t. $\times_5$.

**15.** Show that the set of integers $\{1, 3, 5, 7\}$ form an abelian group w.r.t. $\times_8$.

**16.** Show that the set of integers $\{1, 5, 7, 11\}$ form an abelian group w.r.t. multiplication modulo 12.

**17.** Show that the set of residue classes modulo 5 form an abelian group w.r.t. the addition of residue classes.

**18.** Show that the non-zero residue classes multiplication modulo 5 form an abelian group w.r.t. multiplication of residue classes.

## 2.16. LAW OF INTEGRAL EXPONENTS

Laws of indices for real numbers are very well known, to the students. We shall now discuss certain definitions and laws analogous to the laws of indices using the group axioms.

**Definition.** Let $(\mathbf{G}, .)$ be a group. Let $a \in \mathbf{G}$. Then by closure law $a, aa, aaa, \ldots$ are all elements of $\mathbf{G}$. Since the composition in $\mathbf{G}$ obeys general associative law, $aaa, \ldots a$ ($n$ times) is independent of the manner in which the elements are grouped.

For every integer $n$, we define $a^n$ as follows :

(i) $a^0 = e, e$ is the identity element (ii) $a^1 = a$

(iii) For $n > 1, a^{n+1} = a^n a$ (iv) For $n > 0, a^{-n} = (a^{-1})^n$

**e.g.** $a^2 = a^1 a = aa, a^3 = a^2 a = (aa)a = aaa$, etc.

$$a^{-4} = (a^{-1})^4 = (a^{-1})^3 (a^{-1})^1 = [(a^{-1})^2 (a^{-1})^1] a^{-1}$$
$$= [(a^{-1})^1 (a^{-1})^1] a^{-1} a^{-1} = a^{-1} a^{-1} a^{-1} a^{-1}, \text{ etc.}$$

**Note 1.** $a^n = a.a.a \ldots\ldots a$ ($n$ times) and $a^n \in \mathbf{G}$.

**2.** $a^{-n} = (a^{-1})(a^{-1}) \ldots (a^{-1})$ ($n$ times) and $a^{-n} \in \mathbf{G}$.

**3.** If additive operation + is taken as the operation, then $a^n$ in multiplicative notation becomes $na$ in additive notation.

Identity element = 0 and inverse of $a$ is $-a$.

$$na = a + a \ldots\ldots + a \ (n \text{ times}) \text{ and}$$
$$-na = (-a) + (-a) + (-a) + \ldots\ldots + (-a) \ (n \text{ times}) \text{ when}$$

$n$ is a positive integer. Also $na, -na \in \mathbf{G}$.

**Theorem 19.** *Let $(\mathbf{G}, \cdot)$ be a group and $a \in \mathbf{G}$. If $n$ is any positive integer, then* (i) $a.a^n = a^n.a$ *and* (ii) $a^n, a^{-n}$ *are inverse elements to one another.*

**Proof.** We prove the statements by using the principle of Mathematical induction.

(i) Let $\mathbf{S}(n)$ be $a.a^n = a^n.a$ for positive integer $n$. Put $n = 1$.

$\therefore\ a.a^1 = a.a = a^1.a$ which implies that $\mathbf{S}(1)$ is true.

Let $\mathbf{S}(k)$ be true $\quad\therefore\ a.a^k = a^k.a \qquad \ldots(1)$

Now, $a.a^{k+1} = a.(a^k.a^1) = (a.a^k).a$ (associativity)

$= (a^k.a).a$ using (1) $= a^{k+1}.a$.

$\therefore$ $\mathbf{S}(k+1)$ is true. $\therefore$ By induction $\mathbf{S}(n)$ is true for every positive integer $n$.

(ii) Let $\mathbf{S}(n)$ be that $a^n$ and $a^{-n}$ are inverses to one another. Let $e$ be the identity in $\mathbf{G}$.

Since $a.a^{-1} = e = a^{-1}.a \Rightarrow a^1.a^{-1} = e = a^{-1}.a^1$, $\mathbf{S}(1)$ is true.

Let $\mathbf{S}(k)$ be true. $\therefore$ $a^k.a^{-k} = e = a^{-k}.a^k$ …(1)

Now $a^{k+1}.a^{-(k+1)} = a^{k+1}.(a^{-1})^{k+1} = a^k.a.(a^{-1})^k.a^{-1}$

$= a.a^k.a^{-k}.a^{-1} = a.(a^k.a^{-k}).a^{-1} = a.e.a^{-1}$ using (1) $= a.a^{-1} = e$.

Similarly we can have $a^{-(k+1)}.a^{k+1} = e$

$\therefore$ $a^{k+1}.a^{-(k+1)} = a^{-(k+1)}.a^{k+1}$

$\therefore$ $\mathbf{S}(k+1)$ is true. $\therefore$ By induction $\mathbf{S}(n)$ is true for every positive integer $n$.

**Note.** If $n \in \mathbf{N}, (a^n)^{-1} = a^{-n}$ and $(a^{-n})^{-1} = a^n$

**Theorem 20.** ***Let*** $\mathbf{G}$ ***be a group. Let*** $a, b \in \mathbf{G}$. ***(A.N.U.M 03, A.U.O 01, M.98)***
***Then*** (i) $a^m.a^n = a^{m+n}$ ***for*** $m, n \in \mathbf{N}$. (ii) $(a^m)^n = a^{mn}$ ***for*** $m, n \in \mathbf{N}$
(iii) $(ab)^n = a^n.b^n$ ***when*** $\mathbf{G}$ ***is abelian and*** $n \in \mathbf{N}$. (iv) $e^n = e$ ***for*** $n \in \mathbf{N}$.

**Proof.** We prove the statement by using the principle of Mathematical induction.

(i) Let $\mathbf{S}(n)$ be $a^m.a^n = a^{m+n}$ for $m, n \in \mathbf{N}$.

Put $n = 1$. $\therefore$ $a^m.a^1 = a^{m+1}$ (by definition) $\therefore$ $\mathbf{S}(1)$ is true.

Let $\mathbf{S}(k)$ be true for some $k \in \mathbf{N}$.

$\therefore$ $a^m.a^k = a^{m+k}$ …(1)

Now $a^m.a^{k+1} = a^m.(a^k.a) = (a^m.a^k).a = a^{m+k}.a$ using (1) $= a^{m+k+1}$

$\therefore$ $\mathbf{S}(k+1)$ is true.

$\therefore$ By the principle of Mathematical induction, $\mathbf{S}(n)$ is true for $n \in \mathbf{N}$.

**Note.** $a^m.a^n = a^n.a^m$ since $a^m.a^n = a^{m+n} = a^{n+m} = a^n.a^m$.

(ii) Let $\mathbf{S}(n)$ be : $(a^m)^n = a^{mn}$ for $m, n \in \mathbf{N}$.

Put $n = 1$ $\therefore$ $(a^m)^1 = a^m = a^{m.1}$ (by def.) $\therefore$ $\mathbf{S}(1)$ is true.

Let $\mathbf{S}(k)$ be true for some $k \in \mathbf{N}$. $\therefore$ $(a^m)^k = a^{mk}$ …(1)

Now $(a^m)^{k+1} = (a^m)^k.(a^m)^1 = a^{mk}.a^m$ using (1)

$= a^{mk+m} = a^{m(k+1)}$ $\therefore$ $\mathbf{S}(k+1)$ is true.

$\therefore$ By the Principle of Mathematical induction, $\mathbf{S}(n)$ is true for $n \in \mathbf{N}$.

**Note.** $(a^m)^n = (a^n)^m$ since $(a^m)^n = a^{mn} = (a^n)^m$ for $m, n \in \mathbf{N}$.

(iii) Let $\mathbf{S}(n)$ be : $(ab)^n = a^n b^n$ for $n \in \mathbf{N}$ and $\mathbf{G}$ is abelian

Put $n = 1$ $\therefore$ $(ab)^1 = a^1.b^1$ $\therefore$ $\mathbf{S}(1)$ is true.

Let $\mathbf{S}(k)$ be true for some $k \in \mathbf{N}$.

$\therefore$ $(ab)^k = a^k.b^k$ …(1)

Now $(ab)^{k+1} = (ab)^k.(ab)^1 = (a^k.b^k)(ab)$ using (1)

$= (a^k.b^k).(ba)$ since $\mathbf{G}$ is abelian

$= a^k.(b^k.(ba))$ $= a^k.((b^k.b).a) = a^k.(b^{k+1}.a)$

$= a^k.(a.b^{k+1}) = (a^k.a).b^{k+1}$ $= a^{k+1}.b^{k+1}$

$\therefore$ $\mathbf{S}(k+1)$ is true.

$\therefore$ By the Principle of Mathematical Induction, $\mathbf{S}(n)$ is true for $n \in \mathbf{N}$.

(iv) Let $\mathbf{S}(n)$ be : $e^n = e$ for $n \in \mathbf{N}$

Put $n = 1$ $\quad\therefore\quad$ $e^1 = e$ $\quad\therefore\quad$ $\mathbf{S}(1)$ is true.

Let $\mathbf{S}(k)$ be true for some $k \in \mathbf{N}$. $\quad\therefore\quad$ $e^k = e$ $\quad\ldots(1)$

Now $e^{k+1} = e^k . e = e . e = e$ using (1) $\quad\therefore\ \mathbf{S}(k+1)$ is true.

$\therefore$ By the Principle of Mathematical Induction, $\mathbf{S}(n)$ is true for $n \in \mathbf{N}$.

**Note 1.** The above theorems can also be proved to be true even if $m \in \mathbf{Z}, n \in \mathbf{Z}$.

**2.** If $\mathbf{G}$ is an additive group, the above theorems can be stated thus :

(i) $-(na) = (-n)\,a$ for $n \in \mathbf{Z}$.

(ii) $ma + na = (m+n)\,a = (n+m)\,a = na + ma$ for $m, n \in \mathbf{Z}$.

(iii) $n(ma) = (nm)\,a = (mn)\,a = m(na)$ for $m, n \in \mathbf{Z}$.

(iv) $m(a+b) = ma + mb$ for $m \in \mathbf{Z}$.

(v) $n0 = 0$ for $n \in \mathbf{Z}$ where 0 is the identity element.

**Ex. 23.** *In a group* $\mathbf{G}$ *for every* $a \in \mathbf{G}, a^2 = e$.

*Prove that* $\mathbf{G}$ *is an abelian group.*

**Sol.** Let $a, b \in \mathbf{G}$. $\quad\therefore\quad$ $ab \in \mathbf{G}$.

Since $\forall\, a \in \mathbf{G}, a^2 = e$, we have $(ab)^2 = e$

$\Rightarrow (ab)(ab) = e \Rightarrow (ab) = (ab)^{-1} = b^{-1}a^{-1}$

$\Rightarrow (ab) = b^{-1}a^{-1}$ $\quad\ldots(1)$

But $a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$ $\quad$ Similarly $b^2 = e \Rightarrow b^{-1} = b$

$\therefore$ From (1) $ab = ba$ implying that $\mathbf{G}$ is abelian.

**Ex. 24.** *Show that in a group* $\mathbf{G}$ *for* $a, b \in \mathbf{G}, (ab)^2 = a^2b^2 \Leftrightarrow \mathbf{G}$ *is abelian.*

**Sol.** Let $a, b \in \mathbf{G}$ and $(ab)^2 = a^2b^2$. To prove that $\mathbf{G}$ is abelian.

Then $\quad (ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = (aa)(bb) \quad \Rightarrow a(ba)b = a(ab)b$

$\Rightarrow ba = ab$ by cancellation laws. $\quad\Rightarrow\ \mathbf{G}$ is abelian

Let $\mathbf{G}$ be abelian. To prove that $(ab)^2 = a^2b^2$.

Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$.

**Ex. 25.** *If* $\mathbf{G}$ *is a group of even order, prove that it has an element* $a \neq e$ *satisfying* $a^2 = e$.

**Sol.** Let $\mathbf{O}(\mathbf{G}) = 2n$ where $n \in \mathbf{N}$. We shall prove that $\mathbf{G}$ must have an element $a \neq e$ such that $a^{-1} = a$.

Suppose $\mathbf{G}$ has no element other than the identity element $e$, which is its own inverse. We know that in a group every element possesses a unique inverse and the inverse of the identity element is itself. Further, if $b, c \in \mathbf{G}$ and $b = c^{-1}$, then $c = b^{-1}$.

So, excluding $e$, the remaining $(2n-1)$ elements of $\mathbf{G}$ must be divided into pairs such that each pair consists of an element and its inverse. Since $(2n-1)$ is odd, it is not possible. Hence our assumption is wrong.

Hence in the group $\mathbf{G}$ of even order there is at least one element $a\,(\neq e)$ which is its own inverse. If $a$ is taken as that element in $\mathbf{G}$, then $a = a^{-1}$.

$\therefore \quad aa^{-1} = e \Rightarrow aa = e \Rightarrow a^2 = e$.

**Ex. 26.** *If* $\mathbf{G}$ *is a group such that* $(ab)^m = a^m b^m$ *for three consecutive integers* $m$ *for all* $a, b \in \mathbf{G}$, *show that* $\mathbf{G}$ *is abelian.*

**Sol.** $a, b \in \mathbf{G}$. Let $m, m+1, m+2$ be three consecutive integers.

$\therefore$ By hyp. $(ab)^m = a^m b^m, (ab)^{m+1} = a^{m+1}b^{m+1}$, $(ab)^{m+2} = a^{m+2}.b^{m+2}$

$\therefore \quad (ab)^{m+2} = (ab)^{m+1}(ab)$

$\Rightarrow \quad a^{m+2}b^{m+2} = a^{m+1}b^{m+1}ab \Rightarrow aa^{m+1}b^{m+1}b = aa^m b^m bab$

$\Rightarrow \quad a^{m+1}.\, b^{m+1} = a^m b^m ba \quad \Rightarrow (ab)^{m+1} = (ab)^m (ba)$

$\Rightarrow \quad (ab)^m (ab) = (ab)^m (ba) \Rightarrow ab = ba \Rightarrow \mathbf{G}$ is abelian.

## 2.17. ORDER OF AN ELEMENT OF A GROUP

**Definition.** Let $(\mathbf{G}, .)$ be a group and $a$ be any element of $\mathbf{G}$. Then the order of the element $a$ is defined as the least positive integer $n$ such that $a^n = e$.

(In the additive notation, $na = e$)

If there exists no positive integer $n$ such that $a^n = e$, then we say that $a$ is of infinite order or zero order.

We denote the order of $a$ by $\mathbf{O}(a)$ or $|a|$.

If $a^m = e$ in a group $\mathbf{G}$ where $m$ is a positive integer, then the order of $a$ is finite. Also $\mathbf{O}(a) \leq m$. Observe that, by definition, $\mathbf{O}(a) \not> m$.

Since $e^1 = e, \mathbf{O}(e) = 1$. If $\mathbf{O}(a) = 1$ then $a = e$.

If $(\mathbf{G}, +)$ is the group and $ma = e$ where $a \in \mathbf{G}$ and $m$ is the least positive integer, then $\mathbf{O}(a) = m$. It may be noted that $a^m = e$ in multiplicative notation is equivalent to $ma = e$ in the additive notation.

**e.g. 1.** If $\mathbf{G} = \{1, -1\}$ then $\mathbf{G}$ is a finite group under usual multiplication. Here $\mathbf{O}(1) = 1$ and $\mathbf{O}(-1) = 2$ since $(-1)^2 = 1$.

**e.g. 2.** If $\mathbf{G} = \{1, \omega, \omega^2\}$, then $\mathbf{G}$ is a finite group under usual multiplication. $\mathbf{O}(1) = 1, \mathbf{O}(\omega) = 3 \quad (\because \omega^3 = 1)$ and $\mathbf{O}(\omega^2) = 3 \quad (\because (\omega^2)^3 = 1)$

**e.g. 3.** If $\mathbf{G}$ is a set of non-zero rational numbers, then $\mathbf{G}$ is an infinite group under usual multiplication.

Here $\mathbf{O}(1) = 1$. $(\because$ 1 is the identity) and $\mathbf{O}(-1) = 2$ since $(-1)^2 = 1$.

The order of every other element of $\mathbf{G}$ is infinite since $3 \in \mathbf{G}$ and $3^m \neq 1$ for any positive integer $m$.

**e.g. 4.** $(\mathbf{Z}, +)$ is an infinite group. 0 is the identity element.

For $a\,(\neq 0) \in \mathbf{Z}$, there is no $n \in \mathbf{N}$ such that $na = 0 \qquad \therefore \quad \mathbf{O}(a)$ is infinite.

**Theorem 21.** ***The order of every element of a finite group is finite and is less than or equal to the order of the group.***

**Proof.** Let $(\mathbf{G}, .)$ be a finite group, Let $a \in \mathbf{G}$.

By closure, we have $a^2, a^3, \ldots \in \mathbf{G}$. Since $\mathbf{G}$ is finite, all the positive integral powers of $a$ i.e. $a, a^2, a^3, \ldots$ cannot be distinct elements of $\mathbf{G}$.

Let $a^r = a^s$ where $r, s \in \mathbf{N}$ and $r > s$.

$\therefore\ a^r = a^s \Rightarrow a^{r-s} = a^0 = e \Rightarrow a^m = e$ where $r - s = m$

Since $r > s$, $m$ is a positive integer.

$\therefore\ \exists$ a positive integer $m$ such that $a^m = e$.

Hence if $n$ is the least positive integral value of $m$ such that $a^n = e$, then $\mathbf{O}(a) = n$.

$\therefore\ \mathbf{O}(a)$ is finite.

To prove that $\mathbf{O}(a) \le \mathbf{O}(\mathbf{G})$.

If possible let $\mathbf{O}(a) > \mathbf{O}(\mathbf{G})$. Let $\mathbf{O}(a) = n$.

By closure, we have $a, a^2, a^3, \ldots a^n \in \mathbf{G}$. No two of these elements are equal. For, if possible, let $a^r = a^s, 1 \le s < r \le n$. Then $a^{r-s} = e$. Since $\mathbf{O} < r - s < n, \mathbf{O}(a) < n$ which is a contradiction. Hence the $n$ elements $a, a^2, \ldots a^n$ are distinct elements of $\mathbf{G}$.

Since $n > \mathbf{O}(\mathbf{G})$, this is not possible.

$\therefore\ \mathbf{O}(a) \le \mathbf{O}(\mathbf{G})$.

**Theorem 22.** ***In a group*** $\mathbf{G}$, ***if*** $a \in \mathbf{G}$, ***then*** $\mathbf{O}(a) = \mathbf{O}(a^{-1})$.

**Proof.** Let $\mathbf{O}(a) = p$ and $\mathbf{O}(a^{-1}) = q$.

Now $\mathrm{O}(a) = p \Rightarrow a^p = e \Rightarrow (a^p)^{-1} = e^{-1} \Rightarrow a^{-p} = e$

$\Rightarrow (a^{-1})^p = e \Rightarrow \mathbf{O}(a^{-1}) \le p \Rightarrow q \le p$

Further $\mathrm{O}(a^{-1}) = q \Rightarrow (a^{-1})^q \Rightarrow a^{-q} = e$

$\Rightarrow (a^q)^{-1} = e^{-1} \Rightarrow a^q = e \Rightarrow \mathrm{O}(a) \le q \Rightarrow p \le q$

$\therefore q \le p$ and $p \le q \Rightarrow p = q \Rightarrow \mathbf{O}(a) = \mathbf{O}(a^{-1})$

**Theorem 23.** ***The order of any positive integral power of an element*** $a$ ***in a group*** $\mathbf{G}$ ***cannot exceed the order of*** $a$ ***i.e. in a group*** $\mathbf{G}$, $\mathbf{O}(a^m) \le \mathbf{O}(a), a \in \mathbf{G}$ ***and*** $m \in \mathbf{N}$.

**Proof.** Let $\mathbf{O}(a) = n$. If $m$ is a positive integer, then $a^m \in \mathbf{G}$.

$\mathbf{O}(a) = n, a^n = e \Rightarrow (a^n)^m = e^m \Rightarrow a^{mn} = e \Rightarrow (a^m)^n = e$.

$\Rightarrow \mathbf{O}(a^m) \le n \Rightarrow \mathbf{O}(a^m) \le \mathbf{O}(a)$.

**Theorem 24.** ***If*** $a$ ***is an element of a group*** $\mathbf{G}$ ***such that*** $\mathbf{O}(a) = n$, ***then*** $a^m = e$ ***iff*** $n/m$.

**Proof.** (i) Let $n/m$. To prove that $a^m = e$.

$\therefore$ There exists a positive integer $q$ such that $m = nq$.

Also $\mathbf{O}(a) = n \Rightarrow a^n = e$. $\therefore\ a^m = a^{nq} = (a^n)^q = e^q = e$.

(ii) Let $a^m = e$. To prove that $n/m$.

Since $n$ is a positive integer, by division algorithm, there exists integers $q$ and $r$ such that $m = nq + r, 0 \le r < n$.

Now $a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r$ $\quad\therefore\ a^m = e \Rightarrow a^r = e$

which is absurd since $\mathbf{O}(a) = n$ and $o \le r < n$ unless $r = 0$.

$\therefore\ a^m = e \Rightarrow m = nq \Rightarrow n/m$

***Theorem 25. If $a$ is an element of a group $\mathbf{G}$ such that $\mathbf{O}(a) = n$, then the set $\mathbf{H} = \{a^1, a^2, a^3, \ldots a^n\}$ forms a group w.r.t. the composition in $\mathbf{G}$.***

**Proof.** Let $(\mathbf{G}, .)$ be a group and $a \in \mathbf{G}$. Since $\mathbf{O}(a) = n, a^n = e$ where $e$ is the identity in $\mathbf{G}$.

Let $a^p, a^q \in \mathbf{H}$. Then $a^p.a^q = a^{p+q} = a^r \in \mathbf{H}$ when $p + q \equiv r \pmod n$ as $a^n = e$.

Hence closure is true in $\mathbf{H}$.

Again $(a^p.a^q).a^r = a^{(p+q)+r} = a^{p+(q+r)} = a^p.a^{q+r} = a^p(a^q.a^r)$ for $a^p, a^q, a^r \in \mathbf{H}$.

Hence associativity is true in $\mathbf{H}$.

Identity in $\mathbf{H}$ is $a^n = e = a^0$.

Also $a^p.a^{n-p} = a^n = e = a^{n-p}.a^p$ for $a^p, a^{n-p} \in \mathbf{H}$.

$\therefore$ Every element of $\mathbf{H}$ is invertible and $(a^p)^{-1} = a^{n-p}$.

Hence $\mathrm{H} = \{e = a^0 = a^n, a^1, a^2, \ldots, a^{n-1}\}$ is a group w.r.t. the composition in $\mathbf{G}$.

**Note 1.** (Vide definition of cyclic group Art. 8.2) $\mathbf{H}$ is cyclic subgroup of $\mathbf{G}$.

**2.** $\mathbf{O}(a) = n = \mathbf{O}(\mathbf{H})$.

***Theorem 26. If $a$ is an element of order $n$ of a group $\mathbf{G}$ and $p$ is prime to $n$, then $a^p$ is also of order $n$.***

**Proof.** Let $\mathbf{O}(a) = n$. Let $e$ be the identity in the group $(\mathbf{G}, \cdot)$. Let $\mathbf{O}(a^p) = m$.

$\therefore\ a^n = e \Rightarrow (a^n)^p = e^p \Rightarrow (a^p)^n = e \Rightarrow \mathbf{O}(a^p) \le n \Rightarrow m \le n$

Since $n, p$ are relatively prime $px + ny = 1$,

$a = a^1 = a^{px+ny} = a^{px}a^{ny} = a^{px}.(a^n)^y = a^{px}e^y = a^{px}e = (a^p)^x$

Now $a^m = [(a^p)^x]^m = (a^p)^{mx} = [(a^p)^m]^x = e^x = e$ [$\because\ \mathbf{O}(a^p) = m \Rightarrow (a^p)^m = e$]

$\therefore\ \mathbf{O}(a) \le m \Rightarrow n \le m$ $\quad\therefore\ m \le n$ and $n \le m \Rightarrow m = n$.

***Theorem 27. $\mathbf{G}$ is an abelian group. If $a, b \in \mathbf{G}$ such that $\mathbf{O}(a) = m, \mathbf{O}(b) = n$ and $(m, n) = 1$, then $\mathbf{O}(ab) = mn$***

**Proof.** $\mathbf{G}$ is an abelian group. Let $e$ be the identity in $\mathbf{G}$. Since $a, b \in \mathbf{G}$ such that $\mathbf{O}(a) = m, \mathbf{O}(b) = n$ we have $a^m = e$ and $a^n = e$.

Also $ab \in \mathbf{G}$. Let $\mathbf{O}(ab) = p$.

Now $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = ee = e$ $\quad\therefore\ p/mn$ $\quad\ldots(1)$

Also $(ab)^{pn} = [(ab)^p]^n = e^n = e$

and $(ab)^{pn} = a^{pn}b^{pn} = a^{pn}(b^n)^p = a^{pn}e^p = a^{pn}e = a^{pn} \Rightarrow a^{pn} = e \Rightarrow m/pn$

Now $(m, n) = 1 \Rightarrow m/p$ $\quad\ldots(2)$ Similarly we can have $n/p$ $\quad\ldots(3)$

$\therefore$ From (2) and (3) and from $(m, n) = 1$ we have $mn/p$ $\quad\ldots(4)$

$\therefore$ From (1) and (4), $mn = p$. $\quad$ Hence $\mathbf{O}(ab) = p = mn = \mathbf{O}(a)\,\mathbf{O}(b)$.

**Ex. 27.** *Find the order of each element of the multiplicative group* $\mathbf{G} = \{1, -1, i, -i\}$.

**Sol.** Identity element of $\mathbf{G} = 1$.

Now $\mathbf{O}(1) = 1, (-1)^2 = 1 \Rightarrow \mathbf{O}(-1) = 2$;

$(i)^1 = i, (i)^2 = -1, (i)^3 = -i, (i)^4 = 1 \Rightarrow \mathbf{O}(i) = 4$;

$(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1 \Rightarrow \mathbf{O}(-i) = 4$.

**Ex. 28.** *Find the order of each element of the group* $\mathbf{G} = \mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, *the composition being addition modulo 6.*

**Sol.** In additive notation, $ma = e \Rightarrow \mathbf{O}(a) = m$

In $\mathbf{G}$, 0 is the identity and hence $\mathbf{O}(0) = 1$.

Now $1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0 \Rightarrow 6\ (1) = 0 \Rightarrow \mathbf{O}\ (1) = 6$;

$2 +_6 2 +_6 2 = 0 \Rightarrow 3\ (2) = 0 \Rightarrow \mathbf{O}\ (2) = 3$;

$3 +_6 3 = 0 \Rightarrow 2\ (3) = 0 \Rightarrow \mathbf{O}\ (3) = 2$;

$4 +_6 4 +_6 4 = 0 \Rightarrow 3\ (4) = 0 \Rightarrow \mathbf{O}\ (4) = 3$;

$5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0 \Rightarrow 6\ (5) = 0 \Rightarrow \mathbf{O}\ (5) = 6$.

**Ex. 29.** *If every element of a group* $\mathbf{G}$ *except the identity element is of order two, then prove that the group* $\mathbf{G}$ *is abelian.* (

**Sol.** Let $(\mathbf{G}, .)$ be a group and $e$ be the identity in $\mathbf{G}$. $\mathbf{O}(e) = 1$. Also $e^2 = e$.

Since every element $a\ (\neq e)$ of $\mathbf{G}$ is of order 2.

We have $a^2 = e$. $\quad \therefore \quad a^2 = e\ \forall\ a \in \mathbf{G}$.

$a, b \in \mathbf{G} \Rightarrow ab \in \mathbf{G} \Rightarrow (ab)^2 = e$

$\Rightarrow (ab)(ab) = e \Rightarrow (ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab$

But $a^2 = e \Rightarrow aa = e \Rightarrow a = a^{-1}$ Similarly $b = b^{-1}$.

$\therefore \quad ba = ab$ implying that $\mathbf{G}$ is abelian.

**Ex. 30.** *In group* $\mathbf{G}$ *for* $a, b \in \mathbf{G}, \mathbf{O}(a) = 5, b \neq e$ *and* $ab\ a^{-1} = b^2$. *Find* $\mathbf{O}(b)$.

**Sol.** We have $(ab\ a^{-1})^2 = aba^{-1}aba^{-1} = abeba^{-1} = ab^2a^{-1} = aaba^{-1}a^{-1} = a^2ba^{-2}$

$\Rightarrow (aba^{-1})^4 = \{(aba^{-1})^2\}^2 = a^2ba^{-2}a^2ba^{-2}$

$= a^2b^2a^{-2} = a^2aba^{-1}a^{-2} = a^3ba^{-3}$

$\Rightarrow (aba^{-1})^8 = (a^3ba^{-3})^2 = a^3ba^{-3}a^3ba^{-3} = a^3b^2a^{-3}$

$= a^3aba^{-1}a^{-3} = a^4ba^{-4}$

$\Rightarrow (aba^{-1})^{16} = (a^4ba^{-4})^2 = a^4ba^{-4}a^4ba^{-4} = a^4b^2a^{-4}$

$= a^4aba^{-1}a^{-4} = a^5ba^{-5}$

But $\mathbf{O}(a) = 5 \Rightarrow a^5 = e$ and $\mathbf{O}(a^{-1}) = 5 \Rightarrow a^{-5} = e$

$\therefore \quad (aba^{-1})^{16} = ebe = b \Rightarrow (b^2)^{16} = b \Rightarrow b^{32} = be$

$\Rightarrow b^{31} = e \Rightarrow \mathbf{O}(b) / 31$. But 31 is prime

$\therefore \quad \mathbf{O}(b) = 1$ or 31. But $b \neq e$. $\quad \therefore \quad \mathbf{O}(b) \neq \mathbf{O}(e)$ i.e. $\mathbf{O}(b) \neq 1$.

$\therefore \quad \mathbf{O}(b) = 31$.

## EXERCISE 2 ( *c* )

**1.** $\mathbf{S}$ is a semi-group. If $\forall\ x, y \in \mathbf{S}, x^2y = y = yx^2$, prove that $\mathbf{S}$ is an abelian group.

**2.** $\mathbf{G}$ is a group with identity element $e$. If $x, y \in \mathbf{G}$ such that $xy^2 = y^3x$ and $yx^3 = x^2y$, then prove that $x = y = e$.

**3.** Show that the equation $x^2ax = a^{-1}$ is solvable in a group $\mathbf{G}$ iff $a$ is the cube of some element in $\mathbf{G}$.

**4.** For any two elements $a, b \in \mathbf{G}$ where $\mathbf{G}$ is a group, $\mathbf{O}(a) = \mathbf{O}(b^{-1}ab)$.

**5.** For any two elements $a, b \in \mathbf{G}$ where $\mathbf{G}$ is a group $\mathbf{O}(ab) = \mathbf{O}(ba)$.

**6.** $\mathbf{G}$ is a group and $a \in \mathbf{G}$. If $\mathbf{O}(a) = n$ and $m/n$ then prove that $\mathbf{O}(a^m) = \frac{n}{m}$.

**7.** In a group $\mathbf{G}$, if $a \in \mathbf{G}$ and $\mathbf{O}(a) = m$, then $\mathbf{O}(a^k) = \frac{m}{(m, k)}$ where $(m, k)$ denotes the H.C.F. of $m$ and $k$.

# Subgroups

## 3.1. COMPLEX DEFINITION

Any subset of a group $\mathbf{G}$ is called a **complex** of $\mathbf{G}$.

**e.g. 1.** The set of integers is a complex of the group $(\mathbf{R}, +)$.

**e.g. 2.** The set of even integers is a complex of the group $(\mathbf{Z}, +)$.

**e.g. 3.** The set of odd integers is a complex of the group $(\mathbf{R}, +)$.

**e.g. 4.** The set $(1, -1)$ is a complex of the multiplicative group $\mathbf{G} = \{1, -1, i, -i\}$

**Multiplication of two complexes.**

**Definition:** If $\mathbf{M}$ and $\mathbf{N}$ are any two complexes of group $\mathbf{G}$ then

$$\mathbf{MN} = \{mn \in \mathbf{G} / m \in \mathbf{M}, n \in \mathbf{N}\}$$

Clearly $\mathbf{MN} \subseteq \mathbf{G}$ and $\mathbf{MN}$ is called the product of the complexes $\mathbf{M}, \mathbf{N}$ of $\mathbf{G}$.

**Theorem 1 :** ***The multiplication of complexes of a group*** $\mathbf{G}$ ***is associative.***

**Proof :** Let $\mathbf{M}, \mathbf{N}, \mathbf{P}$ be any three complexes in a group $\mathbf{G}$.

Let $m \in \mathbf{M}, n \in \mathbf{N}, p \in \mathbf{P}$ so that $m, n, p \in \mathbf{G}$.

We have $\mathbf{MN} = \{mn \in \mathbf{G} / m \in \mathbf{M}, n \in \mathbf{N}\}$ so that

$$(\mathbf{MN})\,\mathbf{P} = \{(mn)p \in \mathbf{G} / mn \in \mathbf{MN}, p \in \mathbf{P}\} = \{m(np) \in \mathbf{G} / m \in \mathbf{M}, np \in \mathbf{NP}\} = \mathbf{M}(\mathbf{NP})$$

($\because$ associativity is true in $\mathbf{G}$)

**Note.** If $\mathbf{HK} = \mathbf{KH}$ then we cannot imply that $hk = kh$ for all $h \in \mathbf{H}$ and for all $k \in \mathbf{K}$. What we imply is $\mathbf{HK} \subseteq \mathbf{KH}$ and $\mathbf{KH} \subseteq \mathbf{HK}$.

**Definition :** If $\mathbf{M}$ is a complex in a group $\mathbf{G}$, then we define $\mathbf{M}^{-1} = \{m^{-1} \in \mathbf{G} / m \in \mathbf{M}\}$ i.e. $\mathbf{M}^{-1}$ is the set of all inverses of the elements of $\mathbf{M}$. Clearly $\mathbf{M}^{-1} \subseteq \mathbf{G}$.

**Theorem 2 :** ***If*** $\mathbf{M}, \mathbf{N}$ ***are any two complexes in group*** $\mathbf{G}$ ***then*** $(\mathbf{MN})^{-1} = \mathbf{N}^{-1}\mathbf{M}^{-1}$.

**Proof.** We have $\mathbf{MN} = \{mn \in \mathbf{G} / m \in \mathbf{M}, n \in \mathbf{N}\}$

Now $(\mathbf{MN})^{-1} = \{(mn)^{-1} \in \mathbf{G} / m \in \mathbf{M}, n \in \mathbf{N}\}$

$= \{n^{-1}m^{-1} \in \mathbf{G} / m \in \mathbf{M}, n \in \mathbf{N}\} = \mathbf{N}^{-1}\mathbf{M}^{-1}$.

## 3.2. SUBGROUPS

**Definition :** Let $(\mathbf{G}, .)$ be a group. Let $\mathbf{H}$ be a non-empty subset of $\mathbf{G}$ such that $(\mathbf{H}, .)$ be a group. Then $\mathbf{H}$ is called a **subgroup** of $\mathbf{G}$.

It is denoted by $\mathbf{H} \leq \mathbf{G}$ or $\mathbf{G} \geq \mathbf{H}$. And $\mathbf{H} < \mathbf{G}$ or $\mathbf{G} > \mathbf{H}$ we mean $\mathbf{H} \leq \mathbf{G}$ but $\mathbf{H} \neq \mathbf{G}$.

***(A.N.U.M. 97, S96, A.V.A 03, A 02, K.U.A 03, J 02, M99, 0.96, O.U.A 01, S.K.U. 098, O.U. A 01)***

**Note :** A complex of a group $\mathbf{G}$ is only a subset of $\mathbf{G}$ but a subgroup of a group $\mathbf{G}$ is a group. The binary operations in a group and its subgroup are the same.

**e.g. 1.** $(\mathbf{Z}, .)$ is a subgroup of $(\mathbf{Q}, .)$. Also $(\mathbf{Q}^+, \cdot)$ is a subgroup of $(\mathbf{R}^+, \cdot)$

**e.g. 2.** The additive group of even integers is a subgroup of the additive group of all integers.

**e.g. 3.** The multiplicative group $\{1, -1\}$ is a subgroup os the multiplicative group $\{1, -1, i, -i\}$.

For : $\mathbf{G} = \{1, -1, i, -i\}$ is a group under usual multiplication.

Composition table is :

| $\cdot$ | 1 | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| 1 | 1 | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | 1 | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | 1 |
| $-i$ | $-i$ | $i$ | 1 | $-1$ |

Here 1 is the identity and $(i)^{-1} = -i, (-i)^{-1} = i, (-1)^{-1} = -1$.

Consider $\mathbf{H} = \{1, -1\}$ which is a subset of group $(\mathbf{G}, \cdot)$.

Clearly $(\mathbf{H}, \cdot)$ is a group. Here 1 is the identity, $(-1)^{-1} = -1$.

$\therefore$ $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

Similarly $(\{1\}, \cdot), (\{1, -1, i, -i\}, \cdot)$ are subgroups of $(\mathbf{G}, \cdot)$.

**e.g. 4.** $(\mathbf{N}, +)$ is not a subgroup of the group $(\mathbf{Z}, +)$ since identity does not exist in $\mathbf{N}$ under +.

**Note 1:** Every group having at least two elements has at least two subgroups. Suppose $e$ is the identity element in a group $\mathbf{G}$. Then $\{e\} \subseteq \mathbf{G}$ and we have $ee = e, e^{-1} = e$, etc. So $\{e\}$ is a subgroup of $\mathbf{G}$. Also $\mathbf{G} \subseteq \mathbf{G}$. So $\mathbf{G}$ is also a subgroup of $\mathbf{G}$. These two subgroups $\{e\}, \mathbf{G}$ of $\mathbf{G}$ are called trivial or improper subgroups of $\mathbf{G}$. All other subgroups, if exist, are called non-trivial or proper subgroups of $\mathbf{G}$.

**2.** A complex of a group need not be a subgroup of the group. But a subgroup of a group is always a complex of the group.

**3.** A complex of a group $(\mathbf{G}, .)$ need not be a subgroup w.r.t. the binary operation, but it can be a group w.r.t. another binary operation. For example, the complex $\{3^n, n \in z\}$ of the group $(\mathbf{Z}, +)$ is not a subgroup of $(\mathbf{Z}, +)$ w.r.t. binary operation + whereas the same subset is a group under multiplication.

It is clear that every subgroup of abelian group is abelian. But for non abelian group it may not be true..

For example ref. Ex. 15 Chapter 2.

$\mathbf{P}_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ set of all bisections on three sysmbols is a non-abelian group.

But $\mathbf{A}_3 = \{f_1, f_5, f_6\}$ and $\mathbf{H} = \{f_1, f_2\}$ an abelian subgroup of $\mathbf{P}_3$.

**Lattice Diagram.** Often it is useful to show the subgroups of a group by a Lattice diagram. In this diagram we show the larger group near the top of the diagram followed by a line running towards a subgroup of the group.

We give below Lattice Diagram for the multiplicative group $\{1, -1, i, -i\}$.

$\{1, -1, i, -i\}$

|

$\{1, -1\}$

|

$\{1\}$

## 3.3. THE IDENTITY AND INVERSE OF AN ELEMENT OF A SUBGROUP $\mathbf{H}$ OF A GROUP $\mathbf{G}$.

**Theorem 3 :** ***The identity of a subgroup*** $\mathbf{H}$ ***of a group is same as the identity of*** $\mathbf{G}$ **.** *(A.N.U.J 03, S 02)*

**Proof.** Let $a \in \mathbf{H}$ and $e'$ be the identity of $\mathbf{H}$.

Since $\mathbf{H}$ is a group, $a\,e' = a$ …(1) Let $e$ be the identity in $\mathbf{G}$.

Again $a \in \mathbf{H} \Rightarrow a \in \mathbf{G}$. $\therefore$ $a\,e = a$ …(2)

Also $e' \in \mathbf{H} \Rightarrow e' \in \mathbf{G}$.

From (1) and (2), $a\,e' = ae \Rightarrow e' = e$ (using left cancellation law).

**Theorem 4.** ***The inverse of any element of a subgroup*** $\mathbf{H}$ ***of a group*** $\mathbf{G}$ ***is same as the inverse of that element regarded as an element of the group*** $\mathbf{G}$ **.**

**Proof.** Let $e$ be the identity in - $\mathbf{G}$. Since $\mathbf{H}$ is a subgroup of $\mathbf{G}$, $e$ is also the identity in $\mathbf{H}$.

Let $a \in \mathbf{H}$. $\therefore$ $a \in \mathbf{G}$.

Let $b$ be the inverse of $a$ in $\mathbf{H}$ and $c$ be the inverse of $a$ in $\mathbf{G}$.

Then $ab = e$ and $ac = e$. $\Rightarrow ab = ac \Rightarrow b = c$ (using left cancellation law)

**Theorem 5.** ***If*** $\mathbf{H}$ ***is any subgroup of a group*** $\mathbf{G}$***, then*** $\mathbf{H^{-1}} = \mathbf{H}$**.** *(S. V. U. A11, A.N.U.M.02, S.K.U.M 02, M 09)*

**Proof.** Let $\mathbf{H}$ be a subgroup of a group $\mathbf{G}$. Let $h^{-1} \in \mathbf{H}^{-1}$. By def. of $\mathbf{H}^{-1}$, $h \in \mathbf{H}$.

Since $\mathbf{H}$ is a subgroup of a group $\mathbf{G}$, $h^{-1} \in \mathbf{H}$.

$\therefore$ $h^{-1} \in \mathbf{H}^{-1} \Rightarrow h^{-1} \in \mathbf{H}$ $\therefore$ $\mathbf{H}^{-1} \subseteq \mathbf{H}$.

Again $h \in \mathbf{H} \Rightarrow h^{-1} \in \mathbf{H}$. $\Rightarrow (h^{-1})^{-1} \in \mathbf{H}^{-1} \Rightarrow h \in \mathbf{H}^{-1}$

$\therefore$ $\mathbf{H} \subseteq \mathbf{H}^{-1}$. Hence $\mathbf{H}^{-1} = \mathbf{H}$

**Note.** The converse of the above theorem is not true i.e. if $\mathbf{H}$ is any complex of a group $\mathbf{G}$ such that $\mathbf{H}^{-1} = \mathbf{H}$, then $\mathbf{H}$ need not be a subgroup of $\mathbf{G}$.

**e.g.** $\mathbf{H} = \{-1\}$ is a complex of the multiplicative group $\mathbf{G} = \{1, -1\}$. Since the inverse of $-1$ is $-1$, then $\mathbf{H}^{-1} = \{-1\}$.

But $\mathbf{H} = \{-1\}$ is not a group under multiplication since $(-1)(-1) = 1 \notin \mathbf{H}$ (Closure is not true) i.e. $\mathbf{H}$ is not a subgroup of $\mathbf{G}$. Hence even if $\mathbf{H}^{-1} = \mathbf{H}$, $\mathbf{H}$ is not a subgroup of $\mathbf{G}$.

**Theorem 6.** ***If*** $\mathbf{H}$ ***is any subgroup of a group*** $\mathbf{G}$***, then*** $\mathbf{HH} = \mathbf{H}$**.** *(S. V. U. A11, S.K.U.0.97)*

**Proof.** Let $x \in \mathbf{HH}$ so that $x = h_1.h_2$ where $h_1 \in \mathbf{H}$ and $h_2 \in \mathbf{H}$.

Since $\mathbf{H}$ is a subgroup, $h_1h_2 \in \mathbf{H}$ $\therefore$ $x \in \mathbf{H}$ $\therefore$ $\mathbf{HH} \subseteq \mathbf{H}$.

Let $h_3 \in \mathbf{H}$ and $e$ be the identity in $\mathbf{H}$.

Then $h_3 = h_3e \in \mathbf{HH}$ $\therefore$ $\mathbf{H} \subseteq \mathbf{HH}$. $\therefore$ $\mathbf{HH} = \mathbf{H}$.

## 3.4. CRITERION FOR A COMPLEX TO BE A SUBGROUP.

**Theorem 7.** ***A non-empty complex*** $\mathbf{H}$ ***of a group*** $\mathbf{G}$ ***is a subgroup of*** $\mathbf{G}$ ***if and only if*** (i) $a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$, (ii) $a \in \mathbf{H}, a^{-1} \in \mathbf{H}$ *(O. U. 12, A. U. 12, A.U.M.99, M97, K.U.J. 03, S 01, A98)*

**Proof.** The conditions are necessary.

Let **H** be a subgroup of the group **G**. To prove that (i), (ii) are true

$\therefore$ **H** is a group.

$\therefore$ By closure axiom $a, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$ and by inverse axiom $a \in \mathbf{H} \Rightarrow a^{-1} \in \mathbf{H}$

The conditions are sufficient.

Let (i) and (ii) be true. To prove that **H** is a subgroup of **G**.

**1.** By (i) closure axiom is true in **H**.

**2.** The elements of **H** are also elements of **G**. Since **G** is a group, the composition in **G** is associative and hence the composition in **H** is associative.

**3.** Since **H** is non-empty, let $a \in \mathbf{H}$. $\therefore$ By (ii) $a^{-1} \in \mathbf{H}$

$\therefore$ $a \in \mathbf{H}, a^{-1} \in \mathbf{H} \Rightarrow aa^{-1} \in \mathbf{H}$

$\Rightarrow$ $e \in \mathbf{H}$ ($\because$ $aa^{-1} \in \mathbf{H} \Rightarrow aa^{-1} \in \mathbf{G} \Rightarrow aa^{-1} = e$ where $e$ is the identity in **G**).

$\Rightarrow$ $e$ is the identity in **H**.

**4.** Since we have $a \in \mathbf{H} \Rightarrow a^{-1} \in \mathbf{H}$ and $aa^{-1} = e$, every element of **H** possesses inverse in **H**.

Hence **H** itself is a group for the composition in **G**.

So **H** is a subgroup of **G**.

**Note 1.** If the operation in **G** is +, then the conditions in the above theorem can be stated as follows : (i) $a, b \in \mathrm{H} \Rightarrow a + b \in \mathrm{H}$, (ii) $a \in \mathbf{H} \Rightarrow -a \in \mathbf{H}$.

**2.** It is called **Two - step subgroup Test.**

**Theorem. 8 .** ***H is a non-empty complex of a group G. The necessary and sufficient condition for H to be a subgroup of G is*** $a, b \in \mathbf{H} \Rightarrow ab^{-1} \in \mathbf{H}$ ***where*** $b^{-1}$ ***is the inverse of*** $b$ ***in G .*** *(A.N.U. A11, A12, S02, S01, M00, M99, M97, S96, O.U.M 08, 02,O99, A.U.A.03, A 02, A01, S00, M00, S99, K.U.M11, M12, M.05, M01, 099, M99, 098, S.V.U. 11, 12, 00, 098)*

**Proof.** The condition is necessary.

Since **H** is a group by itself, $b \in \mathbf{H} \Rightarrow b^{-1} \in \mathbf{H}$

$\therefore$ $a \in \mathbf{H}$, $b \in \mathbf{H} \Rightarrow a \in \mathbf{H}$, $b^{-1} \in \mathbf{H} \Rightarrow ab^{-1} \in \mathbf{H}$ (by closure axiom).

The condition is sufficient.

**1.** Since $\mathbf{H} \neq \phi$, let $a \in \mathbf{H}$. By hyp. $a \in \mathbf{H}$, $b \in \mathbf{H} \Rightarrow ab^{-1} \in \mathbf{H}$.

$\therefore$ $a \in \mathbf{H}$, $a^{-1} \in \mathbf{H} \Rightarrow aa^{-1} \in \mathbf{H} \Rightarrow aa^{-1} \in \mathbf{G}$

But in **G**, $a \in \mathbf{G} \Rightarrow aa^{-1} = e, e$ is the identity in **G**. $\therefore$ $e \in \mathbf{H}$.

**2.** We have $e \in \mathbf{H}, a \in \mathbf{H} \Rightarrow ea^{-1} \in \mathbf{H} \Rightarrow a^{-1} \in \mathbf{H}$ $\therefore$ $a \in \mathbf{H} \Rightarrow a^{-1} \in \mathbf{H}$.

**3.** $b \in \mathbf{H} \Rightarrow b^{-1} \in \mathbf{H}$ $\therefore$ $a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow a, b^{-1} \in \mathbf{H} \Rightarrow a\,(b^{-1})^{-1} \in \mathbf{H}$

$\Rightarrow$ $ab \in \mathbf{H}$

**4.** Since all the elements of **H** are in **G** and since the composition is associative in **G**, the composition is associative in **H**.

$\therefore$ **H** is a group for the composition in **G** and hence **H** is a subgroup of **G**.

**Note 1.** If the operation in $\mathbf{G}$ is +, then the condition in the above theorem can be stated as follows :

$$a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow a - b \in \mathbf{H}$$

**2.** The above theorem can be used to prove that a certain non-empty subset of a given group is a subgroup of the group. It is called **One - step subgroup Test.**

**Theorem 9.** ***A necessary and sufficient condition for a non-empty complex*** $\mathbf{H}$ ***of a group*** $\mathbf{G}$ ***to be a subgroup of*** $\mathbf{G}$ ***is that*** $\mathbf{HH}^{-1} \subseteq \mathbf{H}$. ***(A.N.U.J. 04)***

**Proof.** The condition is necessary.

Let $\mathbf{H}$ be a subgroup of $\mathbf{G}$. Let $ab^{-1} \in \mathbf{HH}^{-1}$ so that $a \in \mathbf{H}, b \in \mathbf{H}$

Since $\mathbf{H}$ is a group we have $b^{-1} \in \mathbf{H}$.

$\therefore$ $a \in \mathbf{H} \Rightarrow b^{-1} \in \mathbf{H} \Rightarrow ab^{-1} \in \mathbf{H}$, (By closure axiom)

$\therefore$ $\mathbf{HH}^{-1} \subseteq \mathbf{H}$. The condition is sufficient.

Let $\mathbf{HH}^{-1} \subseteq \mathbf{H}$ Let $a, b \in \mathbf{H}$. $\therefore$ $ab^{-1} \in \mathbf{HH}^{-1}$

Since $\mathbf{HH}^{-1} \subseteq \mathbf{H}, ab^{-1} \in \mathbf{H}$ $\therefore$ $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

**Theorem 10.** ***A necessary and sufficient condition for a non-empty subset*** $\mathbf{H}$ ***of a group*** $\mathbf{G}$ ***to be a subgroup of*** $\mathbf{G}$ ***is that*** $\mathbf{HH}^{-1} = \mathbf{H}$.

**Proof.** The condition is necessary.

Let $\mathbf{H}$ be a subgroup of $\mathbf{G}$. Then we have $\mathbf{HH}^{-1} \subseteq \mathbf{H}$.

Let $e$ be the identity in $\mathbf{G}$. $\therefore$ $e$ is the identity in $\mathbf{H}$.

Let $h \in \mathbf{H}$ $\therefore$ $h = he = he^{-1} \in \mathbf{HH}^{-1}$

$\therefore$ $\mathbf{H} \subseteq \mathbf{HH}^{-1}$ $\therefore$ $\mathbf{HH}^{-1} \subseteq \mathbf{H}$ The condition is sufficient.

Let $\mathbf{HH}^{-1} = \mathbf{H}$. $\therefore$ $\mathbf{HH}^{-1} \subseteq \mathbf{H}$ $\therefore$ $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

**Theorem 11.** ***The necessary and sufficient condition for a finite complex*** $\mathbf{H}$ ***of a group*** $\mathbf{G}$ ***to be a subgroup of*** $\mathbf{G}$ ***is*** $a, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$.

**OR**

***Prove that a non-empty finite subset of a group which is closed under multiplication is a subgroup of*** $\mathbf{G}$. ***(A.U.0 01, M12, K.U.A. 03, J 02, M99, 097, M96, N.U.J 03, M 02, S97, O.U.A. 01, SKU 0 03, 0 01, 0 00, A99, 098, S.V.U. M11, O 02, M 01, A 00, 099, 097)***

**Proof.** The condition is necessary.

$\mathbf{H}$ be a subgroup of $\mathbf{G}$.

By closure axiom, $a, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$. The condition is sufficient.

Let $a, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$ $\therefore$ $(\because \mathbf{H} \neq \phi)$

Let $a \in \mathbf{H}$. By hyp. we have $a \in \mathbf{H}, a \in \mathbf{H} \Rightarrow a.a \in \mathbf{H} \Rightarrow a^2 \in \mathbf{H}$

Again $a^2 \in \mathbf{H}, a \in \mathbf{H} \Rightarrow a^2.a \in \mathbf{H} \Rightarrow a^3 \in \mathbf{H}$

By induction we can prove that $a^n \in \mathbf{H}$ where $n$ is any positive integer. Thus all the elements $a$, $a^2$, $a^3$, …, $a^n$, … belong to $\mathbf{H}$ and they are infinite in number.

But $\mathbf{H}$ is a finite subset of $\mathbf{G}$. Therefore, there must be repetitions in the collection of elements.

Let $a^r = a^s$ for some positive integers $r$ and $s$ such that $r > s$

$\therefore \quad a^r.a^{-s} = a^s.a^{-s} = a^{s-s} = a^0 = e$ where $e$ is the identity in $\mathbf{G}$.

Since $r - s$ is a positive integer, $a^{r-s} \in \mathbf{H} \Rightarrow e \in \mathbf{H}$

$\therefore \quad e = a^0 \in \mathbf{H}$.

Now $r > s \Rightarrow r - s \geq 1 \qquad \therefore \quad r - s - 1 \geq 0$ and hence $a^{r-s-1} \in \mathbf{H}$

Also $a^{r-s-1}a = a^{r-s} = e = a.a^{r-s-1}$

$\therefore$ We have for $a \in \mathbf{H}, a^{r-s-1} \in \mathbf{H}$ as the inverse of $a$.

Thus each element of $\mathbf{H}$ is invertible.

Since all the elements of $\mathbf{H}$ are elements of $\mathbf{G}$, associativity is satisfied.

$\mathbf{H}$ is a group for the composition in $\mathbf{G}$ and hence $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

**Cor.** A finite non-empty subset $\mathbf{H}$ of a group $\mathbf{G}$ is also a subgroup of $\mathbf{G}$ if and only if $\mathbf{HH} = \mathbf{H}$.

**e.g.** $(\mathbf{Z}_6, +_6)$ is a group and $(\mathbf{H} = \{0, 2, 4\}, +_6)$ is a subgroup of it.

For : $\mathbf{H} \subset \mathbf{Z}_6$. Also $0 +_6 0 = 0, 0 +_6 2 = 2, 0 +_6 4 = 4, 2 +_6 4 = 0, 4 +_6 4 = 2$ etc.

So $a, b \in \mathbf{H} \Rightarrow a +_6 b \in \mathbf{H}$.

**Note.** The criterion given in the above theorem is valid only for finite subsets of a group $\mathbf{G}$. It is not valid for an infinite subset of an infinite group $\mathbf{G}$. ***(O.U. 2001)***

**e.g.** $(\mathbf{Z}, +)$ is a group. Let $\mathbf{N}$ be the set of all positive integers.

$\therefore \quad \mathbf{N} \subset \mathbf{Z}$. Also $(\mathbf{N}, +)$ is not a group even though $a, b \in \mathbf{N} \Rightarrow a + b \in \mathbf{N}$.

$\therefore \quad (\mathbf{N}, +)$ is not a subgroup of $(\mathbf{Z}, +)$. Hence the above theorem is not satisfied.

**Theorem 12.** ***A non-empty subset $\mathbf{H}$ of a finite group $\mathbf{G}$ is a subgroup if $a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$.*** ***(S.K.U. 01/0)***

**OR**

***A necessary and sufficient condition for a complex $\mathbf{H}$ of a finite group $\mathbf{G}$ to be a subgroup is that $a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$.***

**Proof. The condition is necessary.**

Let $\mathbf{H}$ be a subgroup of a finite group $\mathbf{G}$. Then $\mathbf{H}$ is closed w.r.t. the composition in $\mathbf{G}$.

$\therefore \quad a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$.

**The condition is sufficient.**

$\mathbf{H}$ is a non-empty subset (complex of $\mathbf{G}$) of a finite group $\mathbf{G}$ such that $a \in \mathbf{H}, b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$.

Now we have to prove that $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

**Associativity.** Since $\mathbf{H}$ is a subset of $\mathbf{G}$, all the elements of $\mathbf{H}$ are the elements of $\mathbf{G}$ and hence associativity is true in $\mathbf{H}$ w.r.t. the composition in $\mathbf{G}$.

**Existence of identity.** Let $a \in \mathbf{H}$. $\therefore \quad a \in \mathbf{G}$. Since $\mathbf{G}$ is finite and since every element of a finite group is of finite order, it follows that the order of $a$ is finite.

Let $0(a) = n$. $\therefore \quad a^n = e$ where $e$ is the identity in $\mathbf{G}$.

By closure law in $\mathbf{H}$, we have $a^2, a^3, \ldots, a^n, \ldots \in \mathbf{H}$. …(1)

Since $a^n = e = a^0$, we have $a^0 = e \in \mathbf{H}$ i.e. identity exists in $\mathbf{H}$.

**Existence of inverse**. Let $a \in \mathbf{H}$ Here $e = a^n = a^0$.

$\therefore \quad a \in \mathbf{G}$ and $0(a) = n \Rightarrow n$ is the least positive integer such that

$\Rightarrow (n-1) \geq 0$. $\qquad a^n = e$

By (1), $a^{n-1} \in \mathbf{H}$.

Now in $\mathbf{G}$, $a^{n-1}a = a^n = a\,a^{n-1}$.

$\Rightarrow \quad a^{n-1}a = a\,a^{n-1} = e$ true in $\mathbf{H}$. $\qquad \Rightarrow \quad a^{-1} = a^{n-1}$

$\Rightarrow$ every element of $\mathbf{H}$ is invertible.

$\Rightarrow$ $\mathbf{H}$ is a group and hence a subgroup of $\mathbf{G}$.

## 3.5. CRITERION FOR THE PRODUCT OF TWO SUBGROUPS TO BE A SUBGROUP

**Theorem 13.** *If* $\mathbf{H}$ *and* $\mathbf{K}$ *are two subgroups of a group* $\mathbf{G}$, *then* $\mathbf{HK}$ *is a subgroup of* $\mathbf{G}$ *iff* $\mathbf{HK} = \mathbf{KH}$. *(S.V.U. S 93, A 97, 2K, N.U. O 89, A 93, S.K.U. A 00 A.N.U.J 04, S 00, S98, M96, A90, O.U.M 03, S.K.U. O 03, M 07, O 01, 0 00, A 00, 099, A97)*

**Proof.** Let $\mathbf{H}, \mathbf{K}$ be any two subgroups of $\mathbf{G}$.

**1st part.** Let $\mathbf{HK} = \mathbf{KH}$. To prove that $\mathbf{HK}$ is a subgroup of $\mathbf{G}$.

So it is sufficient to prove that $(\mathbf{HK})(\mathbf{HK})^{-1} = \mathbf{HK}$.

$(\mathbf{HK})(\mathbf{HK})^{-1} = (\mathbf{HK})(\mathbf{K}^{-1}\mathbf{H}^{-1})$ (Theorem 2.)

$= \mathbf{H}(\mathbf{KK}^{-1})\mathbf{H}^{-1}$ ($\because$ Complex multiplication is associative).

$= \mathbf{H}(\mathbf{K})\mathbf{H}^{-1}$ (Theorem 10) $= (\mathbf{HK})\mathbf{H}^{-1}$ (Theorem 1)

$= (\mathbf{KH})\mathbf{H}^{-1}$ (Hyp.) $= \mathbf{K}(\mathbf{HH}^{-1}) = \mathbf{KH} = \mathbf{HK}$.

$\mathbf{HK} = \mathbf{KH} \Rightarrow \mathbf{HK}$ is subgroup of $\mathbf{G}$.

**2nd part.** Let $\mathbf{HK}$ be a subgroup of a group $\mathbf{G}$.

$\therefore \quad (\mathbf{HK})^{-1} = \mathbf{HK} \Rightarrow \mathbf{K}^{-1}\mathbf{H}^{-1} = \mathbf{HK} \Rightarrow \mathbf{KH} = \mathbf{HK}$.

($\because$ $\mathbf{K}$ is a subgroup, $\mathbf{K}^{-1} = \mathbf{K}$ and $\mathbf{H}$ is a subgroup, $\mathbf{H}^{-1} = \mathbf{H}$)

**Cor.** If $\mathbf{H}, \mathbf{K}$ are subgroups of an abelian group $\mathbf{G}$, then $\mathbf{HK}$ is a subgroup of $\mathbf{G}$.

**For :** Since $\mathbf{G}$ is abelian, $\mathbf{HK} = \mathbf{KH}$. By the above theorem $\mathbf{HK}$ is a subgroup of $\mathbf{G}$.

**Ex.1:** *If* $\mathbf{Z}$ *is the additive group of integers, then prove that the set of all multiples of integers by a fixed integer* $m$ *is a subgroup of* $\mathbf{Z}$.

**Sol :** We have $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Let $\mathbf{H} = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\} = mz$

where $m$ is a fixed integer.

Let $a = rm$, $b = sm$ be any two elements of $\mathbf{H}$ where $r, s$ are integers.

Then $a - b = rm - sm = (r-s)m = pm$ where $p$ is an integer

$\Rightarrow \quad a - b \in \mathbf{H}$.

$\therefore \quad a, b \in \mathbf{H} \Rightarrow a - b \in \mathbf{H}$. $\qquad \therefore \quad \mathbf{H}$ is a subgroup of $\mathbf{Z}$.

**Ex. 2 :** *Prove that in the dihedral group of order* 8, *denoted by* $\mathbf{D}_4$, *the subset* $\mathbf{H} = \{r_{360}, r_{180}, x, y\}$ *is subgroup of* $\mathbf{D}_4$.

**Sol :** Vide Ex. 17 of Chapter 2.

We can observe from the composition table of $\mathbf{D}_4$.

(i) Closure is obvious.

(ii) Associativity is evident since the composition of maps is associative.

(iii) The identity element of $\mathbf{H}$ is $r_{360}$.

(iv) Each element of $\mathbf{H}$ is inverse of itself.

$\therefore$ $\mathbf{H}$ is a group. Here $\mathbf{H}$ is a subgroup of $\mathbf{D}_4$.

**Ex. 3 :** *From Ex. 15 of chapter 2,* $\mathbf{P}_3$ *is a non-abelian group of order 6.* $\mathbf{A}_3$ *is a subgroup of* $\mathbf{P}_3$. *Also* $\mathbf{A}_3$ *is an abelian subgroup of* $\mathbf{P}_3$.

**Ex. 4 :** *In Ex. 16 of chapter 2, we have* $\mathbf{G} = \{r_0, r_1, r_2, f_1, f_2, f_3\}$ *the set of all symmetries of an equilateral triangle, as a non-abelian group.*

*Consider* $\mathrm{H} = \{r_0, r_1, r_2\}$. *We can see from the composition table that* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$. *Also* $\mathbf{H}$ *is abelian. Hence a non-abelian group can have an abelian subgroup.*

**Ex. 5 :** $\mathbf{S}$, *the set of all ordered pairs* $(a, b)$ *of real numbers for which* $a \neq 0$ *w.r.t. the operation* $\times$ *defined by* $(a, b) \times (c, d) = (ac, bc + d)$ ***is a non-abelian group.*** (vide Ex. 7 of chapter 2). *Let* $\mathbf{H} = \{(1, b) \mid b \in \mathbf{R}\}$ *be a subset of* $\mathbf{S}$. *Show that* $\mathbf{H}$ *is a subgroup of the group* $(\mathbf{S}, \times)$.

**Sol :** Identity in $\mathbf{S}$ is $(1, 0)$. Clearly $(1, 0) \in \mathbf{H}$.

Inverse of $(a, b)$ in $\mathbf{S}$ is $\left(\frac{1}{a}, -\frac{b}{a}\right)$ $(\because \ a \neq 0)$.

Inverse of $(1, c)$ in $\mathbf{S}$ is $\left(\frac{1}{1}, -\frac{c}{1}\right)$ i.e. $(1, -c)$. Clearly $(1, c) \in \mathbf{H}$. Let $(1, b) \in \mathbf{H}$.

$\therefore$ $(1,b)\ (1,c)^{-1} = (1,b) \times (1, -c) = (1 . 1, b . 1 - c) = (1, b - c) \in \mathbf{H}$ since $b - c \in \mathbf{R}$.

$\therefore$ $(1,b), (1,c) \in \mathrm{H} \Rightarrow (1,b) \times (1,c)^{-1} \in \mathrm{H}$ $\therefore$ $\mathbf{H}$ is a subgroup of $(\mathbf{S}, \times)$.

**Note.** $(1, b) \times (1, c) = (1 . 1, b . 1 + c) = (1, b + c) = (1, c + b) = (1, c) \times (1, b)$

$\mathbf{H}$ is an abelian subgroup of the non-abelian group $(\mathbf{S}, \times)$.

*Hence a non-abelian group can have an abelian subgroup.*

## 3. 6. UNION AND INTERSECTION OF SUBGROUPS

**Theorem 14.** ***If*** $\mathbf{H}_1$ ***and*** $\mathbf{H}_2$ ***are two subgroups of a group*** $\mathbf{G}$ ***then*** $\mathbf{H}_1 \cap \mathbf{H}_2$ ***is also a subgroup of*** $\mathbf{G}$. ***(O.U. 01/0, N.U. O 92, O.U. 93, 0 02, 01, M 05, K.U. M 04, M 01, O 02, A 00, S.K.U.M 05 M.96)***

**Proof.** Let $\mathbf{H}_1$ and $\mathbf{H}_2$ be two subgroups of $\mathbf{G}$.

Let $e$ be the identity in $\mathbf{G}$.

$\therefore$ $e \in \mathbf{H}_1$ and $e \in \mathbf{H}_2 \Rightarrow e \in \mathbf{H}_1 \cap \mathbf{H}_2$ $\therefore$ $\mathbf{H}_1 \cap \mathbf{H}_2 \neq \phi$

Let $a \in \mathbf{H}_1 \cap \mathbf{H}_2, b \in \mathbf{H}_1 \cap \mathbf{H}_2$ $\therefore$ $a \in \mathbf{H}_1, a \in \mathbf{H}_2$ and $b \in \mathbf{H}_1, b \in \mathbf{H}_2$

Since $\mathbf{H}_1$ is a subgroup, $a \in \mathbf{H}_1$ and $b \in \mathbf{H}_1 \Rightarrow ab^{-1} \in \mathbf{H}$;

Similarly $ab^{-1} \in \mathbf{H}_2$. $\therefore$ $ab^{-1} \in \mathbf{H}_1 \cap \mathbf{H}_2$

Thus we have $a \in \mathbf{H}_1 \cap \mathbf{H}_2, b \in \mathbf{H}_1 \cap \mathbf{H}_2 \Rightarrow ab^{-1} \in \mathbf{H}_1 \cap \mathbf{H}_2$

$\therefore$ $\mathbf{H}_1 \cap \mathbf{H}_2$ is a subgroup of $\mathbf{G}$.

**Note 1.** Intersection of a arbitrary family of subgroups of a group is a subgroup of the group i.e. if $\{\mathbf{H}_i / i \in \Delta\}$ is any set of subgroups of a group $\mathbf{G}$, then $\underset{i\in\Delta}{\cap} \mathbf{H}_i$ is a subgroup of $\mathbf{G}$.

**2.** $\mathbf{H}_1 \cap \mathbf{H}_2$ is the largest subgroup of $\mathbf{G}$ contained in $\mathbf{H}_1$ and $\mathbf{H}_2$ *i.e.* $\mathbf{H}_1 \cap \mathbf{H}_2$ is the subgroup contained in $\mathbf{H}_1$ and $\mathbf{H}_2$ and is the subgroup that contains every subgroup of $\mathbf{G}$ contained in both $\mathbf{H}_1$ and $\mathbf{H}_2$.

**3.** The union of two subgroups of a group need not be a subgroup of the group.

***(O.U. 0 2001/0, N.U. O 92, K.U. 2004, M96, S.K.V. A 97)***

**e.g.** Let $(\mathbf{Z}, +)$ be the group of all integers.

Let $\mathbf{H}_1 = \{\ldots -6, -4, -2, 0, 2, 4 \ldots\} = 2\,\mathbf{Z}$ and

$\mathbf{H}_2 = \{\ldots -12, -9, -6, -3, 0, 3, 6, 9 \ldots\} = 3\,\mathbf{Z}$ be two subgroups of $\mathbf{Z}$.

We have $\mathbf{H}_1 \cup \mathbf{H}_2 = \{\ldots, -12, -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9 \ldots\}$

Since $4 \in \mathbf{H}_1 \cup \mathbf{H}_2$, $3 \in \mathbf{H}_1 \cup \mathbf{H}_2$ does not imply $4 + 3 \in \mathbf{H}_1 \cup \mathbf{H}_2$, $\mathbf{H}_1 \cup \mathbf{H}_2$ is not closed under +.

$\therefore$ $\mathbf{H}_1 \cup \mathbf{H}_2$ is not a subgroup of $(\mathbf{Z}, +)$.

So the intersection of two subgroups of a group is a subgroup of the group whereas the union of two subgroups of a group need not be a subgroup of the group.

Thus we conclude : An arbitrary intersection of subgroups of a group $\mathbf{G}$ is a subgroup but union of subgroups need not be a subgroup. ***(O.U. O 98)***

**Theorem 15.** ***The union of two subgroups of a group is a subgroup iff one is contained in the other.*** ***(A. U. M 12, N.U. S 93, S.V.U. 01, S. K. U. M 09)***

**Proof.** Let $\mathbf{H}_1$ and $\mathbf{H}_2$ be two subgroups of a group $(\mathbf{G}, .)$

To prove that $\mathbf{H}_1 \cup \mathbf{H}_2$ is a subgroup $\Leftrightarrow \mathbf{H}_1 \subseteq \mathbf{H}_2$ or $\mathbf{H}_2 \subseteq \mathbf{H}_1$.

**The condition is necessary.**

Let $\mathbf{H}_1 \subseteq \mathbf{H}_2$ $\quad\therefore\quad$ $\mathbf{H}_1 \cup \mathbf{H}_2 = \mathbf{H}_2$

Since $\mathbf{H}_2$ is a subgroup of $\mathbf{G}$, $\mathbf{H}_1 \cup \mathbf{H}_2$ is a subgroup of $\mathbf{G}$.

Similarly $\mathbf{H}_2 \subseteq \mathbf{H}_1 \Rightarrow \mathbf{H}_1 \cup \mathbf{H}_2$ is a subgroup of $\mathbf{G}$.

**The condition is sufficient.**

Let $\mathbf{H}_1 \cup \mathbf{H}_2$ be a subgroup of $\mathbf{G}$.

We prove that $\mathbf{H}_1 \subseteq \mathbf{H}_2$ or $\mathbf{H}_2 \subseteq \mathbf{H}_1$. Suppose that $\mathbf{H}_1 \not\subset \mathbf{H}_2$ and $\mathbf{H}_2 \not\subset \mathbf{H}_1$

Since $\mathbf{H}_1 \not\subset \mathbf{H}_2$, $\exists\ a \in \mathbf{H}_1$ and $a \notin \mathbf{H}_2$. …(1)

Again $\mathbf{H}_2 \not\subset \mathbf{H}_1 \Rightarrow \exists\ b \in \mathbf{H}_2$ and $b \notin \mathbf{H}_1$. …(2)

From (1) and (2) we have that $a \in \mathbf{H}_1 \cup \mathbf{H}_2$ and $b \in \mathbf{H}_1 \cup \mathbf{H}_2$.

Since $\mathbf{H}_1 \cup \mathbf{H}_2$ is a subgroup, we have $ab \in \mathbf{H}_1 \cup \mathbf{H}_2$.

$\therefore$ $ab \in \mathbf{H}_1$ or $ab \in \mathbf{H}_2$ or $ab \in \mathbf{H}_1 \cap \mathbf{H}_2$.

Suppose $ab \in \mathbf{H}_1$. Since $\mathbf{H}_1$ is a subgroup, $a \in \mathbf{H}_1$ and $ab \in \mathbf{H}_1$.

$\Rightarrow$ $a^{-1} \in \mathbf{H}_1$ and $ab \in \mathbf{H}_1 \Rightarrow a^{-1}(ab) \in \mathbf{H}_1$

$\Rightarrow (a^{-1}a)\,b \in \mathbf{H}_1 \Rightarrow eb \in \mathbf{H}_1 \Rightarrow b \in \mathbf{H}_1$ which is absurd by (2).

$\therefore$ $ab \notin \mathbf{H}_1$.

Similarly we can show that $ab \notin \mathbf{H}_2$. $\therefore$ $ab \notin \mathbf{H}_1 \cap \mathbf{H}_2$

$\therefore$ $ab \notin \mathbf{H}_1 \cup \mathbf{H}_2$ which is a contradiction that $\mathbf{H}_1 \cup \mathbf{H}_2$ is a group.

$\therefore$ we must have $\mathbf{H}_1 \subseteq \mathbf{H}_2$ or $\mathbf{H}_2 \subseteq \mathbf{H}_1$.

**Note.** $(\mathbf{Z}_{16}, +_{16})$ is a group. $\mathbf{S} = \{0,8\}, \mathbf{T} = \{0,4,8,12\}$ under $+_{16}$ are two groups. Clearly they are subgroups of $\mathbf{Z}_{16}$. Since $\mathbf{S} \cup \mathbf{T} = \{0,4,8,12\} = \mathbf{T}$, we have $(\mathbf{S} \cup \mathbf{T}, +_{16})$ as a subgroup of $\mathbf{Z}_{16}$. Observe that $\mathbf{S} \subset \mathbf{T}$ *i.e.* **S** is contained in **T**.

**Ex.6.** *Prove that set of all multiples of 3 is a sub group of the group of integers under aditon.* ***(A.N.U.M. 99)***

**Sol. :** Consider $3Z = \{3n / n \in \mathbf{Z}\}$

$3\mathbf{Z} \neq \phi$ and $3\mathbf{Z}$ is a subset of **Z**.

Let $3m, 3n \in 3\mathbf{Z} \Rightarrow m, n \in \mathbf{Z}$

$3m - 3n = 3(m-n) \in 3\mathbf{Z}$

$\therefore$ $(3\mathbf{Z}, +)$ is a sub group of $(\mathbf{Z}, +)$ (using Th.8)

**Note :** $nz = \{nx / x \in \mathbf{Z}\}$ os a sub group of $(\mathbf{Z}, +)$.

**Ex. 7.** ***G*** *is a group non-zero real numbers under multiplication. Prove that (i)* $\mathbf{H} = \{x \in \mathbf{G} / x = 1$ *or* $x$ *is irrational* $\}$ *(ii)* $\mathbf{K} = \{x \in \mathbf{G} / x \geq 1\}$ *are not subgroups of* ***G****.*

**Sol. :** (i) $\sqrt{2}, \sqrt{2} \in \mathbf{H}$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin \mathbf{H}$.

So **H** is not a sub group even though $\mathbf{H} \subset \mathbf{G}$.

(ii) 1 is the identity in **G** and $\mathbf{K} \subset \mathbf{G}$.

$2 \in \mathbf{K}$ but $2^{-1} = (1/2) \notin \mathbf{K}$. So **K** is not a subgroup.

**Ex. 8.** $(\mathbf{Z}_6 = \{0,1,2,3,4,5\}, +_6)$ *is a group. Prove that* $\mathbf{S} = \{0,2,4\}$, $\mathbf{T} = \{0,3\}$ *are subgroups of* $\mathbf{Z_6}$ *and* $\mathbf{S} \cup \mathbf{T}$ *is not a subgroup of* $\mathbf{Z_6}$.

**Sol. :** $\mathbf{S} = \{0,2,4\}, \mathbf{T} = \{0,3\}$ are subsets of $\mathbf{Z_6}$ and

From the tables 0 is the identity

| $+_6$ | 0 | 2 | 4 |
|---|---|---|---|
| 0 | 0 | 2 | 4 |
| 2 | 2 | 4 | 0 |
| 4 | 4 | 0 | 2 |

(*i*)

| $+_6$ | 0 | 3 |
|---|---|---|
| 0 | 0 | 3 |
| 3 | 3 | 0 |

(*ii*)

(i) $0^{-1} = 0, 2^{-1} = 4, 4^{-1} = 2$

(ii) $0^{-1} = 0, 3^{-1} = 3$

Clearly $(\mathbf{S}, +_6), (\mathbf{T}, +_6)$ are subgroups of $\mathbf{Z_6}$.

Now $\mathbf{S} \cup \mathbf{T} = \{0,2,3,4\}$ is not a subgroup of $\mathbf{Z_6}$ as $1,5 \notin \mathbf{S} \cup \mathbf{T}$.

## EXERCISE 3

1. Show that all the subgroups of an abelian group are abelian.
2. If $e$ is the identity in a group **G**, show that for all the subgroups of **G**, $e$ is the identity.
3. Can an abelian group have a non-abelian subgroup? Can a non-abelian group have an abelian subgroup?

**4.** Show that the set of all elements $a$ of an abelian group $\mathbf{G}$ which satisfy $a^2 = e$ forms a subgroup of $\mathbf{G}$. ***(N.U. O 90)***

**5.** Let $(\mathbf{G}, .)$ be an abelian group and $\mathbf{H}, \mathbf{K}$ be two subgroups of $\mathbf{G}$. Show that $\mathbf{HK}$ is a subgroup of $\mathbf{G}$.

**6.** Let $\mathbf{H}$ be a finite non-empty subset of a group $\mathbf{G}$. Prove that $\mathbf{H}$ is a subgroup of $\mathbf{G}$ iff $\mathbf{HH} \subset \mathbf{H}$.

**7.** If $\mathbf{G}$ is a group and $\mathbf{N}(a) = \{x \in \mathbf{G} / ax = xa\}$ for $a \in \mathbf{G}$, then prove that $\mathbf{N}(a)$ is a subgroup of $\mathbf{G}$. ***(K. U. 08, S.K.U. O 00)***

**8.** Let $a$ be an element of a group $\mathbf{G}$. The set $\mathbf{H} = \{a^n \mid n \in \mathbf{Z}\}$ is a subgroup of $\mathbf{G}$. If $\mathbf{K}$ is a subgroup of $\mathbf{G}$ and $a \in \mathbf{K}$, then prove that $\mathbf{H} \subset \mathbf{K}$.

**9.** If $\mathbf{G} = \{1, -1, i, -i\}$ is a group under multiplication then write all the subgroups of $\mathbf{G}$. ***(N.U. 95)***

**10.** Prove that $\{\mathbf{Q}, +\}$ is a subgroup of $\{\mathbf{R}, +\}$ and $(\mathbf{R} - \mathbf{Q}, +)$ is not. ***(N.U. 99)***

**ANSWERS**

**3.** No; Yes **9.** $\{1\}, \{1, -1\}, \{1, -1, i, -i\}$

# Cosets and Lagrange's Theorem

## 4.1. COSETS

**Definition.** Let $(\mathbf{H}, .)$ be a subgroup of the group $(\mathbf{G}, .)$.

Let $a \in \mathbf{G}$. Then the set $a\mathbf{H} = \{ah \mid h \in \mathbf{H}\}$ is called a **left coset** of $\mathbf{H}$ in $\mathbf{G}$ generated by $a$ and the set $\mathbf{H}a = \{ha \mid h \in \mathbf{H}\}$ is called a **right coset** of $\mathbf{H}$ in $\mathbf{G}$ generated by $a$. Here the operation in G is denoted multiplicatively. Also $a\mathbf{H}, \mathbf{H}a$ are called **cosets of H** generated by $a$ in $\mathbf{G}$. ***(A.N.U.J 04, B.A., O 90, O. U. A12)***

Since every element of $a\mathbf{H}$ or $\mathbf{H}a$ is in $\mathbf{G}$, $a\mathbf{H}$ and $\mathbf{H}a$ are complexes of $\mathbf{G}$.

If $e$ is the identity in $\mathbf{G}$, then $e\mathbf{H} = \{eh \mid h \in \mathbf{H}\} = \{h \mid h \in \mathbf{H}\} = \mathbf{H}$

and $\mathbf{H}e = \{he \mid h \in \mathbf{H}\} = \mathbf{H}$. Hence the subgroup of $\mathbf{G}$ is itself a left and a right coset of $\mathbf{H}$ in $\mathbf{G}$.

If $e$ is the identity in $\mathbf{G}$, it is also the identity in $\mathbf{H}$. Therefore, for $a \in \mathbf{G}, e \in \mathbf{H}$ we have $ea \in \mathbf{H}a$ and $ae \in a\mathbf{H}$. Hence the left coset or the right coset of $\mathbf{H}$ generated by $a$ is non-empty. Further $a \in \mathbf{H}a, a \in a\mathbf{H}$ and $\mathbf{H}a \cap a\mathbf{H} \neq \phi$.

If the group $\mathbf{G}$ is abelian, then for every $h \in \mathbf{H}$, we shall have $ah = ha$. Hence $a\mathbf{H} = \mathbf{H}a$. However, even if $\mathbf{G}$ is not abelian, also we may have $a\mathbf{H} = \mathbf{H}a$ or $a\mathbf{H} \neq \mathbf{H}a$.

**Note 1.** Left or right coset of any subgroup in a group is called **residue class modulo the subgroup of the group.**

**2.** If the operation in $\mathbf{G}$ is denoted additively, then the left subset of $\mathbf{H}$ in $\mathbf{G}$ generated by $a$, denoted by $a + \mathbf{H}$ is $\{a + h \mid h \in \mathbf{H}\}$ i.e. $a + \mathbf{H} = \{a + h \mid h \in \mathbf{H}\}$.

Similarly the right coset of $\mathbf{H}$ is $\mathbf{G}$ generated by $a$.

$$= \mathbf{H} + a = \{h + a \mid h \in \mathbf{H}\}.$$

**3.** Let $\mathbf{H}$ be a subgroup of the group $\mathbf{G}$ and $a, b \in \mathbf{G}$. Then (i) $a(b\mathbf{H}) = (ab)\mathbf{H}$ and $(\mathbf{H}b)a = \mathbf{H}(ba)$.

(ii) $x \in a\mathbf{H} \Rightarrow yx \in y(a\mathbf{H})$ for $y \in \mathbf{G} \Rightarrow yx \in (ya)\mathbf{H}$.

**4.** The element $a$ is called the coset representative of $a\mathbf{H}$ $(\mathbf{H}a)$.

$|a\mathbf{H}|, |\mathbf{H}a|$ denote the number of elements in $a\mathbf{H}, \mathbf{H}a$ respectively.

**e.g. 1.** Consider the group of symmetries of the square (Ex. 17 of chapter 2) *i.e.* $(\mathbf{D}_4, o)$ where $\mathbf{D}_4 = \{r_{90}, r_{180}, r_{360}, x, y, d_1, d_2\}$.

$(\mathbf{H}, o)$ where $\mathbf{H} = \{r_{180}, r_{360}, x, y\}$ is a subgroup of $(\mathbf{D}_4, o)$. Then all the left cosets of $\mathbf{H}$ in $\mathbf{G}$ are $r_{90}\mathbf{H} = \{r_{90} o\, r_{180}, r_{90} o\, r_{360}, r_{90} o\, x, r_{90} o\, y\} = \{r_{270}, r_{90}, d_2, d_1\}$

$r_{180}\mathbf{H} = \{r_{180} o\, r_{180},\ r_{180} o\, r_{360},\ r_{180} o\, x,\ r_{180} o\, y\}$ $= \{r_{360},\ r_{180},\ x,\ y\} = \mathbf{H}$

$r_{270}\mathbf{H} = \{r_{270} o\, r_{180}, \ldots\ldots\}$ $= \{r_{90},\ r_{270},\ d_1,\ d_2\}$

$r_{360}\mathbf{H} = \{r_{360} o\, r_{180}, \ldots\ldots\}$ $= \{r_{180},\ r_{360},\ x,\ y\} = \mathbf{H}$

$x\mathbf{H} = \{x o\, r_{180}, \ldots\ldots\}$ $= \{x,\ y,\ r_{360},\ r_{180}\} = \mathbf{H}$

$y\mathbf{H} = \{y o\, r_{180}, \ldots\ldots\}$ $= \{x,\ y,\ r_{180},\ r_{360}\} = \mathbf{H}$

$d_1\mathbf{H} = \{d_1 o\, r_{180}, \ldots\ldots\}$ $= \{d_2,\ d_1,\ r_{270},\ r_{90}\}$

$d_2\mathbf{H} = \{d_2 o\, r_{180}, \ldots\ldots\}$ $= \{d_1,\ d_2,\ r_{90},\ r_{270}\}$

We have two distinct left cosets, namely, $\{r_{90},\ r_{270},\ d_1,\ d_2\}$ and $\{r_{180},\ r_{360},\ x,\ y\} = \mathbf{H}$

These two may be taken as $r_{90}\mathbf{H}$ and $\mathbf{H}$.

Obviously $r_{90}\mathbf{H} \cap \mathbf{H} = \phi$ and $r_{90}\mathbf{H} \cup \mathbf{H} = \mathbf{D}_4$.

Similarly we can have all the right cosets of $\mathbf{H}$ in $\mathbf{D}_4$.

**Note.** If $a \in \mathbf{H}$, then $a\mathbf{H} = \mathbf{H} = \mathbf{H}a$.

**e.g. 2.** Let $\mathbf{G}$ be the additive group of integers.

Now $\mathbf{G} = \{\ldots\ldots -3, -2, -1, 0, 2, 3, \ldots\ldots\}$ and $0$ is the identity in $\mathbf{G}$.

Also $\mathbf{G}$ is abelian.

Let $\mathbf{H}$ be a subset of $\mathbf{G}$ where elements of $\mathbf{H}$ are obtained by multiplying each element of $\mathbf{G}$ by 3 (say) i.e.,

$$\mathbf{H} = \{\ldots\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\ldots\}$$

Clearly $\mathbf{H}$ is a subgroup of $(\mathbf{G}, +)$. $(\because\ n_1, n_2 \in \mathbf{H} \Rightarrow n_1 - n_2 \in \mathbf{H})$

Since $\mathbf{G}$ is abelian, left coset of $\mathbf{H}$ of an element in $\mathbf{G}$ = right coset of $\mathbf{H}$ in $\mathbf{G}$.

$\therefore\quad 0 + \mathbf{H} = \mathbf{H} = \{\ldots\ldots -9, -6, -3, 0, 3, 6, \ldots\ldots\}$

Since $1 \in \mathbf{G}$, $1 + \mathbf{H} = \{\ldots\ldots, -8, -5, -2, 1, 4, 7, \ldots\ldots\}$

Since $2 \in \mathbf{G}$, $2 + \mathbf{H} = \{\ldots\ldots, -7, -4, -1, 2, 5, 8, \ldots\ldots\}$

Observe that (i) $3 + \mathbf{H} = 6 + \mathbf{H} = \ldots\ldots = 0 + \mathbf{H}$,

$4 + \mathbf{H} = 7 + \mathbf{H} = \ldots\ldots = 1 + \mathbf{H}$,

$5 + \mathbf{H} = 8 + \mathbf{H} = \ldots\ldots = 2 + \mathbf{H}$.

(ii) $0 + \mathbf{H}$, $1 + \mathbf{H}$, $2 + \mathbf{H}$ are disjoint.

(iii) $0 + \mathbf{H} \cup 1 + \mathbf{H} \cup 2 + \mathbf{H} = \mathbf{G}$

## 4.2. PROPERTIES OF COSETS

**Theorem 1.** $\mathbf{H}$ *is any subgroup of a group* $(\mathbf{G}, .)$ *and* $h \in \mathbf{G}$. *Then* $h \in \mathbf{H}$ *iff* $h\mathbf{H} = \mathbf{H} = \mathbf{H}h$. *(S.K.U. 0 2002)*

**Proof.** (i) $h \in \mathbf{H}$ to prove that $h\mathbf{H} = \mathbf{H} = \mathbf{H}h$.

Let $h'$ be an arbitrary element of $\mathbf{H}$. Then $hh'$ is an arbitrary element of $h\mathbf{H}$. Since $\mathbf{H}$ is a subgroup of $\mathbf{G}, h, h' \in \mathbf{H} \Rightarrow hh' \in \mathbf{H}$

Thus every element of $h\mathbf{H}$ is also an element of $\mathbf{H}$.

$\therefore\quad h\mathbf{H} \subseteq \mathbf{H}$ …(1)

Again $h' = eh' = (hh^{-1})\, h' = h\,(h^{-1}h') \in h\mathbf{H}$

[$\therefore\ e$ is the identity in $\mathbf{H}$, $h \in \mathbf{H} \Rightarrow h^{-1} \in \mathbf{H}$ and $h^{-1} \in \mathbf{H}$, $h' \in \mathbf{H} \Rightarrow h^{-1}h' \in \mathbf{H}$ ]

$\therefore\quad \mathbf{H} \subseteq h\mathbf{H}$. …(2)

$\therefore$ From (1) and (2), $h\mathbf{H} = \mathbf{H}$.

Similarly we can prove $\mathbf{H} = \mathbf{H}h$.

$\therefore\ h \in \mathbf{H}$. $\therefore\ h\mathbf{H} = \mathbf{H} = \mathbf{H}h$.

(ii) Let $h\mathbf{H} = \mathbf{H} = \mathbf{H}h$. To prove that $h \in \mathbf{H}$.

Now $h \in \mathbf{G}$. Since $h = he, h \in h\mathbf{H}$.

But $h\mathbf{H} = \mathbf{H}$ $\therefore\ h \in \mathbf{H}$.

Similarly $\mathbf{H}h = \mathbf{H} \Rightarrow h \in \mathbf{H}$ $\therefore$ $h\mathbf{H} = \mathbf{H} = \mathbf{H}h \Rightarrow h \in \mathbf{H}$

**Theorem 2.** *If $a, b$ are any two elements of a group $(\mathbf{G}, .)$ and $\mathbf{H}$ any subgroup of $\mathbf{G}$, then $\mathbf{H}a = \mathbf{H}b \Leftrightarrow ab^{-1} \in \mathbf{H}$ and $a\mathbf{H} = b\mathbf{H} \Leftrightarrow a^{-1}b \in \mathbf{H}$.*
*(O.U.O 03, S.K.U. M 11, M 03, A97, A.N.U.J 04)*

**Proof.** $a \in \mathbf{H}a, \mathbf{H}a = \mathbf{H}b \Rightarrow a \in \mathbf{H}b \Rightarrow ab^{-1} \in (\mathbf{H}b)b^{-1}$.

$\Rightarrow ab^{-1} \in \mathbf{H}(bb^{-1}) \Rightarrow ab^{-1} \in \mathbf{H}e \Rightarrow ab^{-1} \in \mathbf{H}$.

Now $ab^{-1} \in \mathbf{H}ab^{-1} = \mathbf{H} \Rightarrow \mathbf{H}ab^{-1}b = \mathbf{H}b$

$\Rightarrow \mathbf{H}a(b^{-1}b) = \mathbf{H}b \Rightarrow \mathbf{H}ae = \mathbf{H}b \Rightarrow \mathbf{H}a = \mathbf{H}b$.

Similarly we can prove that $a\mathbf{H} = b\mathbf{H} \Leftrightarrow a^{-1}b \in \mathbf{H}$

**Note.** If $ab^{-1} \in \mathbf{H}$ then $(ab^{-1})^{-1} \in \mathbf{H} \Rightarrow (b^{-1})^{-1}a^{-1} \in \mathbf{H} \Rightarrow ba^{-1} \in \mathbf{H}$

Similarly $a^{-1}b \in \mathbf{H} \Rightarrow b^{-1}a \in \mathbf{H}$.

**Theorem 3.** *If $a, b$ are any two elements of a group $\mathbf{G}$ and $\mathbf{H}$ any subgroup of $\mathbf{G}$, then $a \in b\mathbf{H} \Leftrightarrow a\mathbf{H} = b\mathbf{H}$ and $a \in \mathbf{H}b \Leftrightarrow \mathbf{H}a = \mathbf{H}b$* *(A.N.U.M.98, O 98)*

**Proof.** $a \in b\mathbf{H} \Rightarrow b^{-1}a \in b^{-1}b\mathbf{H}$

$\Rightarrow b^{-1}a \in e\mathbf{H} \Rightarrow b^{-1}a \in \mathbf{H} \Rightarrow b^{-1}a\mathbf{H} = \mathbf{H} \Rightarrow bb^{-1}a\mathbf{H} = b\mathbf{H} \Rightarrow a\mathbf{H} = b\mathbf{H}$

Converse : Let $a\mathbf{H} = b\mathbf{H}$

$\therefore\ a \in a\mathbf{H} \Rightarrow a \in b\mathbf{H}$ Similarly other result can be proved.

**Theorem 4.** *Any two left (right) cosets of a subgroup are either disjoint or identical.* *(B.A.) (N.U. O 90, A 93, 95, O.U. O 98, A.N.U.J 04, S 02, K.U.J 03, A 02, A98, O97, A97)*

**Proof.** Let $\mathbf{H}$ be a subgroup of a group $\mathbf{G}$. Let $a\mathbf{H}$ and $b\mathbf{H}$ be two left cosets of $\mathbf{H}$ in $\mathbf{G}$. If $a\mathbf{H}$ and $b\mathbf{H}$ are disjoint, there is nothing to prove. If $a\mathbf{H} \cap b\mathbf{H} \neq \phi$, then there exists at least one element $c$ such that $c \in a\mathbf{H}$ and $c \in b\mathbf{H}$. Let $c = ah_1$ and $c = bh_2$ where $h_1, h_2 \in \mathbf{H}$.

$\therefore\ ah_1 = bh_2 \Rightarrow ah_1h_1^{-1} = bh_2h_1^{-1} \Rightarrow ae = b(h_2\, h_1^{-1}) \Rightarrow a = b(h_2\, h_1^{-1})$

Since $\mathbf{H}$ is a subgroup, $h_2\, h_1^{-1} \in \mathbf{H}$. Let $h_3 = h_2\, h_1^{-1}$

$\therefore\ h_3 \in \mathbf{H}$. Now $a = bh_3$

$\therefore\ a\mathbf{H} = bh_3\mathbf{H} = b\mathbf{H}$ $(\because\ h_3 \in \mathbf{H} \Rightarrow h_3\mathbf{H} = \mathbf{H})$

Two left cosets are identical if they are not disjoint.

$\therefore\ a\mathbf{H} \cap b\mathbf{H} = \phi$ or $a\mathbf{H} = b\mathbf{H}$.

Similarly we can prove that $\mathbf{H}a \cap \mathbf{H}b = \phi$ or $\mathbf{H}a = \mathbf{H}b$.

**Cor.** $\mathbf{H}$ is any subgroup of a group $\mathbf{G}$. If the cosets $a\mathbf{H}$, $b\mathbf{H}$, $c\mathbf{H}$, … are all disjoint, then $\mathbf{G} = \mathbf{H} \cup a\mathbf{H} \cup b\mathbf{H} \cup c\mathbf{H} \ldots$ where $\mathbf{H}$ is the coset corresponding to the identity element in $\mathbf{G}$. *(O.U. O 98)*

Also $\mathbf{G} = \mathbf{H} \cup \mathbf{H}a \cup \mathbf{H}b \cup \mathbf{H}c \cup \ldots$

## 4.3. CONGRUENCE MODULO H

**Definition.** Let $(\mathbf{G},.)$ be a group and $(\mathbf{H},.)$ be a subgroup of $\mathbf{G}$. For $a,b\in\mathbf{G}$, if $b^{-1}a\in\mathbf{H}$ we say that $a\equiv b \pmod{\mathbf{H}}$. *(O.U.O. 03)*

**Theorem 5.** *If $\mathbf{H}$ is a subgroup of group $\mathbf{G}$, for $a,b\in\mathbf{G}$ the relation $a\equiv b \pmod{\mathbf{H}}$ is an equivalence relation. (A.N.U. 03, A.U.A. 01, K.U.A 00, O.U. O 03)*

**Proof.** (i) **Reflexive :** Let $e$ be the identity in $(\mathbf{G},.)$.

Since $\mathbf{H}$ is a subgroup of $\mathbf{G}$, $e$ is the identity in $\mathbf{H}$.

Let $a\in\mathbf{G}$. Since $a^{-1}a=e$, we have $a^{-1}a\in\mathbf{H}$.

$\therefore a\equiv a \pmod{\mathbf{H}} \Rightarrow$ relation is reflexive.

(ii) **Symmetric :** Let $a\equiv b \pmod{\mathbf{H}}$ for $a,b\in\mathbf{G}$.

$\therefore b^{-1}a\in\mathbf{H}\Rightarrow (b^{-1}a)^{-1}\in\mathbf{H}\Rightarrow a^{-1}b\in\mathbf{H}\Rightarrow b\equiv a \pmod{\mathbf{H}}\Rightarrow$ relation is symmetric.

(iii) **Transitive :** Let $a\equiv b \pmod{\mathbf{H}}$ and $b\equiv c \pmod{\mathbf{H}}$ for $a,b,c\in\mathbf{G}$.

$\therefore\ b^{-1}a\in\mathbf{H}$ and $c^{-1}b\in\mathbf{H}\Rightarrow (c^{-1}b)(b^{-1}a)\in\mathbf{H}$

$\Rightarrow c^{-1}(bb^{-1})a\in\mathbf{H}\Rightarrow c^{-1}(ea)\in\mathbf{H}$

$\Rightarrow c^{-1}a\in\mathbf{H}\Rightarrow a\equiv c \pmod{\mathbf{H}}\Rightarrow$ relation is transitive.

Since the congruence modulo $\mathbf{H}$ is reflexive, symmetric and transitive, it is an equivalence relation.

**Note :** Let $\mathbf{H}$ be a subgroup of group G and $a\in$ G, then the equalence class containing $a$ w.r.t. the equivalence relation ($\equiv \bmod \mathbf{H}$) is denoted by $\bar{a}$.

**Theorem 6.** *Let $(\mathbf{H},.)$ be a subgroup of a group $(\mathbf{G},.)$. For $a\in\mathbf{G}$, let the equivalence class $\bar{a}=\{x\in\mathbf{G}/\,x\equiv a \pmod{\mathbf{H}}\}$. Then $\bar{a}=a\mathbf{H}$. (N.U.J 03, S.K.U 02)*

**Proof.** To prove that $\bar{a}=a\mathbf{H}$

Let $e$ be the identity in $\mathbf{G}$. $\therefore$ $e$ is also the identity in $\mathbf{H}$.

$$
\begin{aligned}
x\in\bar{a} &\Leftrightarrow x\equiv a \pmod{\mathbf{H}}\\
&\Leftrightarrow a^{-1}x\in\mathbf{H}\\
&\Leftrightarrow a^{-1}x=h\in\mathbf{H} \text{ for some } h\in\mathbf{H}\\
&\Leftrightarrow a(a^{-1}x)=ah\in a\mathbf{H} \text{ for some } h\in\mathbf{H}\\
&\Leftrightarrow (aa^{-1})x=ah\in a\mathbf{H} \text{ for some } h\in\mathbf{H}\\
&\Leftrightarrow ex=ah\in a\mathbf{H} \text{ for some } h\in\mathbf{H}\\
&\Leftrightarrow x=ah\in a\mathbf{H} \text{ for some } h\in\mathbf{H}\\
&\Leftrightarrow x\in a\mathbf{H}. \qquad \therefore \bar{a}=a\mathbf{H}.
\end{aligned}
$$

**Note 1.** The equivalence relation $a\equiv b \pmod{\mathbf{H}}$ induces a partition in $\mathbf{G}$ which is nothing but the left coset decomposition of $\mathbf{G}$. w.r.t. $\mathbf{H}$. No left coset of $\mathbf{H}$ in $\mathbf{G}$ will be empty. Every element of $\mathbf{G}$ belongs to one and only one left coset of $\mathbf{G}$.

**2.** The relation in $\mathbf{G}$, defined by $a\equiv b \pmod{\mathbf{H}}$ if $ab^{-1}\in\mathbf{H}$, is an equivalence relation. This relation induces a partition in $\mathbf{G}$ which is nothing but the right coset decomposition of $\mathbf{G}$.

**Theorem 7.** *Let $(\mathbf{H},.)$ be a subgroup of a group $(\mathbf{G},.)$. Then there exists a bijection between any two left cosets of $\mathbf{H}$ in $\mathbf{G}$. (A.U.S. 00, M99, S99)*

**Proof.** Let $a\mathbf{H}, b\mathbf{H}$ be two left cosets of $\mathbf{H}$ for $a,b\in\mathbf{G}$.

Define $f : a\mathbf{H} \to b\mathbf{H}$ such that $f(ah) = bh$ for $h \in \mathbf{H}$.

For $h_1, h_2 \in \mathbf{H}, ah_1, ah_2 \in a\mathbf{H}$ and $bh_1, bh_2 \in b\mathbf{H}$.

Now $f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2 \Rightarrow h_1 = h_2 \Rightarrow ah_1 = ah_2$.

$\therefore$ $f$ is $1-1$.

Now $bh \in b\mathbf{H} \Rightarrow \exists\ h \in \mathbf{H}$ such that $bh \in b\mathbf{H}$

$\Rightarrow \exists\ h \in \mathbf{H}$ such that $ah \in a\mathbf{H}$

$\therefore$ For $ah \in a\mathbf{H}$, $f(ah) = bh$ $\quad\therefore\quad$ $f$ is onto.

$\therefore$ $f$ is a bijection and there exists $1-1$ correspondence between any two left cosets of $\mathbf{H}$ in $\mathbf{G}$.

**Note 1.** Let $\mathbf{H}$ be a subgroup of a finite group $\mathbf{G}$. Since there is $1-1$ correspondence between any two left cosets of $\mathbf{H}$, every left coset has the same number of elements including $\mathbf{H}$ ($\because$ $\mathbf{H}$ is also a left coset).

**2.** The above theorem can be proved between two right cosets. Also every right coset of $\mathbf{H}$ of a finite group $\mathbf{G}$ has the same number of elements including $\mathbf{H}$.

($\because$ $\mathbf{H}$ is also a right coset).

**Theorem 8.** ***If $\mathbf{H}$ is a subgroup of a group $\mathbf{G}$, then there is one to one correspondence between the set of all distinct left cosets of $\mathbf{H}$ in $\mathbf{G}$ and the set of all distinct right cosets of $\mathbf{H}$ in $\mathbf{G}$.*** ***(N.U. S 93, S.V.U. A 01, S.K.U. 01/0, A.N.U.M 00, S93, K.U.S 01, O.U.M 03)***

**Proof.** In $\mathbf{G}$, let $\mathbf{G}_1$ = the set of all distinct left cosets

and $\mathbf{G}_2$ = the set of all distinct right cosets.

Define a mapping $f : \mathbf{G}_1 \to \mathbf{G}_2$ such that $f(a\mathbf{H}) = \mathbf{H}a^{-1}$ $\forall$ $a \in \mathbf{G}$

For : Let $a\mathbf{H}, b\mathbf{H} \in \mathbf{G}_1$.

Now $a\mathbf{H} = b\mathbf{H} \Rightarrow b^{-1}a \in \mathbf{H} \Rightarrow (b^{-1}a)^{-1} \in \mathbf{H}$

$\Rightarrow a^{-1}(b^{-1})^{-1} \in \mathbf{H} \Rightarrow \mathbf{H}a^{-1} = \mathbf{H}b^{-1} \quad \Rightarrow f(a\mathbf{H}) = f(b\mathbf{H})$

***f* is one-one :** Let $a\mathbf{H}, b\mathbf{H} \in \mathbf{G}_1$

$\therefore$ $f(a\mathbf{H}) = f(b\mathbf{H}) \Rightarrow \mathbf{H}a^{-1} = \mathbf{H}b^{-1}$

$\Rightarrow a^{-1}(b^{-1})^{-1} \in \mathbf{H} \Rightarrow a^{-1}b \in \mathbf{H} \Rightarrow (a^{-1}b)^{-1} \in \mathbf{H}$

$\Rightarrow b^{-1}a \in \mathbf{H} \Rightarrow a\mathbf{H} = b\mathbf{H}$ $\quad\therefore\quad$ $f$ is $1-1$.

***f* is onto :** Let $\mathbf{H}a \in \mathbf{G}_2$. Since $a \in \mathbf{G}, a^{-1} \in \mathbf{G}$

$\therefore$ $a^{-1}\mathbf{H} \in \mathbf{G}_1$ and $f(a^{-1}\mathbf{H}) = \mathbf{H}(a^{-1})^{-1} = \mathbf{H}a$ $\quad\therefore\quad$ $f$ is onto.

There is one to one correspondence between $\mathbf{G}_1$ and $\mathbf{G}_2$.

**Note 1.** If $\mathbf{H}$ is a subgroup of a finite group $\mathbf{G}$, then the number of distinct left cosets of $\mathbf{H}$ in $\mathbf{G}$ is the same as the number of distinct right cosets of $\mathbf{H}$ in $\mathbf{G}$.

**2.** Since $\mathbf{H}$ is common to both the set of left cosets of $\mathbf{H}$ of a finite group $\mathbf{G}$ and the set of right cosets of $\mathbf{H}$ of the finite group $\mathbf{G}$, the number of elements in a left coset of $\mathbf{H}$ is equal to the number of elements in a right coset of $\mathbf{H}$.

**Index of a subgroup of a finite group.**

**Definition.** If $\mathbf{H}$ is a subgroup of a finite group $\mathbf{G}$, then the number of distinct left (right) cosets of $\mathbf{H}$ in $\mathbf{G}$ is called the index of $\mathbf{H}$ in $\mathbf{G}$. It is denoted by $(\mathbf{G} : \mathbf{H})$ or $i_{\mathbf{G}}(\mathbf{H})$

*(K.U. M 12, M 05, M01, S.V.U. A 93)*

## 4.4. LANGRANGE'S THEOREM

**Theorem 9.** ***The order of a subgroup of a finite group divides the order of the group.*** *(S.V.U. M11, A 02, O 01, O 00, A 97, O98, S 00, S.K.U. M 09, O 03, M 02, O 00, O97, A.N.U.M 05, J 04, J 03, M 02, S 01, S 00, S 99, S 97, S 96, M 96, A 93, A 90, A 85, A.U.M. 05, A 03, A 02, M 00, S 99, S 97, S 96, A 96, K.U. M 11, M 08, J 03, M 01, S 00, O99, A97, O96, O.U.M. 05, O99, A99)*

**Proof.** Since $\mathbf{H}$ is a subgroup of a finite group $\mathbf{G}$, $\mathbf{H}$ is finite.

(i) If $\mathbf{H} = \mathbf{G}$, then $\mathbf{O}(\mathbf{H}) / \mathbf{O}(\mathbf{G})$

(ii) If $\mathbf{H} \neq \mathbf{G}$, let $\mathbf{O}(\mathbf{G}) = n$ and $\mathbf{O}(\mathbf{H}) = m$

We know that every right coset of $\mathbf{H}$ in $\mathbf{G}$ has the same number of elements and the number of right cosets of $\mathbf{H}$ in $\mathbf{G}$ is finite.

Also since $\mathbf{H} = \mathbf{H}e, \mathbf{H}$ is a right coset of $\mathbf{H}$ in $\mathbf{G}$.

$\therefore$ If $\mathbf{H}a, \mathbf{H}b, \mathbf{H}c, \ldots\ldots$ are right cosets of $\mathbf{H}$ in $\mathbf{G}$, then

$$\mathbf{O}(\mathbf{H}a) = \mathbf{O}(\mathbf{H}b) = \mathbf{O}(\mathbf{H}c) = \ldots\ldots = \mathbf{O}(\mathbf{H}) = m$$

Let the number of distinct right cosets of $\mathbf{H}$ of $\mathbf{G}$ be $k$.

All these right cosets are disjoint and induce a partition of $\mathbf{G}$.

$\therefore$ $\mathbf{O}(\mathbf{G}) = \mathbf{O}(\mathbf{H}a) + \mathbf{O}(\mathbf{H}b) + \mathbf{O}(\mathbf{H}c) + \ldots\ldots + \mathbf{O}(\mathbf{H})$ ($k$ terms).

$$= m + m + m + \ldots + m \ (k \text{ times}) \Rightarrow n = km \Rightarrow k = \frac{n}{m}$$

$\therefore$ $\mathbf{O}(\mathbf{H})$ divides $\mathbf{O}(\mathbf{G})$ *i.e.* $\mathbf{O}(\mathbf{H}) / \mathbf{O}(\mathbf{G})$.

**Note 1.** Lagranage's theorem can also be proved by taking right cosets of $\mathbf{H}$ in $\mathbf{G}$.

**2.** Lagranage's theorem deals with finite groups only.

Let $\mathbf{O}(\mathbf{G}) = n$. If $m$ is not a divisor of $n$, then there can be no subgroup of $\mathbf{G}$ of order $m$.

**3.** Since $k = \frac{n}{m}$ number of distinct left (right) cosets of $\mathbf{H}$ in $\mathbf{G} = \frac{|\mathbf{G}|}{|\mathbf{H}|}$

$$= \frac{\text{order of the group } \mathbf{G}}{\text{order of the subgroup } \mathbf{H} \text{ of } \mathbf{G}} = \text{Index of } \mathbf{H} \text{ in } \mathbf{G} = (\mathbf{G} : \mathbf{H}).$$

**4.** Converse of Lagrange's theorem is not true.

(i) Consider $\mathbf{G} = \{1, -1, i, -i\}$. Clearly $\mathbf{G}$ is a group of order 4 w.r.t. multiplication. Since 2 is a divisor of 4 i.e. the order of the group $\mathbf{G}$, let us examine whether a complex $\mathbf{H}$ (of order 2) of $\mathbf{G}$, which is a subgroup of $\mathbf{G}$, exists.

Consider a complex $\mathbf{H}_1 = \{i, -i\}$. Since $-i \,.\, i = 1$ and since $1 \notin \mathbf{H}_1$. $\mathbf{H}_1$ is not a subgroup of $\mathbf{G}$.

Again consider a complex $\mathbf{H}_2 = \{1, -1\}$. Clearly $\mathbf{H}_2$ is a subgroup of $\mathbf{G}$.

$\therefore$ In conclusion, even if $m$ is a divisor of $n$, a subgroup of order $m$ in $\mathbf{G}$ need not exist.

(ii) Consider Ex. 16 of Chapter 2.

**G** is a finite group of order 6. Since 3 is a divisor of 6 i.e. the order of the group **G**, let us examine whether a complex **H** (of order 3) of **G**, which is a subgroup of **G**, exists.

Consider a complex $\mathbf{H}_1 = \{r_0, f_1, f_2\}$ of **G**. Since $f_1 o f_2 = r_1$ and since $r_1 \notin \mathbf{H}_1$, $\mathbf{H}_1$ is not a subgroup of **G**.

Again consider a complex $\mathbf{H}_2 = \{r_0, r_1, r_2\}$. Clearly $\mathbf{H}_2$ is a subgroup of **G** with identity $r_0$ and with $r_0^{-1} = r_0, r_1^{-1} = r_2$ and $r_2^{-1} = r_1$.

$\therefore$ In conclusion even if $m$ is a divisor of $n$, a subgroup of order $m$ in **G** need not exist. Thus the converse of Lagrange's Theorem does not hold.

**Cor. :** The order of an element of a finite group divides the order of the group. (Vide Th.2, Art 8.2)

**Theorem 10.** ***Suppose H and K are subgroups of a group G such that*** $\mathbf{K} \le \mathbf{H} \le \mathbf{G}$ ***and suppose*** $(\mathbf{H} : \mathbf{K})$ ***and*** $(\mathbf{G} : \mathbf{H})$ ***are both finite. Then*** $(\mathbf{G} : \mathbf{K})$ ***is finite, and*** $(\mathbf{G} : \mathbf{K}) = (\mathbf{G} : \mathbf{H})\,(\mathbf{H} : \mathbf{K})$ ***(K. U. M12)***

**Proof :** **H** and **K** are subgroups of a group **G** such that $\mathbf{K} \le \mathbf{H} \le \mathbf{G}$ and suppose $(\mathbf{H} : \mathbf{K})$ and $(\mathbf{G} : \mathbf{H})$ are both finite.

$(\mathbf{G} : \mathbf{H})$ = the index of subgroup **H** in **G** is the number of distinct left cosets of **H** in **G** and $(\mathbf{H} : \mathbf{K})$ = the index of subgroup **K** in **H** is the number of distinct left cosets of **K** in **H**.

Thus by Lagrange's Theorem :

$$(\mathbf{G} : \mathbf{H}) = \frac{|\mathbf{G}|}{|\mathbf{H}|} \text{ and } (\mathbf{H} : \mathbf{K}) = \frac{|\mathbf{H}|}{|\mathbf{K}|}$$

$$\therefore (\mathbf{G} : \mathbf{H})\,(\mathbf{H} : \mathbf{K}) = \frac{|\mathbf{G}|}{|\mathbf{H}|} \cdot \frac{|\mathbf{H}|}{|\mathbf{K}|} = \frac{|\mathbf{G}|}{|\mathbf{K}|} = (\mathbf{G} : \mathbf{K})$$

implying that $(\mathbf{G} : \mathbf{K})$ is finite and $(\mathbf{G} : \mathbf{K}) = (\mathbf{G} : \mathbf{H})\,(\mathbf{H} : \mathbf{K})$

**OR :**

Suppose that the collection of distinct left cosets of **H** in $\mathbf{G} = \{a_i\mathbf{H} : i = 1, 2, ....., r\}$ and the collection of distinct left cosets of **K** in $\mathbf{H} = \{b_j\mathbf{K} : j = 1, 2, ....., s\}$. Now we show that $\{a_i b_j \mathbf{K} : i = 1, 2, .....r, j = 1, 2, ...., s\}$ is the collection of distinct left cosets of K in G.

$$\mathbf{G} = \bigcup_{i=1 \text{ to } r} a_i\mathbf{H}, a_i \in \mathbf{G} \text{ and } \mathbf{H} = \bigcup_{i=1 \text{ to } s} b_j\mathbf{K}, b_j \in \mathbf{G}$$

Now $x \in \mathbf{G} \Rightarrow x \in \bigcup_i a_i\mathbf{H} \Rightarrow x = a_1 h, h \in \mathbf{H}$ and

$$h \in \mathbf{H} \Rightarrow h \in \bigcup_j b_j\mathbf{K} \Rightarrow h = b_j\mathbf{K}, k \in \mathbf{K}$$

$$\therefore\ x = a_i h = a_i b_j \mathbf{K}, k \in \mathbf{K} \Rightarrow x \in \bigcup_{i,j} a_i b_j \mathbf{K} \Rightarrow \mathbf{G} = \bigcup_{i,j} a_i b_j \mathbf{K}$$

Now we show $a_i b_j \mathbf{K} = a_{i'} b_{j'} \mathbf{K} \Leftrightarrow i = i', j = j'$

If $i = i', j = j'$, then $a_i b_j \mathbf{K} = a_{i'} b_{j'} \mathbf{K}$

If possible, $a_i b_j \mathbf{K} = a_{i'} b_{j'} \mathbf{K}$ when $i = i', j \neq j'$.

Then $b_j \mathbf{K} \cap b_{j'} \mathbf{K} = \phi \Rightarrow a_i b_j \mathbf{K} \cap a_{i'} b_{j'} \mathbf{K} = \phi$

$\Rightarrow$ it is a contradiction. $\therefore \; j = j'$

If possible, $a_i b_j \mathbf{K} = a_{i'} b_{j'} \mathbf{K}$ when $i \neq i', j = j'$.

Then $b_j \mathbf{K} = b_{j'} \mathbf{K}$ and $a_i \mathbf{H} \cap a_{i'} \mathbf{H} = \phi \Rightarrow a_i b_j \mathbf{K} \cap a_{i'} b_{j'} \mathbf{K} = \phi$

$\Rightarrow$ it is a contradiction. $\therefore \; i = i'$.

when $i \neq i', j = j', a_i \mathbf{H} \cap a_{i'} \mathbf{H} = \phi$ and

$b_i \mathbf{K} \cap b_i, \mathbf{K} = \phi \Rightarrow a_i b_j \mathbf{K} \cap a_{i'} b_{j'} \mathbf{K} = \phi$

$\therefore \; a_i b_j \mathbf{K} = a_{i'} b_{j'} \mathbf{K} \Leftrightarrow i = i', j = j'$

Thus **G** is the collection of distinct left cosets of **K** in **G**.

Hence (**G** : **K**) is finite and (**G** : **K**) = (**G** : **H**) (**H** : **K**)

**Theorem 11.** ***If*** $n$ ***is a positive integer and*** $a$ ***is an integer relatively prime to*** $n$ ***then*** $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$ ***where*** $\phi$ ***is the Euler's*** $\phi$***-function.***

(***Euler's*** $\phi$***-function.*** It is the function $\phi : Z^+ \to Z^+$ defined as (*i*) For $1 \in Z^+, \phi(1) = 1$ and (*ii*) for $n\,(>1) \in Z^+, \phi(n) =$ the number of positive integers less than $n$ and relatively prime to $n$.)

**Proof :** Let $x$ be any integer. Let $[x]$ denote the residue class of the set of integers mod $n$. **G** = {$[a]/a$ is an integer relatively prime to $n$}.

Then **G** is a group of order $\phi(n)$ with respect to multiplication of residue classes.

The identity in **G** is [1]

$[a] \in \mathbf{G} \Rightarrow [a]^{0(\mathbf{G})} = [1] \Rightarrow [a]^{\phi(n)} = [1] \Rightarrow [a\ a\ a \ldots . \text{ to } \phi((n) \text{ times}] = [1]$

$\Rightarrow [a^{\phi(n)}] = [1] \Rightarrow a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$

This theorem is known as *Euler's theorem.*

## 4.5. NORMALIZER OF AN ELEMENT OF A GROUP

**Definition.** If $a$ is an element of a group **G**, then the normalizer on $a$ in **G** is the set of all those elements of **G** which commute with $a$. The normalizer of $a$ in **G** is denoted by $\mathbf{N}(a)$ where $\mathbf{N}(a) = \{x \in \mathbf{G} / ax = xa\}$. ***(N.U. O 88, 2K)***

The normalizer $\mathbf{N}(a)$ is a subgroup of **G** (Refer Theorem .17 Chapter 5)

**Note.** If $e$ is the identity in group **G**, $ex = xe = x \;\forall\; x \in \mathbf{G} \;\Rightarrow\; \mathbf{N}(e) = \mathbf{G}$

**Ex. 1.** *Use Lagranage's Theorem to prove that a finite group cannot be expressed as the union of two of its proper subgroups.*

**Sol.** Let $\mathbf{G}$ be a finite group of order $n$. Assume that $\mathbf{H} \cup \mathbf{K} = \mathbf{G}$ where $\mathbf{H}, \mathbf{K}$ are two proper subgroups of $\mathbf{G}$.

Since $e \in \mathbf{H}$ and $e \in \mathbf{K}$ at least one of $\mathbf{H}, \mathbf{K}$ (say $\mathbf{H}$) must contain more that half the number of elements of $\mathbf{G}$.

Let $\mathbf{O}(\mathbf{H}) = p$

$\therefore \quad \frac{n}{2} < p < n \quad (\because \ \mathbf{H}$ is a proper subgroup of $\mathbf{G})$

$\therefore \quad n$ is not divisible by $p$ which contradicts Lagranage's theorem.

Hence our assumption that $\mathbf{H} \cup \mathbf{K} = \mathbf{G}$ is wrong.

$\therefore$ A finite group cannot be expressed as the union of two of its proper subgroups.

**Ex. 2.** *Show that two right cosets* $\mathbf{H}a, \mathbf{H}b$ *of a group* $\mathbf{G}$ *are distinct if and only if the two left cosets* $a^{-1}\mathbf{H}, b^{-1}\mathbf{H}$ *of* $\mathbf{G}$ *are distinct.* **(S. K. U. A 00)**

**Sol.** Suppose that $(\mathbf{H}a) = (\mathbf{H}b)$.

$$\mathbf{H}a = \mathbf{H}b \Leftrightarrow ab^{-1} \in \mathbf{H} \Leftrightarrow ab^{-1}\mathbf{H} = \mathbf{H} \Leftrightarrow a^{-1}ab^{-1}\mathbf{H} = a^{-1}\mathbf{H}$$
$$\Leftrightarrow b^{-1}\mathbf{H} = a^{-1}\mathbf{H} \Leftrightarrow a^{-1}\mathbf{H} = b^{-1}\mathbf{H}$$

$\therefore \quad \mathbf{H}a, \mathbf{H}b$ are distinct iff $a^{-1}\mathbf{H}$ and $b^{-1}\mathbf{H}$ are distinct.

**Ex. 3.** *Show that every finite group of prime order does not have any proper subgroup.*

**Sol.** Let $\mathbf{G}$ be a finite group of order $n$ where $n$ is prime.

If possible, let $\mathbf{H}$ be a subgroup of order $m$, say

Then $m \le n$. But by Lagrange's theorem $m$ is a divisor of $n$.

Also since $n$ is prime, either $m = 1$ or $m = n$.

$\therefore \quad \mathbf{H} = \{e\}$ or $\mathbf{H} = \mathbf{G}$. But these two are improper subgroups of $\mathbf{G}$.

$\therefore$ Any group of prime order does not have any proper subgroup.

**Note.** Thus the total number of subgroups of a group of prime order is 2.

**Ex. 4.** Vide Ex. 15 of Chapter 2.

$\mathbf{P}_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ is a non-abelian group over $\mathbf{S}$.

$\mathbf{H} = \{f_1, f_2\}$ is a subgroup of $\mathbf{P}_3$.

Let us form the left cosets of $\mathbf{H}$ in $\mathbf{P}_3$.

$$f_1\mathbf{H} = \mathbf{H}, \ f_2\mathbf{H} = \mathbf{H}, \ f_3\mathbf{H} = \mathbf{H} = \{f_3, f_6\}, \ f_4\mathbf{H} = \{f_4, f_5\}$$
$$f_5\mathbf{H} = \mathbf{H} = \{f_5, f_4\}, \ f_6\mathbf{H} = \{f_6, f_3\}$$

Thus we get only three distinct left cosets i.e. $\mathbf{H}, f_3\mathbf{H}, f_4\mathbf{H}$ of $\mathbf{H}$ in $\mathbf{P}_3$.

Thus $\mathbf{P}_3 = \mathbf{H} \cup f_3\mathbf{H} \cup f_4\mathbf{H}$ and index of subgroup $\mathbf{H}$ in $\mathbf{P}_3$ is 3.

Observe that the number of elements in each left coset is the same as in $\mathbf{H}$.

Further $f_3\mathbf{H} \neq \mathbf{H}f_3$ since $\mathbf{H}f_3 = \{f_3, f_5\}$.

We can observe similar results by taking all the right cosets of $\mathbf{H}$ in $\mathbf{G}$.

**Note.** $\mathbf{A}_3 = \{f_1, f_5, f_6\}$ is a commutative subgroup of $\mathbf{P}_3$.

Two distinct left cosets of $\mathbf{A}_3$ are $\mathbf{A}_3, f_2\mathbf{A}_3$ where $f_2\mathbf{A}_3 = \{f_2, f_3, f_4\}$.

Also $\mathbf{P}_2 = \mathbf{A}_3 \cup f_2\mathbf{A}_3$ and index of subgroup of $\mathbf{A}_3$ in $\mathbf{P}_3$ is 2.

**Ex. 5.** *Let* $\mathbf{H}$ *be a subgroup of a group* $\mathbf{G}$ *and let* $\mathbf{T} = \{x \in \mathbf{G} / x\mathbf{H} = \mathbf{H}x\}$. *Show that* $\mathbf{T}$ *is a subgroup of* $\mathbf{G}$. ***(N.U. A 85, O.U. 93)***

**Sol.** $\mathbf{H}$ is a subgroup of a group $\mathbf{G}$.

Let $x_1, x_2 \in \mathbf{T}$. $\therefore$ $x_1\mathbf{H} = \mathbf{H}x_1$, $x_2\mathbf{H} = \mathbf{H}x_2$

Now $x_2\mathbf{H} = \mathbf{H}x_2 \Rightarrow x_2^{-1}(x_2\mathbf{H})\,x_2^{-1} = x_2^{-1}(\mathbf{H}x_2)\,x_2^{-1}$

$\Rightarrow \mathbf{H}x_2^{-1} = x_2^{-1}\mathbf{H} \Rightarrow x_2^{-1} \in \mathbf{T}$

Also $(x_1x_2^{-1})\,\mathbf{H} = x_1(x_2^{-1}\mathbf{H}) = x_1(\mathbf{H}x_2^{-1}) = (x_1\mathbf{H})x_2^{-1}$

$= (\mathbf{H}x_1)x_2^{-1} = \mathbf{H}(x_1x_2^{-1}) \Rightarrow x_1x_2^{-1} \in \mathbf{T}$

Thus $x_1, x_2 \in \mathbf{T} \Rightarrow x_1, x_2^{-1} \in \mathbf{T}$ $\therefore$ $\mathbf{T}$ is a subgroup of $\mathbf{G}$.

## 4.6. SELF-CONJUGATE ELEMENT OF A GROUP

**Definition.** $(\mathbf{G}, .)$ is a group and $a \in \mathbf{G}$ such that $a = x^{-1}ax \ \forall\ x \in \mathbf{G}$. Then $a$ is called self conjugate element of $\mathbf{G}$. A self-conjugate element is sometimes called an invariant element.

Here $a = x^{-1}ax \Rightarrow xa = ax \ \forall\ x \in \mathbf{G}$

**The centre of a group.**

**Definition.** The set $\mathbf{Z}$ of all self-conjugate elements of a group $\mathbf{G}$ is called the centre of the group $\mathbf{G}$.

Thus $\mathbf{Z} = \{z \in \mathbf{G} / zx = xz \ \forall\ x \in \mathbf{G}\}$

If $\mathbf{G}$ is abelian, then centre of $\mathbf{G}$ is $\mathbf{G}$. (Vide Theorem 18 Chapter 5)

### EXERCISE 4

**1.** If $\mathbf{H} = \{1, -1\}$ and $\mathbf{G} = \{1, -1, i, -i\}$ then prove that $(\mathbf{H}, .)$ is a subgroup of the group $(\mathbf{G}, .)$. Find all the right cosets of $\mathbf{H}$ in $\mathbf{G}$.

**2.** Prove that $(\{0, 3, 6, 9, 12\}, +_{15})$ is a subgroup of $(\mathbf{Z}_{15}, +_{15})$. Find the left cosets of the above subgroup in $\mathbf{Z}_{15}$. Find the index of the supgroup in $\mathbf{G}$. ***(K.U.A. 03)***

**3.** (*i*) Determine the coset decomposition of the additive group of integers relative to a subgroup of all integral multiples of $4 = 4\mathbf{Z}$. ***(O.U. 12)***

(*ii*) Find all cosets and index of the subgroup $<4>$ of $\mathbf{Z}_{12}$. ***(K.U. 12)***

**4.** $\mathbf{H}, \mathbf{K}$ are two subgroups of a group $\mathbf{G}$. Show that any coset relative to $\mathbf{H} \cap \mathbf{K}$ is the intersection of a coset relative to $\mathbf{H}$ with a coset relative to $\mathbf{K}$. ***(N.U. A 85)***

**5.** Let $\mathbf{G}$ be a finite group. If $\mathbf{H}_1, \mathbf{H}_2$ be finite subgroups of prime order $p$ and $q$ respectively of $(p \neq q)$ then show that $\mathbf{H}_1 \cap \mathbf{H}_2 = \{e\}$. ***(A.N.U.M.97, K.U.J 02)***

## ANSWERS

**1.** $1\mathbf{H} = \mathbf{H},\ (-1)\mathbf{H} = \{-1, 1\},\ i\mathbf{H} = \{i, -i\}, (-i)\mathbf{H} = \{-i, i\}$

**2.** $0 +_{15} \mathbf{H} = \{0, 3, 6, 9, 12\} = \mathbf{H},\ 1 +_{15} \mathbf{H} = \{1, 4, 7, 10, 13\},\ 2 +_{15} \mathbf{H} = \{2, 5, 8, 11, 14\},$
$3 +_{15} \mathbf{H} = \mathbf{H},\ 4 +_{15} \mathbf{H} = 1 +_{15} \mathbf{H} = 1 +_{15} \mathbf{H},\ 5 +_{15} \mathbf{H} = 2 +_{15} \mathbf{H},$ etc.

**3.** (*i*) $\mathbf{Z} = (0+\mathbf{H}) \cup (1+\mathbf{H}) \cup (2+\mathbf{H}) \cup (3+\mathbf{H})$.

(*ii*) $\mathbf{Z}_{12} = 0 +_{12} \mathbf{H} \cup 1 +_{12} \mathbf{H} \cup 2 +_{12} \mathbf{H} \cup 3 +_{12} \mathbf{H}$ where $\mathbf{H} = \{0,4,8\} = <4>$.

The index of the subgroup H of $\mathbf{Z_{12}}$ is 4.

# Normal Subgroups

**5.1.** Let $\mathbf{G}$ be a multiplicative abelian group and $\mathbf{H}$ a subgroup of $\mathbf{G}$. For $x \in \mathbf{G}$, $x\mathbf{H}$ is a left coset and $\mathbf{H}x$ is a right coset of $\mathbf{H}$ in $\mathbf{G}$ such that $x\mathbf{H} = \mathbf{H}x$. However, even if $\mathbf{G}$ is not abelian there exists a subgroup $\mathbf{H}$ of $\mathbf{G}$ such that $x\mathbf{H} = \mathbf{H}x$ for $x \in \mathbf{G}$. This fact was first discovered by a great French mathematician Galois. Such subgroups of a group $\mathbf{G}$ are termed normal subgroups and they play a very important role in Abstract Algebra.

## 5.2. Normal Subgroup.

**Definition.** A subgroup $\mathbf{H}$ of a group $\mathbf{G}$ is said to be a normal subgroup of $\mathbf{G}$ if $\forall\, x \in \mathbf{G}$ and $\forall\, h \in \mathbf{H}, xhx^{-1} \in \mathbf{H}$. ***(S.V.U. S 93, N.U. 95, S.V.U. A 00, M. 03, S99, M.98, S97, M.96, A92, O90, A89, A.U. M05, S00, S98, K.U. M11, O96, O.U. M11, M12, O 03, O 02, A 00, O99, A99, S.K.U. O99, O97)***

From the definition we conclude that

(i) $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$ iff $x\mathbf{H}x^{-1} \subseteq \mathbf{H}\ \forall\ x \in \mathbf{G}$
where $x\mathbf{H}x^{-1} = \{xhx^{-1} \mid h \in \mathbf{H},\ x \in \mathbf{G}\}$

(ii) $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$ iff $x^{-1}\mathbf{H}x \subseteq \mathbf{H}\ \forall\ x \in \mathbf{G}$
$(\because\ x \in \mathbf{G} \Rightarrow x^{-1} \in \mathbf{G}, \forall\ h \in \mathbf{H},\ x^{-1}h(x^{-1})^{-1} \in \mathbf{H} \Rightarrow x^{-1}hx \in \mathbf{H})$.

(iii) the improper subgroup $\mathbf{H} = \{e\}$ is a normal subgroup.
$(\because\ e \in \mathbf{H} \Rightarrow xex^{-1} \in \mathbf{H}\ \forall\ x \in \mathbf{G})$ and

(iv) the improper subgroup $\mathbf{H} = \mathbf{G}$ is a normal subgroup.
$(\because\ h \in \mathbf{G} \Rightarrow xhx^{-1} \in \mathbf{G}\ \forall\ x \in \mathbf{G})$

$\mathbf{H} = \{e\}$ and $\mathbf{H} = \mathbf{G}$ are called improper or trivial normal subgroups of a group $\mathbf{G}$ and all other normal subgroups of $\mathbf{G}$, if exist, are called proper normal subgroups of $\mathbf{G}$.

**Notation.** If $\mathbf{N}$ is a normal subgroup of $\mathbf{G}$ we write $\mathbf{N} \triangleleft \mathbf{G}$. We read $\mathbf{N} \triangleleft \mathbf{G}$ as '$\mathbf{N}$ normal subgroup $\mathbf{G}$'.

**Note.** Any non-abelian group whose every subgroup is normal, is called a **Hamilton group.**

**Theorem 1.** ***A subgroup $\mathbf{H}$ of a group $\mathbf{G}$ is normal, if $x\mathbf{H}x^{-1} = \mathbf{H}\ \forall\ x \in \mathbf{G}$.***
***(S.V.U. M 11, S 93, 00) (B.A.) (N.U. O 90)(A.N.U. J 03, M01, M98, M96, A91, A.U.S.98, M98, K.U.M99, O.U.M 03, O 02, S.K.U.M 01, O97)***

**Proof.** (i) Let $x\mathbf{H}x^{-1} = \mathbf{H}\ \forall\ x \in \mathbf{G}$. We prove that $\mathbf{H}$ is normal.
Since $x\mathbf{H}x^{-1} \subseteq \mathbf{H}\ \forall\ x \in \mathbf{G}$, $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

(ii) Again let $\mathbf{H}$ be a normal subgroup of $\mathbf{G}$. We prove that $x\mathbf{H}x^{-1} = \mathbf{H}\ \forall\ x \in \mathbf{G}$.

$\therefore \qquad x\mathbf{H}x^{-1} \subseteq \mathbf{H}\ \forall\ x \in \mathbf{G} \qquad \ldots(1)$

Also $x \in \mathbf{G} \Rightarrow x^{-1} \in \mathbf{G}$ and hence $\forall\ x \in \mathbf{G},\ x^{-1}\mathbf{H}(x^{-1})^{-1} \subseteq \mathbf{H}$

$\Rightarrow \quad x^{-1}\mathbf{H}x \subseteq \mathbf{H} \Rightarrow x(x^{-1}\mathbf{H}x)x^{-1} \subseteq x\mathbf{H}x^{-1}$

$\Rightarrow \quad \mathbf{H} \subseteq x\mathbf{H}x^{-1}$ …(2)

$\therefore$ From (1) and (2), $x\mathbf{H}x^{-1} = \mathbf{H} \ \forall \ x \in \mathbf{G}$.

$\therefore \quad \mathbf{H} \lhd \mathbf{G} \Leftrightarrow x\mathbf{H}x^{-1} = \mathbf{H}, \ \forall / \ x \in \mathbf{G}$.

**Theorem 2.** ***A subgroup $\mathbf{H}$ of a group $\mathbf{G}$ is a normal subgroup of $\mathbf{G}$ iff each left coset of $\mathbf{H}$ in $\mathbf{G}$ is a right coset of $\mathbf{H}$ in $\mathbf{G}$.***

***(S.V.U. S 93, N.U. 92, A.N.U.J 04, J 03, M 03, S2002, S 01,S96, S93, A.U.A 01, M.99, S96, A96, K.U.J. 02, O97, O96, M96,S.K.U. M 03, S.V.U. M 05, S 03)***

**Proof.** (i) Let $\mathbf{H}$ be a normal subgroup of $\mathbf{G}$.

Then $x\mathbf{H}x^{-1} = \mathbf{H} \ \forall \ x \in \mathbf{G} \Rightarrow (x\mathbf{H}x^{-1})x = \mathbf{H}x \ \forall \ x \in \mathbf{G}$

$\Rightarrow \ x\mathbf{H} = \mathbf{H}x \ \forall \ x \in \mathbf{G}$

$\Rightarrow$ every left coset of $\mathbf{H}$ in $\mathbf{G}$ is a right coset of $\mathbf{H}$ in $\mathbf{G}$.

(ii) Let every left coset of $\mathbf{H}$ in $\mathbf{G}$ be a right coset of $\mathbf{H}$ in $\mathbf{G}$.

Let $x \in \mathbf{G}$. Then $x\mathbf{H} = \mathbf{H}y$ for some $y \in \mathbf{G}$.

Since $e \in \mathbf{H}, xe = x \in x\mathbf{H}$

Since $x\mathbf{H} = \mathbf{H}y, x \in \mathbf{H}y \quad \therefore \quad \mathbf{H}x = \mathbf{H}y$ (vide Th. 3, Chapter 4)

$\therefore \quad x\mathbf{H} = \mathbf{H}x \ \forall \ x \in \mathbf{G}$.

$\Rightarrow \ x\mathbf{H}x^{-1} = \mathbf{H}xx^{-1} \ \forall \ x \in \mathbf{G} \Rightarrow \ x\mathbf{H}x^{-1} = \mathbf{H} \ \forall \ x \in \mathbf{G}$

$\Rightarrow \ \mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

$\therefore \ \mathbf{H} \lhd \mathbf{G} \Leftrightarrow$ every left coset of $\mathbf{H}$ in $\mathbf{G}$ is a right coset of $\mathbf{H}$ in $\mathbf{G}$.

**Theorem 3.** ***A subgroup $\mathbf{H}$ of a group $\mathbf{G}$ is a normal subgroup of $\mathbf{G}$ iff the product of two right (left) cosets of $\mathbf{H}$ in $\mathbf{G}$ is again a right (left) coset of $\mathbf{H}$ in $\mathbf{G}$.***

***(A.N.U. J 04, M 03, M99, O92, A.U.M.00, M97, K.U.A 03, A 00, N.U. S 93, S.K. U. M 11, S.V.U. O 96, O98, M 00, M 09)***

**Proof.** (i) Let $\mathbf{H}$ be a normal subgroup of $\mathbf{G}$. $\forall \ a, b \in \mathbf{G}, ab \in \mathbf{G}$.

$\therefore \quad \mathbf{H}a, \mathbf{H}b, \mathbf{H}ab$ are right cosets of $\mathbf{H}$ in $\mathbf{G}$.

Then $\mathbf{H}a \ \mathbf{H}b = \mathbf{H}(a\mathbf{H})b = \mathbf{H}(\mathbf{H}a)b = \mathbf{H}\mathbf{H}ab$ ($\because$ $\mathbf{H}$ is normal $\Rightarrow a\mathbf{H} = \mathbf{H}a$)

$= \mathbf{H}ab$ ($\because \ \mathbf{H}\mathbf{H} = \mathbf{H}$)

$\therefore$ The product of two right cosets of $\mathbf{H}$ in $\mathbf{G}$ is again a right coset of $\mathbf{H}$ in $\mathbf{G}$.

(ii) For $a, b \in \mathbf{G}, \mathbf{H}a \ \mathbf{H}b = \mathbf{H}ab$.

For $h \in \mathbf{H}, x \in \mathbf{G}$, we have $xhx^{-1} = (ex)(hx^{-1}) \in (\mathbf{H}x)(\mathbf{H}x^{-1})$

$\Rightarrow xhx^{-1} \in \mathbf{H}xx^{-1} \quad \Rightarrow xhx^{-1} \in \mathbf{H}e \Rightarrow xhx^{-1} \in \mathbf{H}$

$\Rightarrow \ \mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

Similarly we can prove the theorem for left cosets.

**Note 1.** Let $\mathbf{H}$ be a normal subgroup of $(\mathbf{G}, .)$. Let $a, b \in \mathbf{G}$. Then $\mathbf{H}a, \mathbf{H}b$ are two right cosets of $\mathbf{H}$ in $\mathbf{G}$. Then cosets multiplication is defined as

$\mathbf{H}a \ \mathbf{H}b = \mathbf{H}ab$

($\because \ a, b \in \mathbf{G} \Rightarrow ab \in \mathbf{G}$; $\mathbf{H}$ is normal $\Rightarrow a\mathbf{H} = \mathbf{H}a$; $\mathbf{H}\mathbf{H} = \mathbf{H}$)

This multiplication of cosets is also true for left cosets since $\mathbf{H}$ is normal.

**2.** If $\mathbf{H}$ is a normal subgroup of a group $(\mathbf{G}, .)$ then the following statements are equivalent to one another.

(i) $x^{-1}hx \in \mathbf{H}$ for $x \in \mathbf{G}$ and $h \in \mathbf{H}$. (ii) $x\mathbf{H}x^{-1} \in \mathbf{H}x$ for $x \in \mathbf{G}$.

(iii) $x\mathbf{H} = \mathbf{H}x$ for $x \in \mathbf{G}$.

(iv) the set of right (left) cosets of $\mathbf{H}$ in $\mathbf{G}$ is closed w.r.t. coset multiplication.

**Theorem 4.** ***Every subgroup of an abelian group is normal.***
***(O. U. M12, 06, N.U.M12, M 04, M02, S01, S00, M00, S99, S97, A.U.S 00, S.K.U. M 05, O97)***

**Proof.** Let $\mathbf{H}$ be a subgroup of an abelian group $\mathbf{G}$.

Let $h \in \mathbf{H}, x \in \mathbf{G}$ and $e$ be the identity in $\mathbf{G}$.

$\therefore\ h = eh = (xx^{-1})\,h = x\,(x^{-1}h) = x\,(hx^{-1})$ ($\because$ $\mathbf{G}$ is abelian $\Rightarrow x^{-1}h = hx^{-1}$)

i.e. $h \in \mathbf{H} \Rightarrow xhx^{-1} \in \mathbf{H},\ \forall\, x \in \mathbf{G}$ $\Rightarrow \mathbf{H} \lhd \mathbf{G}$.

**Theorem 5.** ***If $\mathbf{G}$ is a group and $\mathbf{H}$ is a subgroup of index 2 in $\mathbf{G}$, then $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.*** ***(A.N.U. M 04, M98, A92, A.V.S99, K.U.A. 03, M 01, M96, O.U.A. 00, A99, S.K.U.M. 03, O 00, N.U. A 92, S 93, O.U. 93, O 99, S.K.U. O 2K)***

**Proof.** Since the index of the subgroup $\mathbf{H}$ in $\mathbf{G}$ is 2, the number of distinct right cosets of $\mathbf{H}$ in $\mathbf{G}$ = the number of distinct left cosets of $\mathbf{H}$ in $\mathbf{G} = 2$.

Let $x \in \mathbf{G}$ $\therefore$ The right cosets are $\mathbf{H}, \mathbf{H}x$ and two left cosets are $\mathbf{H}, x\mathbf{H}$.

Now $x \in \mathbf{H}$ or $x \notin \mathbf{H}$

If $x \in \mathbf{H}$, then $\mathbf{H}x = \mathbf{H} = x\mathbf{H}$ and hence $\mathbf{H} \lhd \mathbf{G}$.

If $x \notin \mathbf{H}$, then $\mathbf{H}x$ is distinct from $\mathbf{H}$ and $x\mathbf{H}$ is distinct from $\mathbf{H}$. Since the index of $\mathbf{H}$ is 2, $\mathbf{G} = \mathbf{H} \cup \mathbf{H}x = \mathbf{H} \cup x\mathbf{H}$. Since there is no element common to $\mathbf{H}, \mathbf{H}x$, we must have $\mathbf{H}x = x\mathbf{H}$. $\therefore$ $\mathbf{H} \lhd \mathbf{G}$.

**Theorem 6.** ***The intersection of any two normal subgroups of a group is a normal subgroup.*** ***(A.N.U.M. 02, S99, O.U.M 05, M 03, A 02, A 00, O 01, S.K.U. A 00, A.U.12)***

**Proof.** Let $\mathbf{H}, \mathbf{K}$ be two normal subgroups of a group $(\mathbf{G}, .)$. Since $\mathbf{H}, \mathbf{K}$ are subgroups of $\mathbf{G}, \mathbf{H} \cap \mathbf{K}$ is also a subgroup of $\mathbf{G}$.

Let $n \in \mathbf{H} \cap \mathbf{K}$ and $x \in \mathbf{G}$ $\therefore$ $n \in \mathbf{H}$ and $n \in \mathbf{K}$

$\therefore\ xnx^{-1} \in \mathbf{H}$ and $xnx^{-1} \in \mathbf{K}$ ($\because$ $\mathbf{H}, \mathbf{K}$ are normal subgroups in $\mathbf{G}$)

$\therefore$ $xnx^{-1} \in \mathbf{H} \cap \mathbf{K}$ for $x \in \mathbf{G}$ $\therefore$ $\mathbf{H} \cap \mathbf{K} \lhd \mathbf{G}$.

**Cor.** The arbitrary intersection of any number of normal subgroups of a group $\mathbf{G}$ is also a normal subgroup of $\mathbf{G}$.

**Theorem 7.** ***A normal subgroup of a group $\mathbf{G}$ is commutative with every complex of $\mathbf{G}$.*** ***(A.N.U.S. 02)***

**Proof.** Let $\mathbf{N}$ be a normal subgroup and $\mathbf{H}$ be a complex of $\mathbf{G}$. To prove that $\mathbf{NH} = \mathbf{HN}$.

Let $nh \in \mathbf{NH}$ where $n \in \mathbf{N}$ and $h \in \mathbf{H}$

Since $\mathbf{N}$ is normal subgroup and $nh = hh^{-1}nh$

$= h\,(h^{-1}nh),\ nh \in \mathbf{HN}$ $\therefore$ $\mathbf{NH} \subseteq \mathbf{HN}$. …(1)

Similarly $hn \in \mathbf{HN} \Rightarrow hn \in \mathbf{NH}$ ($\because$ $hn = (hnh^{-1})\,h \in \mathbf{NH}$)

$\therefore$ $\mathbf{HN} \subseteq \mathbf{NH}$ …(2)

$\therefore$ From (1) and (2) $\mathbf{NH} = \mathbf{HN}$.

**Theorem 8.** *If* $\mathbf{N}$ *is a normal subgroup of* $\mathbf{G}$ *and* $\mathbf{H}$ *is any subgroup of* $\mathbf{G}$, *then* $\mathbf{HN}$ *is a subgroup of* $\mathbf{G}$. *(A.N.U.S. 02)*

**Proof.** Since a normal subgroup of $\mathbf{G}$ is commutative with every complex of $\mathbf{G}$, we have $\mathbf{HN} = \mathbf{NH}$.

Now $\mathbf{H}$ and $\mathbf{N}$ are two subgroups of $\mathbf{G}$ such that $\mathbf{HN} = \mathbf{NH}$. (Theorem 12, Chapter 3)

$\therefore$ $\mathbf{HN}$ is a subgroup of $\mathbf{G}$.

**Theorem 9.** *If* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$ *and* $\mathbf{N}$ *is a normal subgroup of* $\mathbf{G}$, *then*
(i) $\mathbf{H} \cap \mathbf{N}$ *is a normal subgroup of* $\mathbf{H}$ (ii) $\mathbf{N}$ *is a normal subgroup of* $\mathbf{HN}$.
*(S.K.U. 2001/0, S.V.U. A 99)*

**Proof.** (i) $\mathbf{H}, \mathbf{N}$ are subgroups of $\mathbf{G} \Rightarrow \mathbf{H} \cap \mathbf{N}$ is a subgroup of $\mathbf{G} \Rightarrow \mathbf{H} \cap \mathbf{N}$ is a subgroup of $\mathbf{H}$. $(\because \mathbf{H} \cap \mathbf{N} \subseteq \mathbf{H})$

Let $x \in \mathbf{H}$ $\therefore$ $x \in \mathbf{G}$

Let $y \in \mathbf{H} \cap \mathbf{N}$. $\therefore$ $y \in \mathbf{H}$ and $y \in \mathbf{N}$.

Now $y \in \mathbf{N} \Rightarrow xyx^{-1} \in \mathbf{N}$, since $\mathbf{N}$ is normal in $\mathbf{G}$ and

$y \in \mathbf{H}$, $x \in \mathbf{H} \Rightarrow x \in \mathbf{H}$, $y \in \mathbf{H}$, $x^{-1} \in \mathbf{H} \Rightarrow xyx^{-1} \in \mathbf{H}$.

$\therefore$ $xyx^{-1} \in \mathbf{H} \cap \mathbf{N}$. $\therefore$ $\mathbf{H} \cap \mathbf{N}$ is a normal subgroup of $\mathbf{G}$.

(ii) $e \in \mathbf{H}$ and $e \in \mathbf{N}$. Let $n \in \mathbf{N}$.

Since $\mathbf{H} \neq \phi$, $\mathbf{N} \neq \phi$, we have $\mathbf{HN} \neq \phi$. Since $en \in \mathbf{HN} \; \forall \, n \in \mathbf{N}$, $\mathbf{N} \subseteq \mathbf{HN}$.

Since $\mathbf{HN}$ is a subgroup of $\mathbf{G}$, $\mathbf{N}$ is a subgroup of $\mathbf{G}$ and $\mathbf{N} \subseteq \mathbf{HN}$, $\mathbf{N}$ is also a subgroup of $\mathbf{HN}$.

Let $n \in \mathbf{N}$ and $h_1 n_1 \in \mathbf{HN}$ where $h_1 \in \mathbf{H}$ and $n_1 \in \mathbf{N}$.

Now $(h_1 n_1)\, n\, (h_1 n_1)^{-1} = h_1 n_1 n n_1^{-1} h_1^{-1} = h_1 (n_1 n n_1^{-1}) n_1^{-1} \in \mathbf{N}$

$(\because$ $h_1 \in \mathbf{H} \Rightarrow h_1 \in \mathbf{G}$ and $\mathbf{N}$ is normal in $\mathbf{G})$

$\therefore$ $\mathbf{N}$ is normal in $\mathbf{HN}$.

**Theorem 10.** *If* $\mathbf{N}$, $\mathbf{M}$ *are normal subgroups of* $\mathbf{G}$, *then* $\mathbf{NM}$ *is also a normal subgroup of* $\mathbf{G}$. *(A.N.U. M 04, M 03, A93, O91, S.K.U. O 02, O.U. 01/O, NU. A 93, A99)*

**Proof.** Since $\mathbf{N} \neq \phi$, $\mathbf{M} \neq \phi$, we have $\mathbf{NM} \neq \phi$ and $\mathbf{MN} \neq \phi$.

Since a normal subgroup of $\mathbf{G}$ is commutative with every complex of $\mathbf{G}$, $\mathbf{NM} = \mathbf{MN}$.

Since $\mathbf{N}$, $\mathbf{M}$ are subgroups of $\mathbf{G}$, $\mathbf{NM}$ is also a subgroup of $\mathbf{G}$.

Let $x \in \mathbf{G}$ and $nm \in \mathbf{NM}$.

$\therefore$ $x(nm)\, x^{-1} - x(nx^{-1}x)\, mx^{-1} = (xnx^{-1})(xmx^{-1}) \in \mathbf{NM}$ $\therefore$ $\mathbf{NM} \lhd \mathbf{G}$.

**Theorem 11.** *If* $\mathbf{M}, \mathbf{N}$ *are two normal subgroups of* $\mathbf{G}$ *such that* $\mathbf{M} \cap \mathbf{N} = \{e\}$. *Then every element of* $\mathbf{M}$ *commutes with every element of* $\mathbf{N}$.
*(K.U. O99, O97, A97, O.U. A 01, M 02, N.U. O 88, O 89, A 95, 2K, S 02, S.V.U. S 89)*

**Proof.** Let $m \in \mathbf{M}$ and $n \in \mathbf{N}$ to prove that $mn = nm$.

Since $n \in \mathbf{N}$, $n^{-1} \in \mathbf{N}$. Since $\mathbf{N}$ is normal in $\mathbf{G}$ and $m \in \mathbf{G}$, we have $mn^{-1}m^{-1} \in \mathbf{N}$.

Also by closure in $\mathbf{N}$, $nmn^{-1}m^{-1} \in \mathbf{N}$. …(1)

Since $\mathbf{M}$ is normal, $nmn^{-1} \in \mathbf{M}$. Also $m^{-1} \in \mathbf{M}$.

By closure in $\mathbf{M}$, $nmn^{-1}m^{-1} \in \mathbf{M}$ …(2)

$\therefore$ From (1) and (2), $nmn^{-1}m^{-1} \in \mathbf{M} \cap \mathbf{N}$ But $\mathbf{M} \cap \mathbf{N} = \{e\}$.

$\therefore\ nmn^{-1}m^{-1} = e \Rightarrow nmn^{-1} = em = m \Rightarrow nm = mn.$

$\therefore$ Every element of $\mathbf{M}$ commutes with every element of $\mathbf{N}$.

## 5.3. SIMPLE GROUP

**Definition.** A group $\mathbf{G}$ is called simple if it has no proper normal subgroups.

***(A.V.M. 05, O.U. 02, S.V.U.A 02, S.V.U. S 93)***

**Note.** $\mathbf{G}$ is simple $\Leftrightarrow$ $\mathbf{G}$ has no normal subgroups other than $\mathbf{G}$ and $\{e\}$.

**Theorem 12.** ***Every group of prime order is simple.***

***(A.N.U.S. 00, A.U.M. 05, S.V.U.A. 02)***

**Proof.** We know that a group of prime order has no proper normal subgroups.

(Ex. 3, Art 4.5)

**Theorem 13.** ***No abelian group of composite order is simple.*** ***(N.U. 00)***

**Proof.** We know that every abelian group of composite order possesses a proper subgroup. Also every subgroup of an abelian group is normal. (Theorem 4, Art 5.2)

$\therefore$ Every abelian group of composite order possesses a proper normal subgroup.

Hence no abelian group of composite order is simple.

## 5. 4. QUOTIENT GROUP OR FACTOR GROUP

**Theorem 14.** $\mathbf{H}$ ***is a normal subgroup of*** $\mathbf{G}$. ***The set*** $\frac{\mathbf{G}}{\mathbf{H}}$ ***of all cosets of*** $\mathbf{H}$ ***in*** $\mathbf{G}$ ***w.r.t. coset multiplication is a group.*** ***(A.N.U.M. 04, M 02, M 01, M98, O92, O90, A89, A.V.A 02, A 02, K.U.M 04, S 00, O99, O.U. M 05, O99, S.K.U. M 07,O 02, S.V.U. A 97)***

**Proof.** $\mathbf{H}$ is a normal subgroup of $(\mathbf{G}, .)$. For $a \in \mathbf{G}$, $a\mathbf{H} = \mathbf{H}a$.

$\therefore$ $\frac{\mathbf{G}}{\mathbf{H}}$ is the set of all cosets of $\mathbf{H}$ in $\mathbf{G}$. For $a, b \in \mathbf{G}$, we have $\mathbf{H}a,\ \mathbf{H}b \in \frac{\mathbf{G}}{\mathbf{H}}$.

We define coset multiplication on $\frac{\mathbf{G}}{\mathbf{H}}$ as $(\mathbf{H}a)(\mathbf{H}b) = \mathbf{H}(ab)$.

We prove that the operation is well defined.

Let $\mathbf{H}a = \mathbf{H}a_1$ and $\mathbf{H}b = \mathbf{H}b_1$ in $\frac{\mathbf{G}}{\mathbf{H}}$

$\therefore$ $ea = a = h_1a_1$ for some $h_1 \in \mathbf{H}$ and $eb = b = h_2b_1$ for some $h_2 \in \mathbf{H}$

Now $\mathbf{H}ab = \mathbf{H}(h_1a_1)(h_2b_1) = \mathbf{H}h_1(a_1h_2)\,b_1 = \mathbf{H}\,h_1(h_3a_1)\,b_1$

[$\because$ $\mathbf{H}$ is normal in $\mathbf{G}$, $a_1\mathbf{H} = \mathbf{H}a$, so that $a_1h_2 = h_3a_1$, for some $h_3 \in \mathbf{H}$]

$= \mathbf{H}(h_1h_3)(a_1b_1) = \mathbf{H}\,a_1b_1$ [$\because$ $h_1h_2 \in \mathbf{H} \Rightarrow \mathbf{H}(h_1h_3) = \mathbf{H}$]

i.e. $\mathbf{H}a\,\mathbf{H}b = \mathbf{H}a_1\mathbf{H}b_1$

$\therefore$ Coset multiplication is well defined.

**Closure:** $\mathbf{H}a,\ \mathbf{H}b \in \frac{\mathbf{G}}{\mathbf{H}} \Rightarrow \mathbf{H}a\,\mathbf{H}b \in \frac{\mathbf{G}}{h}$. since $a, b \in \mathbf{G} \Rightarrow ab \in \mathbf{G}$ and $\mathbf{H}a\,\mathbf{H}b = \mathbf{H}ab \in \frac{\mathbf{G}}{\mathbf{H}}$

**Associativity :** $\mathbf{H}a,\ \mathbf{H}b,\ \mathbf{H}c \in \frac{\mathbf{G}}{\mathbf{H}} \Rightarrow (\mathbf{H}a\,\mathbf{H}b)\,\mathbf{H}c = \mathbf{H}a\,(\mathbf{H}b\,\mathbf{H}c)$,

since $(\mathbf{H}a\,\mathbf{H}b)\,\mathbf{H}c = \mathbf{H}ab\,\mathbf{H}c = \mathbf{H}(ab)\,c = \mathbf{H}a\,(bc) = \mathbf{H}a\,\mathbf{H}bc = \mathbf{H}a\,(\mathbf{H}b\,\mathbf{H}c)$.

**Existence of identity :** Let $\mathbf{H}a \in \frac{\mathbf{G}}{\mathbf{H}}$ $\quad\therefore\ \exists\ \mathbf{H}e\,(=\mathbf{H}) \in \frac{\mathbf{G}}{\mathbf{H}}$

such that $\mathbf{H}a\,\mathbf{H}e = \mathbf{H}ae = \mathbf{H}a = \mathbf{H}ae = \mathbf{H}e\,\mathbf{H}a$.

$\therefore$ Identity exists in $\frac{\mathbf{G}}{\mathbf{H}}$ and it is $\mathbf{H}e\,(=\mathbf{H})$.

**Existence of inverse :** Let $\mathbf{H}a \in \frac{\mathbf{G}}{\mathbf{H}}$

Since $a \in \mathbf{G} \Rightarrow a^{-1} \in \mathbf{G}$, we have $\mathbf{H}a^{-1} \in \frac{\mathbf{G}}{\mathbf{H}}$

Now $\mathbf{H}a\,\mathbf{H}a^{-1} = \mathbf{H}\,(aa^{-1}) = \mathbf{H}e = \mathbf{H}\,(a^{-1}a) = \mathbf{H}a^{-1}\mathbf{H}a.$

$\therefore$ Every element of $\frac{\mathbf{G}}{\mathbf{H}}$ is invertible and $\mathbf{H}\,a^{-1}$ is the inverse of $\mathbf{H}\,a$

$\therefore$ $\frac{\mathbf{G}}{\mathbf{H}}$ is a group w.r.t. coset multiplication.

**Definition.** Let $\mathbf{H}$ be a normal subgroup of a group $(\mathbf{G},.)$. For $a \in \mathbf{G}$, $\mathbf{H}\,a$ is the right coset of $\mathbf{H}$ and $a\mathbf{H}$ is the left coset of $\mathbf{H}$ in $\mathbf{G}$. Since $\mathbf{H}$ is normal, $\mathbf{H}a = a\mathbf{H}$. Thus $\frac{\mathbf{G}}{\mathbf{H}}$ is the set of all cosets of $\mathbf{H}$ in $\mathbf{G}$. Define an operation, called coset multiplication, on $\frac{\mathbf{G}}{\mathbf{H}}$ such that $\mathbf{H}a, \mathbf{H}b \in \frac{\mathbf{G}}{\mathbf{H}} \Rightarrow \mathbf{H}a\,\mathbf{H}b = \mathbf{H}ab$. Now $\frac{\mathbf{G}}{\mathbf{H}}$ is a group w.r.t. coset multiplication. This is called the Quotient group or Factor group of $\mathbf{G}$ by $\mathbf{H}$.

**Theorem 15.** ***If*** $\mathbf{H}$ ***is a normal subgroup of a finite group*** $\mathbf{G}$, ***then*** $\mathbf{O}\left(\frac{\mathbf{G}}{\mathbf{H}}\right) = \frac{\mathbf{O}(\mathbf{G})}{\mathbf{O}(\mathbf{H})}$.

**Proof :** $\mathbf{O}\left(\frac{\mathbf{G}}{\mathbf{H}}\right)$ = number of distinct cosets of $\mathbf{H}$ in $\mathbf{G}$.

$$= \frac{\text{number of elements in } \mathbf{G}}{\text{number of elements in } \mathbf{H}} = \frac{\mathbf{O}(\mathbf{G})}{\mathbf{O}(\mathbf{H})}$$

**Theorem 16.** ***Every quotient group of an abelian group is abelian.***

**Proof.** Let $\mathbf{H}$ be a subgroup of an abelian group $\mathbf{G}$. But every subgroup of an abelian group is normal. So $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$. Let $\frac{\mathbf{G}}{\mathbf{H}}$ be the quotient group of $\mathbf{G}$ by $\mathbf{H}$.

For $a, b \in \mathbf{G}$, $ab = ba$ since $\mathbf{G}$ is abelian.

$\therefore$ $\mathbf{H}a, \mathbf{H}b \in \frac{\mathbf{G}}{\mathbf{H}}$. Now $(\mathbf{H}a)\,(\mathbf{H}b) = (\mathbf{H}ab) = (\mathbf{H}ba) = (\mathbf{H}b)\,(\mathbf{H}a)$

$\therefore$ $\mathbf{G}/\mathbf{H}$ is abelian if $\mathbf{G}$ is abelian.

**Note. Converse.** If $\mathbf{G}/\mathbf{H}$ is abelian, then $\mathbf{G}$ is abelian.

Converse is not true.

**Definition.** If $\mathbf{G}$ is a group and $a \in \mathbf{G}$, then $\mathbf{N}(a) = \{x \in \mathbf{G} : ax = xa\}$ is called normalizer of $a$ in $\mathbf{G}$. ***(A.N.U.M 03, M 00, O.U.A 02)***

**Theorem 17:** *If* **G** *is a group and* $a \in \mathbf{G}$ *then the normalizer* $\mathbf{N}(a)$ *of* $a$ *in* **G** *is a subgroup of* **G.** *(K.U.A 00, O.U.M 05, A 02, S.K.U. O 00)*

**Proof :** Let **G** is a group and $a \in \mathbf{G}$

Consider $\mathbf{N}(a) = \{x / x \in \mathbf{G},\ ax = xa\}$

We have $e \in \mathbf{G}$ and $ae = ea = a \Rightarrow e \in \mathbf{N}(a)$

$\therefore$ $\mathbf{N}(a)$ is a non-empty subset of **G**.

Let $x_1, x_2 \in \mathbf{N}(a) \Rightarrow ax_1 = x_1a$ and $ax_2 = x_2a$.

$$a(x_1x_2) = (ax_1)x_2 = (x_1a)x_2$$

$$= x_1(ax_2) = x_1(x_2a) = (x_1x_2)a$$

$\therefore$ $x_1x_2 \in \mathbf{N}(a)$

Let $x \in \mathbf{N}(a) \Rightarrow ax = xa \Rightarrow x^{-1}axx^{-1} = x^{-1}xax^{-1}$

$\Rightarrow x^{-1}a = ax^{-1} \Rightarrow x^{-1} \in \mathbf{N}(a)$

$\therefore$ $\mathbf{N}(a)$ is a sbugroup of **G**.

**Note :** $\mathbf{N}(e) = \mathbf{G}$.

**CENTRE :**

**Definition :** If **G** is a group then $\{x \in \mathbf{G} / ax = xa \forall a \in \mathbf{G}\}$ is called the centre of **G**. It is denoted by **Z** or **Z**(**G**). *(A.N.U.M 04, S.98, S.97, O.U.A. 00, S.V.U.A.98)*

**Theorem 18 :** *If* **G** *is a group then the centre* **Z** *of* **G** *is a normal subgroup of* **G.** *(A.N.U.M. 04, S98, S97, S.V.U.A.98)*

**Proof :** **G** is a group and $\mathbf{Z} = \{x \in \mathbf{G} / ax = xa \forall a \in \mathbf{G}\}$.

First we prove that **Z** is a subgroup of **G**.

Let $x_1, x_2 \in \mathbf{Z}$. $\therefore$ $ax_1 = x_1a$ and $ax_2 = x_2a \forall a \in \mathbf{G}$

Now $ax_2 = x_2a \Rightarrow x_2^{-1}(ax_2)x_2^{-1} = x_2^{-1}(x_2a)x_2^{-1}$

$\Rightarrow x_2^{-1}a = ax_2^{-1} \Rightarrow x_2^{-1} \in \mathbf{Z}$

Also $(x_1x_2^{-1})a = x_1(x_2^{-1}a) = x_1(ax_2^{-1}) = (x_1a)x_2^{-1}$

$$= (ax_1)x_2^{-1} = a(x_1x_2^{-1}) \Rightarrow x_1x_2^{-1} \in \mathbf{Z}$$

Thus $x_1, x_2 \in \mathbf{Z} \Rightarrow x_1x_2^{-1} \in \mathbf{Z}$

$\therefore$ **Z** is a subgroup of **G**.

Now we show that **Z** is a normal subgroup of **G**.

Let $a \in \mathbf{G}$ and $x \in \mathbf{Z}$.

Then $axa^{-1} = (ax)a^{-1} = (xa)a^{-1} = x(aa^{-1}) = xe = x \in \mathbf{Z}$

Thus $a \in G, x \in \mathbf{Z} \Rightarrow axa^{-1} \in \mathbf{Z}$

$\therefore$ **Z** is a normal subgroup of **G**.

**Note :** If **G** is abelian then **Z = G .**

**Ex. 1.** $\mathbf{G} = \{r_0, r_1, r_2, f_1, f_2, f_3\}$ *is a non-abelian group.*

*(Vide Ex. 16 of chapter 2, composition table)*

Show that $\mathbf{H} = \{r_0, r_1, r_2\}$ is a normal subgroup of **G.**

**Sol.** We have to show that $a\mathbf{H} = \mathbf{H}a$ for $a \in \mathbf{G}$.

Observe that $f_1\mathbf{H} = \mathbf{H}f_1$.

$f_2\mathbf{H} = \mathbf{H}f_2$, $f_3\mathbf{H} = \mathbf{H}f_3$

$r_0\mathbf{H} = \mathbf{H}r_0 = \mathbf{H}$

$r_1\mathbf{H} = \mathbf{H} = \mathbf{H}r_1$

$r_2\mathbf{H} = \mathbf{H} = \mathbf{H}r_2$ and $\mathbf{H}, f_1\mathbf{H}$ are distinct left cosets.

$\therefore$ $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

Also $\dfrac{\mathbf{G}}{\mathbf{H}}$ is a quotient group where $\dfrac{\mathbf{G}}{\mathbf{H}} = \{\mathbf{H}, f_1\mathbf{H}\}$ Since $f_1\mathbf{H} = f_2\mathbf{H} = f_3\mathbf{H}$.

Composition table for $\mathbf{G}/\mathbf{H}$ is :

| | H | $f_1$H |
|---|---|---|
| H | H | $f_1$H |
| $f_1$H | $f_1$H | H |

**Ex. 2.** *Show that* $\mathbf{H} = \{1, -1\}$ *is a normal subgroup of the group of non-zero real numbers under multiplication.*

**Sol.** Let $\mathbf{G} = \mathbf{R} - \{0\}$ and the composition in $\mathbf{G}$ be multiplication. $(\mathbf{G}, .)$ is a group.

Clearly $\mathbf{H} \subset \mathbf{G}$ and $\mathbf{H}$ is a group under multiplication.

For $x \in \mathbf{G}, x.1.x^{-1} = x.\dfrac{1}{x} = 1$ and $x(-1)x^{-1} = -x.\dfrac{1}{x} = -1$

$\therefore$ For $h \in \mathbf{H}$ and $x \in \mathbf{G}, xhx^{-1} \in \mathbf{H}$.

$\therefore$ $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

| | 1 | −1 |
|---|---|---|
| 1 | 1 | −1 |
| −1 | −1 | 1 |

**composition table**

**Ex. 3.** *Show that* $\mathbf{H} = \{1, -1\}$ *is a normal subgroup of the group* $\mathbf{G} = \{1, -1, i, -i\}$ *under multiplication. Also write the composition table for the quotient group* $\mathbf{G}/\mathbf{H}$.

***(N.U. O 89, A90, A.U.S 2000, S.97, S.V.M. 2003)***

**Sol.** Clearly $\mathbf{H} \subset \mathbf{G}$ and $\mathbf{H}$ is a group under multiplication.

1 is the identity in $\mathbf{H}$.$1\mathbf{H} = \{1, -1\} = \mathbf{H}$, $-1\mathbf{H} = \{-1, 1\} = \mathbf{H}$, $i\mathbf{H} = \{i, -i\}$, $-i\mathbf{H} = \{-i, i\}$.

Also $1\mathbf{H} = \mathbf{H}1$, $(-1)\mathbf{H} = \mathbf{H}(-1)$, $i\mathbf{H} = \mathbf{H}i$, $(-i)\mathbf{H} = \mathbf{H}(-i)$.

$\therefore$ $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

$\therefore$ $\mathbf{G}/\mathbf{H}$ is the quotient group of $\mathbf{G}$ by $\mathbf{H}$.

Its composition table is :

| | H | $i$H |
|---|---|---|
| H | H | $i$H |
| $i$H | $i$H | H |

**Ex. 4.** *Show that* $\mathbf{H} = \{1, -1, i, -i\}$ *is a normal subgroup of the group of non-zero complex numbers under multiplication.*

**Sol.** Let $\mathbf{G} = \mathbf{C} - \{0\}$ and $.$ be the composition in $\mathbf{G}$.

$\mathbf{G}$ is a group under $\cdot$ (multiplication)

Clearly $\mathbf{H} \subset \mathbf{G}$ and $\mathbf{H}$ is a group under.

For $z \in \mathbf{G}$, $z.1.z^{-1} = z.\dfrac{1}{z} = 1$, $z(-1)z^{-1} = -1$, $z.i.z^{-1} = i$, $z(-i)z^{-1} = -i$.

$\therefore$ For $h \in \mathbf{H}$ and $z \in \mathbf{G}$, $z\mathbf{H}z^{-1} = \mathbf{H}$ $\quad\therefore$ $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$.

**Ex. 5.** Vide Ex. 15 of Chapter 2.

$\mathbf{A}_3 = \{f_1, f_5, f_6\}$ is a normal subgroup $\mathbf{P}_3$,

For : $f_1\mathbf{A}_3 = \mathbf{A}_3 f_1 = \mathbf{A}_3$, $f_5\mathbf{A}_3 = \mathbf{A}_3 f_5 = \mathbf{A}_3$, $\mathbf{A}_3 f_6 = f_6\mathbf{A}_3 = \mathbf{A}_3$,

$f_2\mathbf{A}_3 = \{f_2, f_3, f_4) = \mathbf{A}_3 f_2$, $f_3\mathbf{A}_3 = \{f_3, f_4, f_2) = \mathbf{A}_3 f_2$,

$f_4\mathbf{A}_3 = \{f_4, f_2, f_3) = \mathbf{A}_3 f_2$

The distinct left cosets of $\mathbf{A}_3$ are $\mathbf{A}_3$, $f_2\mathbf{A}_3$.

$\therefore$ The quotient group of $\mathbf{P}_3$ by $\mathbf{A}_3 = \{\mathbf{A}_3, f_2\mathbf{A}_3\}$

*i.e.* $\dfrac{\mathbf{P}_3}{\mathbf{A}_3} = \{\mathbf{A}_3, f_2\mathbf{A}_3\}$.

Clearly $\dfrac{\mathbf{P}_3}{\mathbf{A}_3}$ is abelian. Note that $\mathbf{P}_3$ is not abelian.

## EXERCISE 5

**1.** If $\mathbf{H}$ is a subgroup of a group $\mathbf{G}$ such that $x^2 \in \mathbf{H}$ for every $x \in \mathbf{G}$, then prove that $\mathbf{Z}$ is normal in $\mathbf{G}$.

**2.** If $\mathbf{G}$ is a group and $\mathbf{Z} = \{x \in \mathbf{G} / ax = xa \; \forall \, a \in \mathbf{G}\}$ prove that $\mathbf{Z}$ is normal in $\mathbf{G}$.

**3.** $\mathbf{N}$ is normal in the group $\mathbf{G}$. Show that $\mathbf{G}/\mathbf{N}$ is abelian iff $\forall\, x, y \in \mathbf{G}$, $xyx^{-1}y^{-1} \in \mathbf{N}$ ***(N.U. O 88)***

**4.** Define a maximal normal subgroup of a group $\mathbf{G}$. Prove that a normal subgroup $\mathbf{N}$ of a group $\mathbf{G}$ is maximal iff the quotient group $\mathbf{G}/\mathbf{N}$ is simple.

**5.** $\mathbf{H}$ is a subgroup of $\mathbf{G}$ and $\mathbf{N}(\mathbf{H}) = \{g \in \mathbf{G} / g\mathbf{H}g^{-1} = \mathbf{H}\}$. Show that (i) $\mathbf{N}(\mathbf{H})$ is a subgroup of $\mathbf{G}$, (ii) $\mathbf{H}$ is a normal subgroup of $\mathbf{N}(\mathbf{H})$, (iii) $\mathbf{H}$ is a normal subgroup in $\mathbf{G}$ iff $\mathbf{N}(\mathbf{H}) = \mathbf{G}$. ***(N.U. A 85)***

# Homomorphisms, Isomorphisms of Groups

## 6.1. HOMOMORPHISM INTO

**Definition.** Let $\mathbf{G}, \mathbf{G}'$ be two groups and $f$, a mapping from $\mathbf{G}$ into $\mathbf{G}'$. If for $a, b \in \mathbf{G}$, $f(a.b) = f(a).f(b)$ ...(1) then $f$ is said to be **homomorphism from G into G'**.

***(A.N.U.S97, S96, A92, O91, A90, A.U.S 00, M99, O.U. M11, M. 03, A 01, S.V.U. A 93, 98)***

The $.$ on the L.H.S. of (1) indicates the composition in $\mathbf{G}$ and the $.$ on the R.H.S. of (1) indicates the composition in $\mathbf{G}'$. Generally, we omit writing $.$ in (1).

The property of $f$ i.e. $f(a.b) = f(a).f(b)$ is commonly described as the image of a product under $f$ is equal to the product of images. Also we say that "the homomorphism $f$ preserves the binary operations of $\mathbf{G}$ and $\mathbf{G}'$". It is for this reason we call that the homomorphism as "the structure preserving mapping".

**Note.** There always exists a homomorphism between any two groups. For : Let $f$ be a function from a group G to a group G′ defined by $f(a) = e' \forall\, a \in \mathrm{G}$, where $e'$ is the identity in G′. For every $a_1, a_2 \in \mathrm{G}, f(a_1\, a_2) = e' = e'e' = f(a_1) f(a_2)$.

This is called **least homomorphism.**

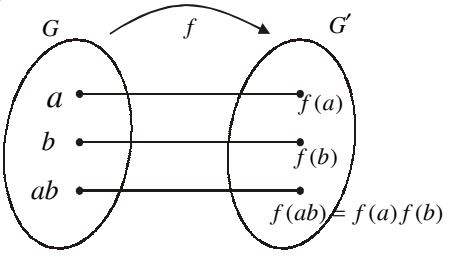



**Image of Homormorphism :** Let $f : \mathbf{G} \to \mathbf{G}'$ is a homomorphism. Then $\{f(a) / a \in \mathbf{G}\}$ is called homorphic image of $f$ or range of $f$.

It is denoted by $f(\mathbf{G})$ or $\mathrm{I}_m(f)$.

Thus $f(\mathbf{G}) = \mathrm{I}_m(f) = \{f(a) / a \in \mathbf{G}\}$. It is clear that $f(\mathbf{G}) \subseteq \mathbf{G}'$.

**Homomorphism onto.** Let $\mathbf{G}, \mathbf{G}'$ be two groups and $f$ a mapping from $\mathbf{G}$ onto $\mathbf{G}'$. If for $a, b \in \mathbf{G}$, $f(ab) = f(a)\, f(b)$ then $f$ is said to be a homomorphism from $\mathbf{G}$ onto $\mathbf{G}'$.

Also then $\mathbf{G}'$ is said to be a homomorph or a homomorphic image of $\mathbf{G}$. We write this as $f(\mathbf{G}) = \mathbf{G}'$. In this case we write $(\mathbf{G}, .) \simeq (\mathbf{G}', .)$ or $\mathbf{G} \simeq \mathbf{G}'$ (read as $\mathbf{G}$ is homomorphic to $\mathbf{G}'$). Homomorphism onto is sometimes called as **epimorphism**.

**Monomorphism.** Definition. If the homomorphism into is one-one, then it is called monomorphism.

**Endomorphism.** A homomorphism of a group $\mathbf{G}$ into itself is called an endomorphism.

**Isomorphism. Definition.** Let $(\mathbf{G}, o)$ and $(\mathbf{G}', .)$ be any two groups and $f$ be a one-one mapping of $\mathbf{G}$ onto $\mathbf{G}'$. If for $a, b \in \mathbf{G}$, $f(aob) = f(a).f(b)$ then $f$ is said to be an isomorphism from $\mathbf{G}$ to $\mathbf{G}'$. In this case we say that $\mathbf{G}$ is isomorphic to $\mathbf{G}'$ and we write $(\mathbf{G}, o) \cong (\mathbf{G}', .)$ *(A.V.A. 01, S.V.U. A 93, S 93)*

**Automorphism : Definition :** An isomorphism from a group $\mathbf{G}$ onto itself is called an automorphism of $\mathbf{G}$.

**Note.** If the group $\mathbf{G}$ is finite, then $\mathbf{G}$ can be isomorphic to $\mathbf{G}'$ only if $\mathbf{G}'$ is also finite and the number of elements in $\mathbf{G}$ is equal to the number of elements in $\mathbf{G}'$. Otherwise, there will exist no mapping from $\mathbf{G}$ to $\mathbf{G}'$. which is one-one and onto.

**e.g. 1.** Consider the multiplicative group $\mathbf{G}$ of all $2 \times 2$ non-singular matrices whose elements ar real numbers. Let $\mathbf{G}'$ be the multiplicative group of non-zero real numbers.

Define a mapping $f : \mathbf{G} \to \mathbf{G}'$ such that

$$f(\mathbf{A}) = |\mathbf{A}| \text{ for } \mathbf{A} \in \mathbf{G}.$$

For any $p (\neq 0) \in \mathbf{G}'$, we can find a $2 \times 2$ matrix $\mathbf{P} \in \mathbf{G}$, such that $f(\mathbf{P}) = |\mathbf{P}| = p$.

$\therefore$ $f$ is onto.

Further : For $\mathbf{A}, \mathbf{B} \in \mathbf{G}, \mathbf{AB} \in \mathbf{G}$. Also $|\mathbf{A}| \neq 0$, $|\mathbf{B}| \neq 0$, $|\mathbf{AB}| \neq 0$.

$\therefore$ $f(\mathbf{AB}) = |\mathbf{AB}| = |\mathbf{A}|\,|\mathbf{B}| = f(\mathbf{A}) f(\mathbf{B})$.

$\therefore$ $f$ is a homomorphism from $\mathbf{G}$ onto $\mathbf{G}'$.

Also $\mathbf{G}'$ is the homomorph or homomorphic image of $\mathbf{G}$. i.e. $\mathrm{G} \cong \mathrm{G}'$.

**e.g. 2.** Let $\mathbf{G}$ be the additive group of integers and $\mathbf{G}'$ be the multiplicative group with elements 1 and $-1$ only. *(N.U. O 87)*

Define a mapping $f : \mathbf{G} \to \mathbf{G}'$ such that for $n \in \mathbf{G}$,

$$f(n) = \begin{cases} 1 \text{ when } n \text{ is even} \\ -1 \text{ when } n \text{ is odd} \end{cases}$$

For 1 or $-1$ in $\mathbf{G}'$ there is preimage (even number or odd number) in $\mathbf{G}$.

$\therefore$ $f$ is onto.

Let $p, q \in \mathbf{G}$. Then we have the following possibilities.

**Case (i)** Both $p$ and $q$ are even. $\therefore$ $p + q$ is even.

$\therefore$ $f(p) = 1,\ f(q) = 1,\ f(p + q) = 1 = 1.1 = f(p).f(q)$.

**Case (ii)** One of $p, q$ is even and the other is odd.

Let $p$ be even and $q$ be odd. $\therefore$ $p + q$ is odd.

$\therefore$ $f(p) = 1,\ f(q) = -1,\ f(p + q) = -1 = 1.-1 = f(p)\,f(q)$.

**Case (iii)** Both $p$ and $q$ are odd. $\therefore$ $p + q$ is even.

$$f(p) = -1,\ f(q) = -1,\ f(p + q) = 1 = (-1)(-1) = f(p)\,f(q).$$

$\therefore$ $f$ is a homomorphism of $\mathbf{G}$ onto $\mathbf{G}'$ i.e. $\mathbf{G} \simeq \mathbf{G}|$ i.e. $f$ is an epimorphism of $\mathbf{G}$ to $\mathbf{G}'$.

**e.g. 3.** Let $\mathbf{G}$ be the additive group of integers.

Let $\mathbf{G}' = \overline{\mathbf{Z}_m} = \{\bar{0},\ \bar{1},\ \bar{2},\ \ldots\ldots,\ \overline{m-1}\}$ be the group of residue classes modulo $m$ w.r.t. addition of residue classes (Theorem 15 Chapter 2).

Define a mapping $f : \mathbf{G} \to \mathbf{G}'$ such that $f(a) = \bar{a}$ for $a \in \mathbf{G}$. Every $a \in \mathbf{G}$ has a unique image in $\mathbf{G}'$. Similarly every element of $\mathbf{G}'$ is the image of some element in $\mathbf{G}$.

$\therefore$ $f$ is onto.

Also for $a, b \in \mathbf{G}$, $f(a+b) = \overline{a+b} = \bar{a} + \bar{b} = f(a) + f(b)$.

$\therefore$ $f$ is a homomorphism of $\mathbf{G}$ onto $\mathbf{G}'$.

**Note.** $f$ is not $1-1$. For if $a = mq + r$, $0 \le r < m$, then $\bar{a} = \bar{r}$, $a \ne r$.

**e.g. 4.** Let $\mathbf{G}$ be a multiplicative group with identity $e$.

Define a mapping $f : \mathbf{G} \to \mathbf{G}$ such that $f(a) = e$ for $a \in \mathbf{G}$.

For $a, b \in \mathbf{G}, ab \in \mathbf{G}$. $\therefore$ $f(a) = e, f(b) = e$

$\therefore$ $f(ab) = e = ee = f(a)f(b)$. $\therefore$ $f$ is a homomorphism from $\mathbf{G}$ into $\mathbf{G}$.

i.e. $f$ is an endomorphism in $\mathbf{G}$.

**e.g. 5.** Let $\mathbf{G}$ be the additive group on integers.

Define a mapping $f : \mathbf{G} \to \mathbf{G}$ such that for $a \in \mathbf{G}$, $f(a) = a + 2$.

For $a, b \in \mathbf{G}$, $a + b \in \mathbf{G}$. $\therefore$ $f(a) = a + 2$, $f(b) = b + 2$ and $f(a) + f(b) = a + b + 4$

$f(a + b) = a + b + 2$. But $f(a + b) \ne f(a) + f(b)$.

$\therefore$ $f$ is not a homomorphism.

**How to show that Groups are Isomorphic :** We now give an outline showing how to proceed from the definition to show that two groups $\mathbf{G}$ and $\mathbf{G}'$ are isomorphic.

**Step 1 :** We Define a function $f$ which gives the isomorphism of $\mathbf{G}$ with $\mathbf{G}'$.

**Step 2 :** We show that $f$ is one-to-one function.

**Step 3 :** We show that $f$ is onto $\mathbf{G}'$

**Step 4 :** We then show that $f(xy) = f(x)\, f(y)$

We illustrate this technique with some examples.

**e.g. 1.** The additive group $\mathbf{G} = \{....,-3,-2,-1,0,1,2,3,.....\}$ and the additive group $\mathbf{G}' = \{....,-2m,-m,0,m,2m,.....\}$ for any given integer $m$, are isomorphic.

**Sol.** Consider $f : \mathbf{G} \to \mathbf{G}'$ such that $f(a) = ma$ for $a \in \mathbf{G}, ma \in \mathbf{G}'$

Clearly $f$ is $1-1$ and onto. Let $a, b \in \mathbf{G}$. Then $ma, mb \in \mathbf{G}'$.

$\therefore$ $f(a+b) = m(a+b) = ma + mb = f(a) + f(b)$

$\Rightarrow$ $f$ is a homomorphism.

$\therefore$ $f$ is an isomorphism.

**e.g. 2.** $\mathbf{G}$ is a group of positive real numbers under multiplication. $\mathbf{G}'$ is a group of all real numbers under addition.

Let $f : \mathbf{G} \to \mathbf{G}'$ such that $f(x) = \log_{10} x$.

(i) Since for $a, b \in \mathbf{G}$, $a = b \Rightarrow \log_{10} a = \log_{10} b$, $f$ is a function from $\mathbf{G}$ to $\mathbf{G}'$.

(ii) Let $x_1, x_2 \in \mathbf{G}$. Then $f(x_1) = f(x_2) \Rightarrow \log_{10} x_1 + \log_{10} x_2$

$\Rightarrow 10^{\log_{10} x_1} = 10^{\log_{10} x_2} \Rightarrow x_1 = x_2 \Rightarrow f$ is $1-1$.

(iii) Let $y \in \mathbf{G}'$.

$\therefore$ $10^y$ is a positive real number i.e. $10^y \in \mathbf{G}$

$\therefore$ $f(10^y) = \log_{10}(10^y) = y$.

$\therefore$ For every $y \in \mathbf{G}', \exists\ 10^y \in \mathbf{G}$ such that $f(10^y) = y$. $\therefore$ $f$ is onto.

(iv) Let $a, b \mathbf{G}$. $\therefore$ $ab \in \mathbf{G}$. Also $f(a), f(b) \in \mathbf{G}'$

$\therefore$ $f(ab) = \log_{10} ab = \log_{10} a + \log_{10} b = f(a) + f(b)$.

$\therefore$ $f$ is a homomorphism from $\mathbf{G}$ into $\mathbf{G}'$.

$\therefore$ From (i), (ii), (iii), (iv) $f$ is an isomorphism from $\mathbf{G}$ to $\mathbf{G}'$. Thus $\mathbf{G} \cong \mathbf{G}'$.

**e.g. 3.** Let $\mathbf{G}$ be the additive group of integers and $\mathbf{G}'$ be the multiplicative group whose elements are $2^m$ for $m \in \mathbf{Z}$.

Consider the mapping $f : \mathbf{G} \to \mathbf{G}' / f(m) = 2^m$ for $m \in \mathbf{Z}$.

$f$ is one-to-one , $f$ is onto.

For $m, n \in \mathbf{G}$, $m + n \in \mathbf{G}$ and for $2^m, 2^n \in \mathbf{G}'$, $2^m . 2^n \in \mathbf{G}$

$\therefore$ $f(m + n) = 2^{m+n} = 2^m . 2^n = f(m) f(n)$.

$\therefore$ $f$ is a isomorphism of $\mathbf{G}$ into $\mathbf{G}'$.

**e.g. 4.** Let H be the subset of $\mathbf{M}_2(\mathbf{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbf{R}$. Show that $\phi : (\mathbf{C}, +) \to (\mathbf{H}, +)$ defined by $\phi(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ is an isomorphism

**Sol.** $(\mathbf{M}_2(\mathbf{R}), +)$ is a group and $\mathbf{H}$ be the subset of it. ***(O. U. 08)***

Let $x = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, y = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \in \mathbf{H}$

Clearly $y^{-1} = \begin{bmatrix} \frac{c}{k} & \frac{d}{k} \\ -\frac{d}{k} & \frac{c}{k} \end{bmatrix}$ when $k = c^2 + d^2$.

$$\therefore\ xy^{-1} = \begin{bmatrix} \frac{ac+bd}{k} & \frac{ad-bc}{k} \\ \frac{bc-ad}{k} & \frac{bd+ac}{k} \end{bmatrix} = \begin{bmatrix} \frac{ac+bd}{k} & -\left(\frac{bc-ad}{k}\right) \\ \frac{bc-ad}{k} & \frac{ac+bd}{k} \end{bmatrix} \in \mathbf{H}.$$

$\therefore$ $(\mathbf{H}, +)$ is a subgroup of $(\mathbf{M}_2(\mathbf{R}), +)$ and hence a group.

Also $(\mathbf{C}, +)$ is a group.

Now $\phi : (\mathbf{C}, +) \to (\mathbf{H}, +)$ defined by $\phi(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ is one - one and onto.

Let $a_1 + ib_1, a_2 + ib_2 \in \mathbf{C}$ where $a_1, b_1, a_2, b_2 \in \mathbf{R}$.

$\therefore$ $a_1 + ib_1 + a_2 + ib_2 = (a_1 + a_2) + i(b_1 + b_2) \in \mathbf{C}$.

$\therefore$ $\phi(a_1 + ib_1 + a_2 + ib_2) = \phi((a_1 + a_2) + i(b_1 + b_2))$

$$= \begin{pmatrix} a_1 + a_2 & -b_1 - b_2 \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} = \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \phi(a_1 + ib_1) + \phi(a_2 + ib_2)$$

$\Rightarrow \phi$ is an isomorphism.

**How to show that Groups are not Isomorphic :** Suppose two groups **G** and **G′** are given. If we want to show that **G** and **G′** are isomorphic we have to prove that there is no one-one function defined from **G** onto **G′** with the property $f(xy) = f(x)f(y)$.

If **G** and **G′** are of finite order and have different number of elements then there will not be any one-one function defined from **G** onto **G′**.

An algebraic property of a group is one whose definition is just in terms of the binary operation of the group and does not depend on the names of some other non-structural characteristics of the elements. To show that two groups **G** and **G′** are not isomorphic though there is a one-one mapping from **G** onto **G′**, we prove one group has some algebraic property that the other does not possess, that is **G** and **G′** are not structurally the same.

**e.g.1 :** Let $\mathbf{G} = \bar{\mathbf{Z}}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ with modulo addition. **G′** = $\mathbf{S}_6$ = Group of all permutations on six symbols. Since the number of elements in **G** is 4 and in **G′** is 6 !. It is not possible to define a one-one function from **G** to **G′**. Hence an isomorphism cannot be defined from **G** to **G′**. Thus **G** is not isomorphic to **G′**.

**e.g.2 :** Consider **G** = **Z** and **G′** = **Q**, both under the operation addition. Since **Z** is cyclic (Art. 8.2) and **Q** is not cyclic, they are not isomorphic.

**e.g.3 :** Let **G** = **Q*** = set of all non-zero rational numbers and **G′** =**R*** = set of all non-zero real numbers both under multiplication. The equation $x^3 = 2$ has a solution in **R*** but the equation has no solution in **Q***. Thus **G′** has an algebraic property which **G** does not have.

So **G′** and **G**, both under multiplication, are not isomorphic.

**e.g.4 :** **G** = $(\mathbf{Z}_4, +_4)$ is not isomorphic to **G′** = Klien - 4 group since **G** is cyclic and **G′** is not cyclic.

## 6. 2. PROPERTIES OF HOMOMORPHISM

**Theorem 1.** ***Let*** $(\mathbf{G}, .)$, $(\mathbf{G}', .)$ ***be two groups. Let*** $f$ ***be a homomorphism from*** **G** into **G'**. ***Then*** (i) $f(e) = e'$ ***where*** $e$ ***is the identity in*** **G** ***and*** $e'$ ***is the identity in*** **G'**.
(ii) $f(a^{-1}) = \{f(a)\}^{-1}$. ***(A.N.U.M.96, O91, S.K.U.O 02, O99, M 03, S.V.U. S 03, A 00, O.U. A 00, A 01, N.U. S 95)***

**Proof.** (i) $f(e) = f(ee)$

$\Rightarrow$ $f(ee) = f(e)$

$\Rightarrow$ $f(e)\,f(e) = e'\,f(e)$ [$\because$ $f$ is a homomorphism and $e', f(e) \in \mathbf{G}'$

$\Rightarrow$ $f(e) = e'$ (By right cancellation law in **G'**)

(iii) Let $a \in \mathbf{G}$. $\therefore$ $a^{-1} \in \mathbf{G}$ and $aa^{-1} = e$.

$\therefore$ $f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$ where $f(a).f(a'), e' \in \mathbf{G}'$

$\therefore$ $f(a^{-1}) = [f(a)]^{-1}$.

**Theorem 2.** ***If*** $f$ ***is a homomorphism from a group*** $(\mathbf{G}, .)$ ***into*** $(\mathbf{G}', .)$ ***then*** $(f(\mathbf{G}), .)$ ***is a subgroup of*** $\mathbf{G}'$. **OR** ***(O.U. 2001/0)***

***The homomorphic image of a group is a group.***

**Proof.** By definition, $f(\mathbf{G}) = \{f(a) / a \in \mathbf{G}\}$ and $f(\mathbf{G}) \subseteq \mathbf{G}'$

Let $a', b' \in f(\mathbf{G})$. $\therefore$ $\exists\ a, b \in \mathbf{G}$ such that $f(a) = a'$, $f(b) = b'$.

$\therefore\ a'(b')^{-1} = f(a)\{f(b)\}^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ ($\because$ $f$ is a homomorphism)

But $a, b \in \mathbf{G} \Rightarrow a, b^{-1} \in \mathbf{G} \Rightarrow ab^{-1} \in \mathbf{G}$.

$\therefore$ For $ab^{-1}$, $f(ab^{-1}) = a'(b')^{-1}$ and hence

$a'(b')^{-1} \in f(\mathrm{G})$ for $a', b' \in f(\mathbf{G})$.

Also $f(\mathbf{G}) \subseteq \mathbf{G}'$. $\therefore$ $f(\mathbf{G})$ is a subgroup of $(\mathbf{G}', .)$.

i.e. the homomorphic image of the group $\mathbf{G}$ is a subgroup of $\mathbf{G}'$.

i.e. the homomorphic image of a group is a group.

**Theorem 3.** ***Every homomorphic image of an abelian group is abelian.*** ***(A. U. M12, O.U. 2001/0)***

**Proof.** Let $(\mathbf{G}, .)$ be an abelian group and $(\mathbf{G}', .)$ be a group.

Let $f : \mathbf{G} \to \mathbf{G}'$ be a homomorphism onto.

$\therefore$ $\mathbf{G}'$ is the homomorphic image of $\mathbf{G}$ i.e. $\mathbf{G}' = f(\mathbf{G})$.

Let $a', b' \in \mathrm{G}'$. $\therefore$ $\exists$ elements $a, b \in \mathbf{G}$ such that $f(a) = a'$, $f(b) = b'$. Also $ab = ba$ since $\mathbf{G}$ is abelian.

$\therefore\ a'b' = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b'a'$.

$\therefore$ $\mathbf{G}'$ is abelian.

**Converse :** If the homomorphic image of a group is abelian then the group is abelian. The converse is not necessarily true.

Consider $\mathbf{P}_3 / \mathbf{A}_3$. (Ex. 15, chapter 2) It is the quotient group of $\mathbf{P}_3$ by $\mathbf{A}_3$ and is also the homomorphic image of the group $\mathbf{P}_3$ (Theorem 8). Now $\mathbf{P}_3 / \mathbf{A}_3$ is abelian whereas $\mathbf{P}_3$ is not abelian.

**Note.** Even $f$ is an isomorphism:

(i) Substitute 'isomorphism' for 'homomorphism' in theorem 1 and it is true. The same proof holds. ***(N.U. A 95)***

(ii) Substitute 'isomorphism' for 'homomorphism' in Theorem 2 and it is true. The same proof holds.

(iii) Substitute 'isomorphism' for 'homomorphism onto' in Theorem 3 and it is true. The same proof holds.

The converse of the Theorem 3 is not true.

## 6. 3. TRANSFERENCE OF GROUP STRUCTURES

**Theorem 4.** ***Let*** $\mathbf{G}$ ***be a group and*** $\mathbf{G}'$ ***be a non-empty set. If there exists a mapping*** $f$ ***of*** $\mathbf{G}$ ***onto*** $\mathbf{G}'$ ***such that*** $f(ab) = f(a)f(b)$ ***for*** $a, b \in \mathbf{G}$, ***then*** $\mathbf{G}'$ ***is a group.***

**Proof.** $f : \mathbf{G} \to \mathbf{G}'$ is onto such that $f(ab) = f(a)f(b)$ for $a, b \in \mathbf{G}$.

To prove that $\mathbf{G}'$ is a group we have to prove that the group-axioms are true in $\mathbf{G}'$.

**Closure.** Let $a', b' \in \mathbf{G}'$. Since $f$ is onto, $\exists\ a, b \in \mathbf{G}$ such that $f(a) = a'$ and $f(b) = b'$. Also $a, b \in \mathbf{G}$ and $f(ab) \in \mathbf{G}'$.

$\therefore \quad a'b' = f(a)f(b) = f(ab)$ i.e., $f(ab) = a'b'$. $\therefore\ a'b' \in \mathbf{G}'$.

**Associativity.** Let $a', b', c' \in \mathbf{G}'$. Since $f$ onto $\exists$ exist $a, b, c \in \mathbf{G}$ such that $f(a) = a'$, $f(b) = b'$, $f(c) = c'$.

Now $a'(b'c') = f(a)(f(b)f(c)) = f(a)f(bc) = f(a(bc))$

$= f((ab)c) = f(ab)f(c) = (f(a)f(b))f(c) = (a'b')c'$.

**Existence of identity.** Let $a' \in \mathbf{G}'$. Let $e$ be the identity in $\mathbf{G}$.

$\therefore \quad f(e) = e' \in \mathbf{G}'$. Also $\exists\ a \in \mathbf{G}$ such that $f(a) = a'$.

$\therefore \quad a'e' = f(a)f(e) = f(ae) = f(a) = a'$ and $e'a' = f(e)f(a) = f(ea) = f(a) = a'$.

$\therefore \quad a'e' = e'a' = a'$.

$\therefore$ Identity exists in $\mathbf{G}'$ and it is $f(e) = e'$.

**Existence of Inverse.** Let $a' \in \mathbf{G}'$. $\exists\ a \in \mathbf{G}$ such that $f(a) = a'$.

$\therefore \quad a^{-1} \in \mathbf{G}$ and $f(a^{-1}) \in \mathbf{G}'$.

$\therefore \quad f(a^{-1})a' = f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$ and

$a'f(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$

$\therefore \quad f(a^{-1})a' = a'f(a^{-1}) = e'$.

$\therefore \quad f(a^{-1})$ is the inverse of $a'$ in $\mathbf{G}'$.

$\therefore$ Every element of $\mathbf{G}'$ is invertible. $\therefore \quad \mathbf{G}'$ is a group.

**Note 1.** When $f$ is a one-one mapping of $\mathbf{G}$ onto $\mathbf{G}'$, this theorem is also true.

**2.** In $\mathbf{G}'$, inverse of $f(a)$ is $f(a^{-1})$.

## 6.4. KERNEL OF A HOMOMORPHISM

**Definition.** If $f$ is a homomorphism of a group $\mathbf{G}$ into a group $\mathbf{G}'$, then the set $\mathbf{K}$ of all those elements of $\mathbf{G}$ which are mapped by $f$ onto the identity $e'$ of $\mathbf{G}'$ is called the **Kernel** of the homomorphism $f$ i.e. Kernel $f = \{x \in \mathbf{G} \mid f(x) = e'\} = \mathbf{K}$.

***(A.N.M.05, K.U.M. 01, O.U.O 02, A. 02, M. 05, N.U. S 93, S.K.U. 01/0, S.V.U. 01)***

Sometimes Kernel $f$ is written as $\ker f$.

**Note.** If $e$ is the identity in $\mathbf{G}$, then $f(e) = e'$ i.e. $e \in \ker f$

Hence $\ker f$ is non-empty.

We know that the function defined over group of positive real numbers under multiplication to group of real numbers under addition such that $f(x) = \log x$ is a homomorphism. '0' is identity in $\mathbf{R}$. $f(1) = \log_a 1 = 0$ and 1 is the only element with this property.

**Ex. 1.** Consider the function $f$ from $<\mathbf{R}, +>$ to $<\mathbf{R}^+, +>$ defined as $f(x) = a^n, a > 0, \neq 1\ n \in \mathbf{Z}$. We know that $f(x)$ is a homomorphism. $f(0) = a^0 = 1$ where 1 as identity in $<\mathbf{R}^+, +>, 0$ is the only element with this property.

$\ker f = \{0\}$

**Ex. 2.** $\mathbf{G}$ is the additive group of the integers and $\mathbf{G}'$ be the multiplicative group with numbers 1 and $-1$. Define $f : \mathbf{G} \to \mathbf{G}'$ as follows : $f(n) = 1$, $n$ is even
$= -1$, $n$ is odd.

1 is the identity of $\mathbf{G}'$. We prove that $f$ is a homomorphism. $\ker f = \{n / n \text{ is even}\}$.

**Theorem 5.** ***If*** **f** ***is a homomorphism of a group*** **G** ***into a group*** **G'**, ***then the Kernel of*** **f** ***is a normal subgroup of*** **G.** ***(A.N.U. M05, S01, S 00, M98, M97, S96, A92, A90, O.U. M 08, O 02, A99, A.U.S. 00, M99, M98, S97, M97, K.U.J 03, M 01, O99, A98, A97, M 07,S.K.U. M 03, M 02, 01, A98, S.V.U. O 02, O 01, M 09)***

**Proof.** Let $e$ be the identity of $\mathbf{G}$ and $e'$ be the identity of $\mathbf{G}'$.

Also $f : \mathbf{G} \to \mathbf{G}'$ is a homomorphism. Let $\mathbf{K} = \ker f$.

$\therefore \quad \mathbf{K} = \{x \in \mathbf{G} \mid f(x) = e'\}$

Since $f(e) = e'$, $e \in \mathbf{K}$ i.e. $\mathbf{K}$ is non-empty.

Let $a, b \in \mathbf{K}$. $\quad \therefore f(a) = e', f(b) = e'$. Also $a, b \in \mathbf{G}$. $\quad \therefore ab^{-1} \in \mathbf{G}$.

Now $f(ab^{-1}) = f(a) f(b^{-1}) = f(a)[f(b)]^{-1} = e'(e')^{-1} = e'e' = e'$

$\therefore \quad ab^{-1} \in \mathbf{K}$. $\quad \therefore \quad \mathbf{K}$ is a subgroup of $\mathbf{G}$. $\quad$ Let $x \in \mathbf{G}$.

$\therefore \quad f(xax^{-1}) = f(x) f(a) f(x^{-1}) = f(x) e' \{f(x)\}^{-1}$

$= f(x)[f(x)]^{-1} = e' \quad \therefore \quad xax^{-1} \in \mathbf{K}$. $\quad \therefore \quad \mathbf{K}$ is normal in $\mathbf{G}$.

**Theorem 6.** ***The necessary and sufficient condition for a homomorphism*** **f** ***of a group*** **G** ***onto a group*** **G'** ***with kernel*** **K** ***to be an isomorphism of*** **G** ***into*** **G'** ***is that*** $\mathbf{K} = \{e\}$. ***(A.N.U.M. 01, S93, O85, A.U.M. 05, K.U.M. 04, S 00, O.U.A 02, O 00, A 00, S.K.U. M 02, A 01, A97, S.V.U. O 00)***

**Proof.** Let $f$ be a homomorphism of a group $\mathbf{G}$ onto a group $\mathbf{G}'$.

Let $e, e'$ be the identities in $\mathbf{G}, \mathbf{G}'$ respectively. Let $\mathbf{K}$ be the kernel of $f$.

Suppose that $f$ is an isomorphism of $\mathbf{G}$ onto $\mathbf{G}'$.

Then $f$ is $1-1$.

Let $a \in \mathbf{K}$. $\quad \therefore \quad f(a) = e' \Rightarrow f(a) = f(e) \Rightarrow a = e$.

$\therefore \quad e$ is the only element of $\mathbf{G}$ which belongs to $\mathbf{K}$. $\quad \therefore \quad \mathbf{K} = \{e\}$.

**Converse.** Suppose that $\mathbf{K} = \{e\}$.

Let $a, b \in \mathbf{G}$. Now $f(a) = f(b) \Rightarrow f(a)[f(b)]^{-1} = f(b)[f(b)]^{-1}$

$\Rightarrow f(a) f(b^{-1}) = e' \Rightarrow f(ab^{-1}) = e'$

$\Rightarrow ab^{-1} \in \mathbf{K} \Rightarrow ab^{-1} = e$

$\Rightarrow ab^{-1}b = eb \quad \Rightarrow ae = b \Rightarrow a = b$

$\therefore \quad f$ is $1-1$. $\quad \therefore \quad f$ is an isomorphism of $\mathbf{G}$ onto $\mathbf{G}'$.

**Theorem 6 (*a*).** ***Let f be a homomorphism froma group*** **G** ***into a group*** **G'** ***then f is monomorphism*** $\Leftrightarrow$ ***ker*** $f = \{e\}$ ***where*** $e \in \mathbf{G}$ ***is identity.***

*Proof follows from Theorem 6.* ***(O. U. M11, K.U.J. 03, M99, O98, A97)***

**Theorem 7.** *Let $f$ be a homomorphism from a group $\mathbf{G}$ onto a group $\mathbf{G}'$. Let $\ker f = \mathbf{K}$. Let $a$ be a given element of $\mathbf{G}$ such that $f(a) = a' \in \mathbf{G}'$. Then the set of all elements of $\mathbf{G}$ each element of which has the image $a'$ in $\mathbf{G}'$ is the coset $\mathbf{K}a$ of $\mathbf{K}$ in $\mathbf{G}$.*

**Proof.** Let $e$ be the identity in $\mathbf{G}$ and $e'$ be the identity in $\mathbf{G}'$. $\mathbf{K}$ is the kernel in $\mathbf{G}$.

Let $a \in \mathbf{G}$ such that $f(a) = a' \in \mathbf{G}'$. $\therefore \quad f^{-1}(a') = \{x \in \mathbf{G} \mid f(x) = a'\}$.

Now to prove that $f^{-1}(a') = \mathbf{K}a$.

Let $y \in \mathbf{K}a$. Then for some $k \in \mathbf{K}$, $y = ka$ and $f(k) = e'$.

$\therefore \quad f(y) = f(ka) = f(k).f(a) = e'f(a) = f(a) = a'$ i.e. $y \in f^{-1}(a')$.

$\therefore \quad \mathbf{K}a \subseteq f^{-1}(a') \qquad \ldots(1)$

Let $z \in f^{-1}(a')$. Then $f(z) = a'$.

$\therefore \quad f(za^{-1}) = f(z)f(a^{-1}) = a'[f(a)]^{-1} = f(a)[f(a)]^{-1} = e'$

$\therefore \quad za^{-1} \in \mathbf{K} \qquad \therefore \quad (za^{-1})\, a \in \mathbf{K}a \Rightarrow z \in \mathbf{K}a. \qquad \therefore \quad f^{-1}(a') \subseteq \mathbf{K}a \quad \ldots(2)$

From (1) and (2) $f^{-1}(a') = \mathbf{K}a$.

**Theorem 8.** *Let $\mathbf{G}$ be a group and $\mathbf{N}$ be a normal subgroup of $\mathbf{G}$. Let f be a mapping from $\mathbf{G}$ to $\mathbf{G/N}$ defined by $f(x) = \mathbf{N}x$ for $x \in \mathbf{G}$. Then f is a homomorphism of $\mathbf{G}$ onto $\mathbf{G/N}$ and $\ker f = \mathbf{N}$.* ***(A.N.U. S98, A91, O.U.M. 05, S.V.U. A 00)***

**Proof.** Let $f : \mathbf{G} \to \mathbf{G/N}$ such that $f(x) = \mathbf{N}x \; \forall \; x \in \mathbf{G}$.

Let $\mathbf{N}x \in \mathbf{G} \mid \mathbf{N}$. Then $x \in \mathbf{G}$ and $f(x) = \mathbf{N}x$. $\therefore \quad f$ is onto.

Let $a, b \in \mathbf{G}$. Then $ab \in \mathbf{G}$ and $f(ab) = \mathbf{N}ab = (\mathbf{N}a)(\mathbf{N}b)$

$= f(a)f(b)$ ($\because$ $\mathbf{N}$ is normal)

$\therefore \quad f$ is a homomorphism of $\mathbf{G}$ onto $\mathbf{G/N}$.

Let $\mathbf{K}$ be the kernel of $f$. The identity of the quotient group $\mathbf{G/N}$ is the coset $\mathbf{N}$.

$\therefore \quad \mathbf{K} = \{y \in \mathbf{G} / f(y) = \mathbf{N}\}$. Now to prove that $\mathbf{K} = \mathbf{N}$.

Let $k \in \mathbf{K}$. $\therefore \quad f(k) = \mathbf{N}$. But def. of $f$, $f(k) = \mathbf{N}k$ for $k \in \mathbf{G}$. ($\because \mathbf{K} \subseteq \mathbf{G}$)

Now $\mathbf{N} = \mathbf{N}k \Rightarrow k \in \mathbf{N}$. $\therefore \quad \mathbf{K} \subseteq \mathbf{N} \qquad \ldots(1)$

Let $n \in \mathbf{N}$. Then we have $f(n) = \mathbf{N}n = \mathbf{N}$. $\therefore \quad n \in \mathbf{K} \quad \therefore \quad \mathbf{N} \subseteq \mathbf{K} \quad \ldots(2)$

From (1) and (2), $\mathbf{K} = \mathbf{N}$.

**Definition :** [The mapping $f : \mathbf{G} \to \mathbf{G/N}$ such that $f(x) = \mathbf{N}x$ for $x \in \mathbf{G}$ is called **Natural** or **Canonical homomorphism.**]

**Ex. 1.** *If for a group $\mathbf{G}$, $f : \mathbf{G} \to \mathbf{G}$ is given by $f(x) = x^2$, $x \in \mathbf{G}$ is a homomorphism, prove that $\mathbf{G}$ is abelian.* ***(A.U. M12, A.01, K.U.M. 01, S.K.U.M 03, S.V.U. S 89, A 99)***

**Sol.** $f : \mathbf{G} \to \mathbf{G}$ such that $f(x) = x^2$, $x \in \mathbf{G}$ is a homomorphism.

$x, y \in \mathbf{G} \Rightarrow xy \in \mathbf{G} \qquad \therefore \quad f(x) = x^2, \; f(y) = y^2, \; f(xy) = (xy)^2$.

Since $f$ is a homomorphism, $f(xy) = f(x)f(y)$

$\Rightarrow \quad (xy)^2 = x^2y^2 \Rightarrow (xy)(xy) = (xx)(yy) \qquad \Rightarrow \quad x(yx)y = x(xy)y$

$\Rightarrow \quad yx = xy$ ($\therefore$ Cancellation laws are true in $\mathbf{G}$)

$\Rightarrow \quad \mathbf{G}$ is abelian.

**Ex. 2.** *Let* $\mathbf{G}$ *be a multiplicative group and* $f : \mathbf{G} \to \mathbf{G}$ *such that for* $a \in \mathbf{G}, f(a) = a^{-1}$. *Prove that* $f$ *is one-one onto. Also prove that* $f$ *is homomorphism iff* $\mathbf{G}$ *is commutative.* ***(N.U. M 82, S.V.U. S 89)***

**Sol.** $f : \mathbf{G} \to \mathbf{G}$ is a mapping such that $f(a) = a^{-1}$ for $a \in \mathbf{G}$.

(i) To prove that $f$ is $1-1$.

Let $a, b \in \mathbf{G}$. $\therefore$ $a^{-1}, b^{-1} \in \mathbf{G}$ and $f(a), f(b) \in \mathbf{G}$

Now $f(a) = f(b) \Rightarrow a^{-1} = b^{-1} \Rightarrow (a^{-1}) = (b^{-1}) \Rightarrow a = b$. $\therefore$ $f$ is $1-1$.

(ii) To prove that $f$ is onto.

Let $a \in \mathbf{G}$. $\therefore$ $a^{-1} \in \mathbf{G}$ such that $f(a^{-1}) = (a^{-1})^{-1} = a$. $\therefore$ $f$ is onto.

(iii) Suppose $f$ is a homomorphism.

For $a, b \in \mathbf{G}, ab \in \mathbf{G}$. Now $f(ab) = f(a) f(b)$

$\Rightarrow (ab)^{-1} = a^{-1}b^{-1} \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1} \Rightarrow ab = ba$. $\therefore$ $\mathbf{G}$ is abelian.

(iv) Suppose $\mathbf{G}$ is abelian.

For $a, b \in \mathbf{G}, f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a) f(b)$

$\therefore$ $f$ is a homomorphism.

**Ex. 3.** *It* $f : \mathbf{G} \to \overline{\mathbf{G}}$ *defined* $f(x) = 1$ *if* $x > 0$ *and* $-1$ *if* $x < 0$ *where* $\mathbf{G} =$ *{set of non-zero real numbers} and* $\overline{\mathbf{G}} = \{1, -1\}$ *are groups w.r.t. multiplication. Prove that* $f$ *is a homomorphism and find kernel.* ***(A. U. M11, O.U. A 97)***

**Sol.** Clearly $\mathbf{G} = \mathbf{R} - \{0\}, \overline{\mathbf{G}} = \{1, -1\}$ are groups w.r.t. multiplication. Identity in $\overline{\mathbf{G}} = 1$.

Let $x, y \in \mathbf{G}$. Then $f(x), f(y) \in \overline{\mathbf{G}}$.

(i) $x > 0,\ y > 0 \Rightarrow xy > 0$. $\therefore$ $f(x) = 1, f(y) = 1$ and $f(xy) = 1$

Now $f(xy) = 1 = (1)(1) = f(x) f(y)$

(ii) $x < 0,\ y < 0 \Rightarrow xy > 0$. $\therefore$ $f(x) = -1, f(y) = -1$ and $f(xy) = 1$.

Now $f(xy) = 1 = (-1)(-1) = f(x) f(y)$

(iii) $x > 0,\ y < 0$ or $x < 0,\ y > 0 \Rightarrow xy < 0$

$\therefore$ $f(x) = 1, f(y) = -1$ or $f(x) = -1, f(y) = 1$ and $f(xy) = -1$.

Now $f(xy) = -1 = (1)(-1)$ or $(-1)(1) = f(x) f(y)$

$\therefore$ From (i), (ii), (iii) we have $\forall\, x, y \in \mathbf{G}, f(xy) = f(x) f(y)$.

$\therefore$ $f$ is a homomorphism from $\mathbf{G}$ to $\overline{\mathbf{G}}$.

$\therefore$ $\ker f = \mathbf{K} = \{x \in \mathbf{G} / f(x) = 1,$ identity in $\overline{\mathbf{G}}\} = \{x \in \mathbf{G} / x > 0\}$.

**Note.** We give below the proof for $\ker f$ to be a normal subgroup.

Thus $\mathbf{K} = \ker f =$ set of $+ve$ real numbers.

Let $a, b \in \mathbf{K}$. $\therefore$ $f(a) = 1, f(b) = 1$ and $ab^{-1} \in \mathbf{G}$.

$\therefore$ $f(ab^{-1}) = f(a)\, f(b^{-1}) = f(a)\,[f(b)]^{-1} = (1)(1) = 1$

$\Rightarrow ab^{-1} \in \mathbf{K} \Rightarrow \mathbf{K}$ is a subgroup of G.

Let $x \in \mathbf{G}$. $\therefore$ $x\, a\, x^{-1} \in \mathbf{G}$. Now $f(x\, a\, x^{-1}) = f(x) f(a) f(x^{-1}) = f(x)(1)[f(x)]^{-1} = 1$.

$\therefore$ $x\, a\, x^{-1} \in \mathbf{K}$ and $\mathbf{K} = \ker f$ is a normal subgroup of $\mathbf{G}$.

**Ex. 4.** *Show that the group* $(\mathbf{G} = \mathbf{Z}_4 = \{0,1,2,3\},\ +_4)$ *and the group* $(\mathbf{G}' = \{1, -1,\ i, -i\},\ .)$ *are isomorphic* ***(A. U. M 12, O.U. 91)***

**Sol.** We have to find an isomorphism $f$ from $\mathbf{G}$ to $\mathbf{G}'$ such that $f$ is one-one onto.

$(\mathbf{G}, +_4)$

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$(\mathbf{G}',\ .)$

| $\bullet$ | 1 | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| 1 | 1 | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | 1 | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | 1 |
| $-i$ | $-i$ | $i$ | 1 | $-1$ |

Identity in $\mathbf{G}$ is 0 and identity in $\mathbf{G}'$ is 1.

Let $f(0) = 1$ and $f(a^{-1}) = [f(a)]^{-1}$ for $a \in \mathbf{G}$.

We note the fact that an isomorphism is also a homomorphism.

Now define : $f(1) = i, f(3) = -i, f(2) = -1$.

Since the image of an inverse must be equal to the inverse of the image.

$$f(3) = f(1^{-1}) = [f(1)]^{-1} = i^{-1} = -i,$$

$$f(2) = f(2^{-1}) = [f(2)]^{-1} = (-1)^{-1} = -1.$$

For $a, b \in \mathbf{G}$, $f(a +_4 b) = f(a) f(b)$

Since $f(0 +_4 2) = f(2) = -1$, $f(0) f(2) = 1(-1) = -1$ etc.

$\therefore$ $f$ is a homomorphism. Also $f$ is one-one and onto.

Thus $f : \mathbf{G} \to \mathbf{G}'$ is an isomorphism such that

$f(0) = 1,\ f(1) = i, f(2) = -1, f(3) = -i.$ $\therefore$ $\mathbf{G} \cong \mathbf{G}'$.

**Ex. 5.** *Let* $\mathbf{A} = \{a, b, c\}$. *Let* $\mathbf{G} = \{\alpha, \beta, \gamma\}$ *so that* $\alpha, \beta, \gamma$ *are bijections on* $\mathbf{A}$ *such that* $\alpha = \{(a,a),(b,b),(c,c)\}, \beta = \{(a,b),(b,c),(c,a)\}, \gamma = \{(a,c),(b,a),(c,b)\}$. *Now* $\mathbf{G}$ *is an abelian group w.r.t. composition of mappings. Let* $\mathbf{G}' = \{1, \omega, \omega^2\}$ *where* $\omega, \omega^2$ *are the complex cube roots of unity. Now* $\mathbf{G}'$ *is an abelian group under multiplication. Show that* $\mathbf{G} \cong \mathbf{G}'$.

**Sol.** $(\mathbf{G},\ o)$ is a group

| 0 | $\alpha$ | $\beta$ | $\gamma$ |
|---|---|---|---|
| $\alpha$ | $\alpha$ | $\beta$ | $\gamma$ |
| $\beta$ | $\beta$ | $\gamma$ | $\alpha$ |
| $\gamma$ | $\gamma$ | $\alpha$ | $\beta$ |

Here $\beta^{-1} = \gamma$ $\gamma^{-1} = \beta$

$\alpha$ is the identity in $\mathbf{G}$.

$(\mathbf{G}',\ .)$ is a group

| | 1 | $\omega$ | $\omega^2$ |
|---|---|---|---|
| 1 | 1 | $\omega$ | $\omega^2$ |
| $\omega$ | $\omega$ | $\omega^2$ | 1 |
| $\omega^2$ | $\omega^2$ | 1 | $\omega$ |

Here $\omega^{-1} = \omega^2$ and $(\omega^2)^{-1} = \omega$

1 is the identity in $\mathbf{G}'$.

Now we have to produce $1-1$ homomorphism $f$ from $\mathbf{G}$ onto $\mathbf{G}'$. Let $f(\alpha) = 1$ and $f(a^{-1}) = [f(a)]^{-1}$ for $a \in \mathbf{G}$. We note the fact that an isomorphism is also a homomorphism.

Now define : $f(\alpha) = 1, f(\beta) = \omega, f(\gamma) = \omega^2$

Observe that $f(\beta) = f(\gamma^{-1}) = [f(\gamma)]^{-1} = (\omega^2)^{-1} = \omega$ and

$$f(\gamma) = f(\beta^{-1}) = [f(\beta)]^{-1} = (\omega)^{-1} = \omega^2 .$$

For $a, b \in \mathbf{G}$, $f(aob) = f(a).f(b)$

since $f(\beta o\gamma) = f(\alpha) = 1, f(\beta)f(\gamma) = \omega\omega^2 = \omega^2 = 1$ etc.

$\therefore$ $f$ is a homomorphism. Also $f$ is one-one and onto.

Thus $f : \mathbf{G} \to \mathbf{G}'$ is an isomorphism such that

$$f(\alpha) = 1, f(\beta) = \omega, f(\gamma) = \omega^2 . \qquad \therefore \quad \mathbf{G} \cong \mathbf{G}'.$$

**Ex. 6.** *Let* $(\mathbf{G}, +)$ *is a group of real numbers under addition and* $(\mathbf{G}', .)$ *is a group of positive real numbers under multiplication.*

*Let* $f : \mathbf{G} \to \mathbf{G}'$ *be a mapping such that* $f(x) = e^x$ *for* $x \in \mathbf{G}$. *Show that* $f$ *is an isomorphism.* ***(K.U.J 02, N.U. O 85, O91)***

**Sol.** If $x$ is a real number, $e^x > 0$ and hence $e^x \in \mathbf{G}'$

Let $a, b \in \mathbf{G}$. $\therefore$ $e^a, e^b \in \mathbf{G}'$. Now $e^a = e^b \Rightarrow a = b$ $\therefore$ $f$ is one-one.

Let $c \in \mathbf{G}'$, i.e. $c$ is a positive real number and $\log c$ is a real number, positive or negative or zero.

Also $\log c \in \mathbf{G}$.

$\therefore$ $f(\log c) = e^{\log c} = c$. Thus $\exists \log c \in \mathbf{G}$ such that $f(\log c) = c$.

$\therefore$ $f$ is onto.

Let $a, b \in \mathbf{G}$. $\therefore$ $a + b \in \mathbf{G}$.

Then $f(a + b) = e^{a+b} = e^a e^b = f(a) f(b)$.

$\therefore$ $f$ is a homomorphism which is one-one and onto.

$\therefore$ $f : \mathbf{G} \to \mathbf{G}'$ is an isomorphism.

**Note.** $\ker f = \{0\}$ since 0 is the identity in $\mathbf{G}$, 1 is the identity in $\mathbf{G}'$, and $e^0 = 1$.

**Ex. 7.** *If* $f$ *is a homomorphism of* $\mathbf{G}$ *onto* $\mathbf{G}'$ *and* $g$ *a homomorphism of* $\mathbf{G}'$ *onto* $\mathbf{G}''$, *show that* $gof$ *is a homomorphism of* $\mathbf{G}$ *onto* $\mathbf{G}''$. *Also show that the kernel of* $f$ *is a subgroup of the kernel of* $gof$.

**Sol.** $f : \mathbf{G} \to \mathbf{G}'$ is a homomorphism of $\mathbf{G}$ onto $\mathbf{G}'$ and

$g : \mathbf{G}' \to \mathbf{G}''$ is a homomorphism of $\mathbf{G}'$ onto $\mathbf{G}''$.

$\therefore$ $gof : \mathbf{G} \to \mathbf{G}''$ is a mapping of $\mathbf{G}$ onto $\mathbf{G}''$ such that

$(gof)(x) = g(f(x))$ for $x \in \mathbf{G}$.

Let $a, b \in \mathbf{G}$.

Then $(gof)(ab) = g(f(ab)) = g(f(a)f(b))$ ($\because$ $f$ is a homomorphism)

$= g(f(a))\, g(f(b))$ ($\therefore$ $g$ is homomorphism)

$= [(gof)(a)]\, [(gof)(b)]$

$\therefore$ $gof$ is a homomorphism from $\mathbf{G}'$ onto $\mathbf{G}''$.

Let $e'$ be the identity in $\mathbf{G}'$. If $\mathbf{K}'$ is the kernel of $f$ then

$$\mathbf{K}' = \{y \in \mathbf{G} / f(y) = e'\} .$$

Let $e''$ be the identity in $\mathbf{G}''$. If $\mathbf{K}''$ is the kernel of $gof$ then

$$\mathbf{K}'' = \{z \in \mathbf{G} / (gof)(z) = e''\}.$$

To show that the kernel of $f$ is a subgroup of the kernel of $gof$ i.e. to show that $\mathbf{K}' \subseteq \mathbf{K}''$.

Let $k' \in \mathbf{K}'$. $\therefore$ $f(k') = e'$. Also $k' \in \mathbf{G}$.

Now $(gof)(k') = g(f(k')) = g(e') = e''$ ($\because$ $g$ is a homomorphism)

$\therefore$ $k' \in \mathbf{K}''$. Thus $k' \in \mathbf{K}' \Rightarrow k' \in \mathbf{K}''$. $\therefore$ $\mathbf{K}' \subseteq \mathbf{K}''$.

**Ex. 8.** *Show that the mapping $f : \mathbf{G} \to \mathbf{G}'$ such that $f(x+iy) = x$ where $\mathbf{G}$ is a group of complex numbers under addition, $\mathbf{G}'$ is a group of real numbers under addition, is a homomorphism onto and find* ker $f$. ***(O.U. 93)***

**Sol.** Let $a = a_1 + ib_1$, $b = a_2 + ib_2 \in \mathbf{G}$

$\therefore$ $a + b \in \mathbf{G}$, $f(a) = f(a_1 + ib_1) = a_1$ and $f(b) = f(a_2 + ib_2) = a_2$

Now $f(a+b) = f((a_1 + a_2) + i\,(b_2 + b_1)) = a_1 + a_2 = f(a) + f(b)$

$\therefore$ $f$ is a homomorphism.

If $c$ is any real number then $c \in \mathbf{G}'$ and $c + iy \in \mathbf{G}$

so that $f(c+iy) = c$ for $y \in \mathbf{R}$. $\therefore$ $f$ is onto.

$\therefore$ $f$ is a homomorphism from $\mathbf{G}$ onto $\mathbf{G}'$.

The identity in $\mathbf{G}'$ is 0.

Since ker $f = (x + iy \in \mathbf{G} / f(x+iy) = x = 0)$ we have ker $f = \{0 + iy / y \in \mathbf{R}\}$.

**Note.** We give below the proof for ker $f$ to be a normal subgroup.

Thus $\mathbf{K} = \ker f = \{0 + iy / y \in \mathbf{R}\}$.

Let $z_1, z_2 \in \mathbf{K}$. $\therefore$ $f(z_1) = 0, f(z_2) = 0$ and $z_1 z_2^{-1} \in \mathbf{G}$.

$\therefore$ $f(z_1 z_2^{-1}) = f(z_1) f(z_2^{-1}) = f(z_1)\,[f(z_2)]^{-1} = (0)\,(0) = 0$

$\Rightarrow z_1 z_2^{-1} \in \mathbf{K} \Rightarrow \mathbf{K}$ is a subgroup of G.

Let $z \in \mathbf{G}$ and $z_1 \in \mathbf{K}$.

$\therefore$ $z\, z_1\, z^{-1} \in \mathbf{G}$.

$\therefore$ $f(z\, z_1\, z^{-1}) = f(z) f(z_1) f(z^{-1}) = f(z)\,(0)\,[f(z)]^{-1} = 0 \Rightarrow z z_1 z^{-1} \in \mathbf{K}$.

$\therefore$ $\mathbf{K} = \ker f$ is a normal subgroup of G.

**Ex. 9.** *Show that the mapping $f : \mathbf{G} \to \mathbf{G}'$ such that $f(z) = |z|$, for $z \in \mathbf{G}$ where $\mathbf{G}$ is a multiplicative group of non-zero complex numbers and $\mathbf{G}'$ is a multiplicative group of non-zero real numbers, is a homomorphism. Find* ker $f$.

**Sol.** Let $z_1, z_2 \in \mathbf{G}$.

$\therefore$ $f(z_1) = |z_1|, f(z_2) = |z_2|$

Now $f(z_1 z_2) = |z_1 z_2| = |z_1|\,|z_2| = f(z_1) f(z_2)$.

The identity in $\mathbf{G}'$ is 1.

$\therefore$ ker $f = \{a + ib$ such that $|a + bi| = \sqrt{a^2 + b^2} = 1\}$.

**Ex. 10.** *If* $\phi : \mathbf{Z}_{10} \to \mathbf{Z}_{20}$ *be a homomorphism defined by* $\phi(1) = 8$, *then find* $\ker f$ *and* $\phi(3)$. ***(S. V. U. M11, K. U. 07)***

**Sol.** $(\mathbf{Z}_{10} = \{0,1,2,3,.....,9\}, +_{10}), (\mathbf{Z}_{20} = \{0,1,2,....,20\}, +_{20})$ are two cyclic groups and $\phi : \mathbf{Z}_{10} \to \mathbf{Z}_{20}$.

Also 0 is identity in $\mathbf{Z}_{10}$ and 0 is identity in $\mathbf{Z}_{20}$ such that $\phi(0) = 0$.

Given $\phi(1) = 8$.

Now
$$\phi(2) = \phi(1 +_{10} 1) = \phi(1) +_{20} \phi(1) = 8 +_{20} 8 = 16,$$
$$\phi(3) = \phi(1 +_{10} 2) = \phi(1) +_{20} \phi(2) = 8 +_{20} 16 = 4,$$
$$\phi(4) = \phi(1 +_{10} 3) = \phi(1) +_{20} \phi(3) = 8 +_{20} 4 = 12,$$
$$\phi(5) = \phi(1 +_{10} 4) = \phi(1) +_{20} \phi(4) = 8 +_{20} 12 = 0,$$
$$\phi(6) = \phi(1 +_{10} 5) = \phi(1) +_{20} \phi(5) = 8 +_{20} 0 = 8,$$
$$\phi(7) = \phi(1 +_{10} 6) = \phi(1) +_{20} \phi(6) = 8 +_{20} 8 = 16,$$
$$\phi(8) = \phi(1 +_{10} 7) = \phi(1) +_{20} \phi(7) = 8 +_{20} 16 = 4,$$
$$\phi(9) = \phi(1 +_{10} 8) = \phi(1) +_{20} \phi(8) = 8 +_{20} 4 = 12.$$

$\therefore$ Ker $\phi = \{0,5\}$ and $\phi(3) = 4$.

**Ex. 11.** $(\mathbf{Z}, +), (\mathbf{G} = \{1, -1, i, -i\}, \cdot)$ *where* $i^2 = -1$, *are groups. Show that* $f : \mathbf{Z} \to \mathbf{G}$ *defined by* $f(n) = i^n \ \forall\ n \in \mathbf{Z}$ *is an onto homomorphism. Also find* $\ker f$.

**Sol.** When $n$ is an integer, $1 = i^{4n}, -1 = i^{4n-2}, -i = i^{4n-1}, i = i^{4n+1}$

It is clear that $f$ is onto but not one-one.

For $a, b \in \mathbf{Z}, a + b \in \mathbf{Z}$ and $f(a+b) = i^{a+b} = i^a . i^b = f(a) . f(b)$

$\therefore$ $f : \mathbf{Z} \to \mathbf{G}$ is an onto homomorphism.

Ker $f = \{n \in \mathbf{Z} / f(n) = 1\}$ where 1 is the identity in $\mathbf{G}$.

Since $f(4n) = i^{4n} = (i^4)^n = 1$ for $n \in \mathbf{Z}$. Ker $f = \{4n / n \in \mathbf{Z}\}$.

## 6.5. FUNDAMENTAL THEOREM ON HOMOMORPHISM OF GROUPS *(N.U. A 95)*

**Theorem 9.** ***Every homomorphic image of a group*** $\mathbf{G}$ ***is isomorphic to some quotient group of*** $\mathbf{G}$. **OR**

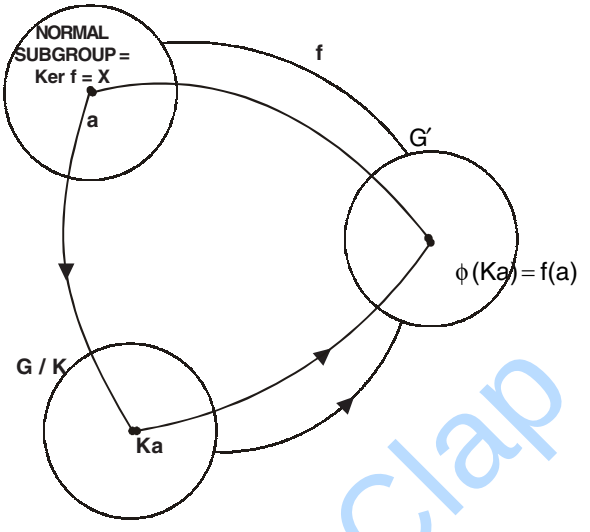
***If*** $\phi$ ***is a homomorphism from a group*** $\mathbf{G}$ ***onto a group*** $\mathbf{G}'$, ***then*** $\mathbf{G} / \ker \phi$ ***is isomorphic with*** $\mathbf{G}'$. **OR**

***If*** $f : \mathbf{G} \to \mathbf{G}'$ ***is a homomorphism and onto with kernel*** $\mathbf{K}$, ***then prove that*** $\mathbf{G} / \mathbf{K} \cong \mathbf{G}'$. ***(S.K.U. M 09, M 05, O 02, O 00, O99, A98, S.V.U. M 01, A99, O97, A.N.U. M11, M12, 07, M 01, M 00, M96, A93, O92, A91, O90, O89, A.U.A 03, A 02, O 01, M 00, S99, M97, S96, A96, K.U. 08, A 02, O97, O96, M96, O.U.O 03, M 01, A 00)***

**Proof.** Let $f$ be a homomorphism from a group $\mathbf{G}$ onto a group $\mathbf{G}'$

$\therefore\ \mathbf{G} \simeq \mathbf{G}'$ ($\mathbf{G}'$ is the homomorphic image of $\mathbf{G}$ under $f$)

(We change $\mathbf{G}'$ to $\phi(\mathbf{G})$ if need be)




Let $\ker f = \mathbf{K}$. Then $\mathbf{K}$ is a normal subgroup of $\mathbf{G}$ and $\mathbf{G/K}$ is the quotient group of $\mathbf{G}$ by $\mathbf{K}$.

Now we shall prove that $\dfrac{\mathbf{G}}{\mathbf{K}} \cong \mathbf{G}$. For $a \in \mathbf{G}$, $\mathbf{K}a \in \mathbf{G/K}$ and $f(a) \in \mathbf{G}'$.

Define a mapping $\phi : \mathbf{G/K} \to \mathbf{G}'$ such that $\phi(\mathbf{K}a) = f(a)$ for $a \in \mathbf{G}$.

For $a, b \in \mathbf{G}$, $\mathbf{K}a = \mathbf{K}b \Rightarrow ab^{-1} \in \mathbf{K} \Rightarrow f(ab^{-1}) = e'$

$\Rightarrow f(a)f(b^{-1}) = e'$ where $e'$ is the identity $\mathbf{G}'$.

$\Rightarrow f(a)f(b^{-1})f(b) = e'f(b)$

$\Rightarrow f(a)e' = f(b) \Rightarrow f(a) = f(b) \Rightarrow \phi(\mathbf{K}a) = \phi(\mathbf{K}b)$.

$\therefore\ \phi$ is well defined.

(ii) To prove that $\phi$ is $1-1$

For $a, b \in \mathbf{G}$, $\mathbf{K}a, \mathbf{K}b \in \mathbf{G/K}$. Now $\phi(\mathbf{K}a) = \phi(\mathbf{K}b) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a)\{f(b)\}^{-1} = f(b)[f(b)]^{-1} \Rightarrow f(a)f(b^{-1}) = e'$

$\Rightarrow f(ab^{-1}) = e' \Rightarrow ab^{-1} \in \mathbf{K} \Rightarrow \mathbf{K}a = \mathbf{K}b$

$\therefore\ \phi$ is $1-1$.

(iii) To prove that $\phi$ is onto.

Let $x \in \mathbf{G}'$. Since $f : \mathbf{G} \to \mathbf{G}'$ is onto. $\exists\ a \in \mathbf{G}$ such that $f(a) = x$.

$\therefore\ \mathbf{K}a \in \mathbf{G/K}$ and so $\phi(\mathbf{K}a) = f(a) = x$. $\therefore\ \phi$ is onto.

(iv) To prove that $\phi$ is a homomorphism.

For $a, b \in \mathbf{G}$, $\mathbf{K}a, \mathbf{K}b \in \mathbf{G/K}$.

Now $\phi[(\mathbf{K}a)(\mathbf{K}b)] = \phi(\mathbf{K}ab)$ ($\because$ coset multiplication is defined in $\mathbf{G/K}$)

$= f(ab) = f(a)f(b) = \phi(\mathbf{K}a)\phi(\mathbf{K}b)$

$\therefore\ \phi$ is an isomorphism from $\mathbf{G/K}$ onto $\mathbf{G}'$. $\therefore\ \mathbf{G/K} \cong \mathbf{G}'$.

**Note.** By the fundamental theorem of homomorphism, $\mathbf{G}$ is homomorphic to $\mathbf{G}'$ and $\frac{\mathbf{G}}{\mathbf{N}} \cong \mathbf{G}'$ where $\mathbf{N}$ is a normal subgroup of $\mathbf{G}$.

$\therefore$ The set of homomorphic images of $\mathbf{G}$ is having $1-1$ correspondence to the set of quotient groups of $\mathbf{G}$. In other words, the number of all possible homomorphic images of a group is same as the number of quotient groups of $\mathbf{G}$.

Conversely, for every normal subgroup of $\mathbf{G}$ we have a quotient group of $\mathbf{G}$ and hence a homomorphic image of $\mathbf{G}$. In other words the number of normal subgroups of $\mathbf{G}$ is same as the number of homomorphic images of $\mathbf{G}$.

## 6.6. AUTOMORPHISM OF A GROUP

**Definition.** If $f : \mathbf{G} \to \mathbf{G}$ is an isomorphism from a group $\mathbf{G}$ to itself, then $f$ is called an **automorphism** of $\mathbf{G}$.

**e.g.** Let $f : \mathbf{Z} \to \mathbf{Z}$ be a mapping such that $f(x) = -x$ for $x \in \mathbf{Z}$ where $\mathbf{Z}$ is an additive group of integers.

Now : (i) $x_1, x_2 \in \mathbf{Z} \Rightarrow -x_1, -x_2 \in \mathbf{Z}$ and $-x_1 = -x_2 \Rightarrow x_1 = x_2$

(ii) For $x \in \mathbf{Z}$ (co-domain), $\exists -x \in \mathbf{Z}$ (domain) so that $f(-x) = -(-x) = x$.

(iii) $x_1, x_2 \in \mathbf{Z} \Rightarrow x_1 + x_2 \in \mathbf{Z}$ and $f(x_1 + x_2)$

$= -(x_1 + x_2) = (-x_1) + (-x_2) = f(x_1) + f(x_2)$.

Hence we infer that $f$ is an automorphism of $\mathbf{Z}$.

**Ex. 12.** *If $\mathbf{G}$ is an additive group of complex numbers, show that $f : \mathbf{G} \to \mathbf{G}$ such that $f(z) = pz$ ($p$ is a non-zero complex number) for $z \in \mathbf{G}$ is an automorphism of $\mathbf{G}$.*

**Sol.** Let $z_1, z_2 \in \mathbf{G}$ (domain). $\therefore$ $f(z_1) = pz_1, f(z_2) = pz_2 \in \mathbf{G}$ (co-domain)

Now $f(z_1) = f(z_2) \Rightarrow pz_1 = pz_2 \Rightarrow z_1 = z_2$.

Let $z' \in \mathbf{G}$ (co-domain). $\exists \frac{z'}{p} \in \mathbf{G}$ (domain) $(\because p \neq 0)$

such that $f\left(\frac{z'}{p}\right) = p \cdot \frac{z'}{p} = z'$.

Also $f(z_1 + z_2) = p(z_1 + z_2) = pz_1 + pz_2 = f(z_1) + f(z_2)$.

Hence $f$ if an automorphism of $\mathbf{G}$.

**Ex. 13.** *Show that the mapping $f : \mathbf{G} \to \mathbf{G}$ such that $f(a) = a^{-1}\ \forall\, a \in \mathbf{G}$, is an automorphism of a group $\mathbf{G}$ iff $\mathbf{G}$ is abelian.* ***(N.U. O 88, A 92, 90, S20, S.K.U O 03)***

**Sol.** Let $f : \mathbf{G} \to \mathbf{G}$ such that $f(a) = a^{-1}$ for $a \in \mathbf{G}$.

(i) Let $f$ be an automorphism. To prove that $\mathbf{G}$ is abelian.

Let $x, y \in \mathbf{G}$, $\therefore$ $xy \in \mathbf{G}$

$\therefore$ $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = f(y)f(x) = f(yx)$ $(\because$ $f$ is a homomorphism)

$\Rightarrow xy = yx$ $(\because$ $f$ is $1-1)$

$\Rightarrow$ $\mathbf{G}$ is abelian.

(ii) Let $\mathbf{G}$ be abelian. To prove that $f$ is an automorphism in $\mathbf{G}$.

Let $x, y \in \mathbf{G}$. $\therefore \quad xy = yx$

Since $f(x) = f(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y$, $f$ is $1-1$.

For $x \in \mathbf{G}$, $x^{-1} \in \mathbf{G}$ Also $f(x^{-1}) = (x^{-1})^{-1} = x$. $\therefore$ $f$ is onto.

For $x, y \in \mathbf{G}$, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$ ($\because$ $\mathbf{G}$ is abelian)

$= f(x)f(y)$

$\therefore$ $f$ is composition preserving. $\therefore$ $f$ is an automorphism of $\mathbf{G}$.

**Ex. 14.** *Let $\mathbf{G}$ be a group and $\mathbf{H}$ a subgroup of $\mathbf{G}$. Let $f$ be an automorphism of $\mathbf{G}$ and $f(\mathbf{H}) = \{f(h) / h \in \mathbf{H}\}$. Prove that $f(\mathbf{H})$ is a subgroup of $\mathbf{G}$.*

**Sol.** $\mathbf{H}$ is a subgroup of the group $\mathbf{G}$. $f$ is an automorphism of $\mathbf{G}$ and $f(\mathbf{H}) = \{f(h) / h \in \mathbf{H}\}$.

Let $a, b \in \mathbf{H}$. $\therefore$ $ab^{-1} \in \mathbf{H}$ and $f(a), f(b) \in f(\mathbf{H})$.

$\therefore$ $f(ab^{-1}) \in f(\mathbf{H}) \Rightarrow f(a)f(b^{-1}) \in f(\mathbf{H}) \Rightarrow f(a)[f(b)]^{-1} \in f(\mathbf{H})$.

Since $f$ is automorphism and $x, y \in f(\mathbf{H}) \Rightarrow xy^{-1} \in f(\mathbf{H})$.

$\therefore$ $f(\mathbf{H})$ is a subgroup of $\mathbf{G}$.

## 6.7. GROUPS OF AUTOMORPHISMS OF GROUPS

**Theorem 10.** ***The set of all automorphisms of a group $\mathbf{G}$ forms a group w.r.t. compositions of mappings.*** ***(S.V.U. A 97, N.U. O 88, S 84, 92, M 05, A.U.O 01)***

**Proof.** Let $\mathbf{A}(\mathbf{G}) = \{ f : f$ is an automorphism of $\mathbf{G} \}$

Here $f : \mathbf{G} \to \mathbf{G}$ is a one-one onto homomorphism.

Let '$o$' be the composition of bijections over $\mathbf{G}$.

**Closure.** Let $f, g \in \mathbf{A}(\mathbf{G})$. $\therefore$ $f, g$ are bijections and hence $gof$ is a bijection.

Let $a, b \in \mathbf{G}$. $\therefore$ $(gof)(ab) = g(f(ab)) = g(f(a)f(b))$

$= [g(f(a))][g(f(b))] = [(gof)(a)][(gof)(b)]$

$\therefore$ $gof$ is a homomorphism of $\mathbf{G}$ and hence an automorphism of $\mathbf{G}$.

$\therefore$ $gof \in \mathbf{A}(\mathbf{G})$.

**Asssociativity.** Composition of mappings in $\mathbf{A}(\mathbf{G})$ is associative.

**Existence of identity.** Let $\mathrm{I} : \mathbf{G} \to \mathbf{G}$ be the identity mapping. Since $\mathrm{I}$ is one-one, onto and structure preserving, $\mathrm{I} \in \mathbf{A}(\mathbf{G})$. Since for $f \in \mathbf{A}(\mathbf{G})$, $f o \mathrm{I} = \mathrm{I} o f = f$, identity exists in $\mathbf{A}(\mathbf{G})$ and it is $\mathrm{I}$.

**Existence of inverse.** Let $f \in \mathbf{A}(\mathbf{G})$.

$\therefore$ $f$ is one-one onto in $\mathbf{G}$ and hence $f^{-1}$ exists and it is one-one onto in $\mathbf{G}$. We have to show that $f^{-1}$ is a homomorphism.

Let $f^{-1}(a) = a'$, $f^{-1}(b) = b'$ for $a', b' \in \mathbf{G}$ $\therefore$ $f(a') = a, f(b') = b$.

Now $f^{-1}(ab) = f^{-1}(f(a')f(b'))$

$= f^{-1}(f(a'b')) = (f^{-1}f)(a'b') = a'b' = f^{-1}(a)f^{-1}(b)$.

$\therefore$ $f^{-1}$ is a homomorphism and hence an automorphism in $\mathbf{G}$. i.e. $f^{-1} \in \mathbf{A}(\mathbf{G})$ such that $f f^{-1} = f^{-1} f = \mathrm{I}$.

$\therefore$ Every element of $\mathbf{A}(\mathbf{G})$ is invertible.

$\therefore$ $\mathbf{A}(\mathbf{G})$ is a group w.r.t. composition of mappings in $\mathbf{G}$.

## 6.8. INNER AUTOMORPHISM, OUTER AUTOMORPHISM

**Theorem 11.** ***Let $a$ be a fixed element of a group $\mathbf{G}$. Then the mapping $f_a : \mathbf{G} \to \mathbf{G}$, defined by $f_a(x) = a^{-1}xa$ for every $x \in \mathbf{G}$, is an automorphism of $\mathbf{G}$.*** ***(A.N.U. O90, K.U. M 12, S 00)***

**Proof.** $a$ is a fixed element of a group $\mathbf{G}$. $f_a : \mathbf{G} \to \mathbf{G}$ such that $f_a(x) = a^{-1}xa$ for $x \in \mathbf{G}$.

To prove that $f_a$ is one-one

Let $x, y \in \mathbf{G}$. $\therefore$ $f_a(x), f_a(y) \in \mathbf{G}$ (co-comain).

Now $f_a(x) = f_a(y) \Rightarrow a^{-1}xa = a^{-1}ya$

$\Rightarrow x = y$ ($\because$ $a, a^{-1}, x, y \in \mathbf{G}$ and cancellation laws are true in $\mathbf{G}$)

$\therefore$ $f_a$ is one-one.

To prove that $f_a$ is onto.

Let $y \in \mathbf{G}$ (co-domain). Since $a \in \mathbf{G}, a^{-1} \in \mathbf{G}$. $\therefore$ $a^{-1}ya \in \mathbf{G}$ (domain).

$\therefore$ $f_a(aya^{-1}) = a^{-1}(aya^{-1})\,a = (a^{-1}a)\,y\,(a^{-1}a) = y$ $\therefore$ $f_a$ is onto

To prove that $f_a$ is a homomorphism

Let $x, y \in \mathbf{G}$. $\therefore$ $xy \in \mathbf{G}$.

$\therefore$ $f_a(xy) = a^{-1}(xy)\,a = a^{-1}x\,a\,a^{-1}ya = (a^{-1}xa)\,(a^{-1}ya) = f_a(x) f_a(y)$

$\therefore$ $f_a$ is an automorphism of $\mathbf{G}$.

**Inner automorphism, outer automorphism**

**Definition.** Let $\mathbf{G}$ be a group. If the mapping $f_a : \mathbf{G} \to \mathbf{G}$, defined by $f_a(x) = a^{-1}xa$ for every $x \in \mathbf{G}$ and $a$, a fixed element of $\mathbf{G}$, is an automorphism of $\mathbf{G}$, then $f_a$ is known as inner automorphism of $\mathbf{G}$.

An automorphism which is not inner called an outer automorphism.

**Theorem 12.** ***In an abelian group the only inner automorphism is the identity mapping on the group.*** ***(S.V.U. S 93)***

**Proof.** Let $\mathbf{G}$ be an abelian group and $f_a$ is an inner automorphism of $\mathbf{G}$ where $a$ is a fixed element of $\mathbf{G}$.

$x \in \mathbf{G}$, $f_a(x) = a^{-1}xa = a^{-1}ax$ ($\because$ $\mathbf{G}$ is abelian)

$= ex = x$.

$\therefore$ $f_a$ is the identity mapping of $\mathbf{G}$. We know that it is an automorphism.

$\therefore$ The identity mapping is the only inner automorphism of an abelian group.

## EXERCISE 6

**1.** If $\mathbf{G}$ is a group and $\phi : \mathbf{G} \to \mathbf{G}$ is defined as $\phi(x) = x^{-1}\ \forall\ x \in \mathbf{G}$, then show that $\phi$ is not a homomorphism.

**2.** If $\mathbf{G}$ is a group of non-zero real numbers under multiplication prove that $\phi : \mathbf{G} \to \mathbf{G}$ where $\phi(x) = x^2\ \forall\ x \in \mathbf{G}$ is a homomorphism. Determine kernel $\phi$.

**3.** $(\mathbf{Z}, +)$ is the group of integers. Prove that $f : \mathbf{Z} \to \mathbf{Z}$ where $f(x) = 2x\ \forall\ x \in \mathbf{Z}$ is a homomorphism. Find $\ker f$. Is it onto homomorphism?

**4.** $(\mathbf{Z}, +)$ is the group of integers $(\mathbf{Z}_n, +_n)$ is the group of integers under addition modulo $n$. If $\phi : \mathbf{Z} \to \mathbf{Z}_n$ is defined by $\phi(x) =$ remainder of $x$ on division by $n$, prove that $\phi$ is a homomorphism.

**5.** $\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3$ are three groups. If $f : \mathbf{G}_1 \to \mathbf{G}_2, g : \mathbf{G}_2 \to \mathbf{G}_3$ are isomorphisms, prove that $gof : \mathbf{G} \to \mathbf{G}_3$ is an isomorphism.

**6.** When do you say that two groups are isomorphic? Prove that under an isomorphism of a group $\mathbf{G}$ onto a group $\mathbf{G}'$ (i) the identity $e$ in $\mathbf{G}$ is mapped into the identity $e'$ in $\mathbf{G}'$ (ii) the inverse of any element $a$ of $\mathbf{G}$ is mapped into the inverse image of $a$ in $\mathbf{G}'$. ***(N.U. O 85)***

**7.** Let $(\mathbf{R}^+, .)$ be a group and $f : \mathbf{R}^+ \to \mathbf{R}^+$ be defined by $f(x) = x^2\ \forall\ x \in \mathbf{R}^+$. Prove that $f$ is an automorphism. ***(K.U.M. 2004)***

**8.** Show that for a group $\mathbf{G}$, $\dfrac{\mathbf{G}}{\{e\}} \cong \mathbf{G}$.

**9.** Prove that : If $(\mathbf{G}, .)$ and $(\overline{\mathbf{G}}, .)$ are two isomophic groups, then $(\mathbf{G}, .)$ is abelian iff $(\overline{\mathbf{G}}, .)$ is abelian.

**10.** Let $(\mathbf{G}, .)$ and $(\overline{\mathbf{G}}, .)$ be two finite groups. If $f : \mathbf{G} \to \overline{\mathbf{G}}$ be an isomorphism and if for $a \in \mathbf{G}, o(a) = n$, then prove that $o(f(a)) = n$. ***(A.N.U.M99, K.U.J 2000, O.U. 2001)***

**11.** Define isomorphism of groups. Show that the group $\mathbf{G} = \{0, 1, 2, 3\}$ addition modulo 4 is isomorphic to the group $\mathbf{G}' = \{1, 2, 3, 4\}$ multiplication modulo 5. ***(S.V.U. A 93)***

**12.** If $\mathbf{G} = \{0,1,2,3,4\}$ with operation $+_5$ defined on it and $\mathbf{G}'$ is the cyclic group $\{a, a^2, a^3, a^4, a^5 = e\}$, show that the mapping $f : \mathbf{G} \to \mathbf{G}'$ such that $f(n) = a^n\ \forall\ n \in \mathbf{G}$ is an isomorphism of $\mathbf{G}$ onto $\mathbf{G}'$ (vide ch. 8 for definition of cyclic group)

**13.** Show that $f : \mathbf{C}_0 \to \mathbf{C}_0$ defined by $f(z) = z^n$ where $z \in \mathbf{C}_0$ and $n$ is a fixed positive integer is an endomorphism of the multiplicative group $\mathbf{C}_0$ of non-zero complex numbers. Find ker $f$.

**14.** $(\mathbf{Z},+)$ and $(\mathbf{G}=\{1,-1,i,-i\},\cdot)$ are two groups. Show that the mapping $f$ defined by $f(n)=i^n \ \forall\ n\in\mathbf{Z}$ is a homomorphism from $(\mathbf{Z},+)$ onto $(\mathbf{G},\cdot)$ and determine $\ker f$.

## ANSWERS

**2.** $\ker\phi=\{1,-1\}$ **3.** $\{x\in\mathbf{Z}/2x=0\}=\{0\}$; Not an onto homomorphism

**13.** $\ker f=\{e^{2\pi r i/n}, r=0,1,2,.....,(n-1)\}$ **14.** $\ker f=\{4^n/n\in\mathbf{Z}\}$

# Permutation Groups

## 7.1. PERMUTATION

**Definition.** A permutation is a one-one mapping of a non empty set onto itself.

Thus a permutation is a bijective mapping of a non-empty set into itself.

**Ex.** $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x+1$ is a permutation of $\mathbf{R}$ since $f$ is an one-one mapping onto itself.

If $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ then a one-one mapping from $\mathbf{S}$ onto itself is called a **permutation of degree** $n$. The number $n$ of elements in $\mathbf{S}$ is called the **degree of permutation.**

**Equal permutations.** ***(A.N.U. S98, A92, O.U. O2000)***

**Definition.** Two permutations $f$ and $g$ defined over a non-empty set $\mathbf{S}$ are said to be equal if $f(a) = g(a)$ for $a \in \mathbf{S}$.

**Permutation multiplication or product of permutations.**

It is the composition of mappings defined over the non-empty set $\mathbf{S}$. If $g, f$ are two permutations (bijective mappings) defined over $\mathbf{S}$, then the product of permutations $f, g$ is defined as $gof$ or $gf$, where $(gf)(a) = g(f(a))$ for $a \in \mathbf{S}$. Further $gf$ is also a bijective mapping over $\mathbf{S}$. In this context we say that permutation multiplication is a binary operation in the set of permutations defined over $\mathbf{S}$.

**Product of permutations or Multiplication of permutations or Composition of permutations in $\mathbf{S}_n$.**

Let $f = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ b_1 & b_2 & \ldots b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 & \ldots b_n \\ c_1 & c_2 & \ldots c_n \end{pmatrix}$ be two elements (permutations) of $\mathbf{S}_n$. Here, $b_1, b_2, \ldots, b_n$ or $c_1, c_2, \ldots, c_n$ are nothing but the elements $a_1, a_2, \ldots, a_n$ of $\mathbf{S}$ in some order.

Now $f(a_1) = b_1, g(b_1) = c_1; f(a_2) = b_2, g(b_2) = c_2$, etc.

$\therefore$ By definition we have $c_1 = g(b_1) = g(f(a_1)) = (gf)(a_1)$ i.e. $(gf)(a_1) = c_1$.

Similarly $(gf)(a_2) = c_2$, $(gf)(a_3) = c_3$, …, $(gf)(a_n) = c_n$.

$$\therefore \quad gf = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ c_1 & c_2 & \ldots c_n \end{pmatrix}.$$

Obviously $gf$ is also a permutation of degree $n$ on $\mathbf{S}$ and hence $gf \in \mathbf{S}_n$ for $g, f \in \mathbf{S}_n$.

Thus : $gf$ is a permutation obtained by first carrying out the operation defined by $f$ and then by $g$ which we followed.

*But some renowned authors write gf as fg implying that f is to be operated first and then g is to be operated next. In this case* $(fg)(a_1) = g(f(a_1) = g(b_1) = c_1$ *etc.*

*So,* $fg = \begin{pmatrix} a_1 & a_2 \ldots\ldots\ldots\ldots a_n \\ c_1 & c_2 \ldots\ldots\ldots\ldots c_n \end{pmatrix}$. **This may be taken note of carefully.**

## 7.2. PERMUTATION GROUP

**Theorem 1.** ***The set*** $\mathbf{A(S)}$ ***of all permutations defined over a non-empty set*** $\mathbf{S}$ ***forms a group under the operation permutation multiplication.*** ***(O.U.O. 00)***

**Proof.** Let $o$ be the permutation multiplication (composition of mappings in $\mathbf{A(S)}$ ).

(For completion of the proof please refer to Ex. 12, Chapter 2).

**Note: 1.** The above group is called group of permutations.

**2.** In the above theorem $\mathbf{S}$ is not assumed to be finite. However, from now on, we deal with permutations defined on finite sets only.

The permutation group is also known as the **symmetric group of degree *n*** on $n$ symbols.

The permutation group on $n$ symbols is generally denoted by $\mathbf{S}_n$ or $\mathbf{P}_n$. The elements of $\mathbf{S}$ can be denoted also by $1, 2, \ldots, n$ or by any other symbols.

**Identity permutation.** If $f$ is a permutation of $\mathbf{S}$ such that $f(a) = a \ \forall a \in \mathbf{S}$, then $f$ is identity of $\mathbf{S}$ and we denote $f$ as $\mathbf{I}$.

**Order of permutation.** If $f \in \mathbf{S}_n$ such that $f^m = \mathbf{I}$, the identity permutation in $\mathbf{S}_n$, where $m$ is the least positive integer, then the order of the permutation $f$ in $\mathbf{S}_n$ is $m$.

**Order of $\mathbf{S}_n$ is n!**

For : Let $f$ be a permutation on $\mathbf{S}$ with $n$ elements (symbols) $a_1, a_2, \ldots, a_n$.

The image of $a_1$ under $f$ can be any one of $a_1, a_2, \ldots, a_n$. So the image of $a_1$ can be chosen in $n$ ways. After the image of $a_1$ is chosen, to choose the image for $a_2$ we have $(n-1)$ choices only. The image of $a_2$ can be chosen in $(n-1)$ ways. Similarly the images of $a_3, a_4, \ldots, a_n$ can be chosen respectively in $(n-2)$ ways, $(n-3)$ ways, ....1 way. Since the ways of choosing images are independent, the total number of ways of choosing the images of $a_1, a_2, \ldots, a_n$ is $n(n-1)(n-2)\ldots 1$ i.e. $n!$.

**Note.** If the number of elements in $\mathbf{S}$ is 1, then $o(\mathbf{S}_n) = 1! = 1$ and hence $\mathbf{S}_n$ forms an abelian group.

If the number of elements in $\mathbf{S}$ is 2, then $o(\mathbf{S}_n) = 2! = 2$ and hence $\mathbf{S}_n$ forms an abelian group.

If the number of elements in $\mathbf{S}$ is 3, then $o(\mathbf{S}_n) = 3! = 6$ and hence $\mathbf{S}_n$ forms a group and so on.

In fact $\mathbf{S}_n$ forms a non-abelian group if $\mathbf{S}$ contains 3 or more than 3 elements.

## 7.3. SYMBOL FOR A PERMUTATION WHEN $\mathbf{S} = \{a_1, a_2, \ldots, a_n\}$.

Let $f : \mathbf{S} \to \mathbf{S}$ be a permutation such that $f(a_1) = b_1, f(a_2) = b_2, \ldots, f(a_n) = b_n$ where $b_1, b_2, \ldots, b_n$ are nothing but the elements $a_1, a_2, \ldots, a_n$ of $\mathbf{S}$ in some order. So we write $f = \begin{pmatrix} a_1, a_2, \ldots, a_n \\ b_1, b_2, \ldots, b_n \end{pmatrix}$, where each element in the second row is the $f$ image of the corresponding element (element lying above) in the first row. Then we have $n!$ elements of the type $f$ in $\mathbf{S}_n$ where $\mathbf{S}_n$ is the set of all permutations defined on $\mathbf{S}$.

If $\mathbf{S} = \{1, 2, 3, 4, 5\}$ and $f : \mathbf{S} \to \mathbf{S}$ is a permutation such that $f = \{(1,3), (2,5), (3,4), (4,2), (5,1)\}$ then we write

$f = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,5\,4\,2\,1 \end{pmatrix}$. We can also write $f$ as $\begin{pmatrix} 2\,1\,4\,5\,3 \\ 5\,3\,2\,1\,4 \end{pmatrix}$

in which the order of the elements in the first row is not followed whereas their corresponding images only are written in the second row (following the order of the elements in the first row). Here we see that :

$1 \to 3, 2 \to 5, 3 \to 4, 4 \to 2$ and $5 \to 1$.

**Equality of permutations on $\mathbf{S} = \{1, 2, 3, 4, 5\}$ :** If

$f = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,5\,4\,2\,1 \end{pmatrix}$ and $g = \begin{pmatrix} 2\,1\,4\,5\,3 \\ 5\,3\,2\,1\,4 \end{pmatrix}$ then $f = g$ since $f(1) = 3 = g(1), f(2) = 5 = g(2), f(3) = 4 = g(3), f(4) = 2 = g(4), f(5) = 1 = g(5)$.

In particular, Identity permutation on $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ in $\mathbf{S}_n$ is given by

$\mathbf{I} = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ a_1 & a_2 & \ldots a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 & \ldots b_n \\ b_1 & b_2 & \ldots b_n \end{pmatrix}$ where the elements $a_1, a_2, \ldots\ldots, a_n$ of S are nothing but the elements $a_1, a_2, \ldots, a_n$ of $\mathbf{S}$ in some order.

If $\mathbf{S} = \{1, 2, 3, 4, 5\}$, then Identity permutation on $\mathbf{A}$ is

$$\mathbf{I} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,4\,5 \end{pmatrix} = \begin{pmatrix} 4\,3\,1\,5\,2 \\ 4\,3\,1\,5\,2 \end{pmatrix}, \text{ etc.}$$

**Ex.1:** If $\mathbf{A} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}$, then find **AB** and **BA.** *(A.N.U 92)*

**Sol.** Since $(\mathbf{AB})(1) = \mathbf{A}(\mathbf{B}(1)) = \mathbf{A}(3) = 1,$ ; $\mathbf{AB}(2) = 2, \mathbf{AB}(3) = 3$, $\mathbf{AB} = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}$

Since $(\mathbf{BA})(1) = \mathbf{B}(\mathbf{A}(1)) = \mathbf{B}(2) = 1,$ ; $\mathbf{BA}(2) = 2$, $\mathbf{BA}(3) = 3$, we have $\mathbf{BA} = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}$.

**Ex.2:** If $f = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,2\,4\,1 \end{pmatrix}$ and $g = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,3\,1\,2\,5 \end{pmatrix}$, then find $fg$ and $gf$.

**Sol.** Since $gf(1) = g(f(1)) = g(5) = 5$, $gf(2) = 1$, $gf(3) = 3$, $gf(4) = 2$, $gf(5) = 4$

we have $gf = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,1\,3\,2\,4 \end{pmatrix}$.

Similarly $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ since $fg(2) = f(g(2)) = f(3) = 2$, etc.

**Note 1 :** Obviously $fg \neq gf$. Thus we notice that multiplication of permutations is not commutative.

**2 :** $f\,\mathbf{I} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix} = f$ and similarly $\mathbf{I}\,f = f$.

**3 :** Sometimes we may have $fg = gf$.

If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ we have $fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = gf$ ***(N.U. A 95)***

**Ex.3:** Multiplication of permutations is associative. Show that.

if $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$, and $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$ then $(fg)h = f(gh)$

**Sol.** We have $gh = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$, $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$,

$(fg)h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$ and $f(gh) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$. So $(fg)h = f(gh)$.

**Inverse of permutation :** It is also a permutation (bijection).

If $f = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ b_1 & b_2 & \ldots b_n \end{pmatrix}$, then its inverse, denoted by $f^{-1}$ is $\begin{pmatrix} b_1 & b_2 & \ldots b_n \\ a_1 & a_2 & \ldots a_n \end{pmatrix}$

$(\because f(a_1) = b_1 \Rightarrow f^{-1}(b_1) = a_1$, etc.$)$

Also $f^{-1}f = \begin{pmatrix} b_1 & b_2 & \ldots b_n \\ a_1 & a_2 & \ldots a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \ldots a_n \\ b_1 & b_2 & \ldots b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ a_1 & a_2 & \ldots a_n \end{pmatrix} = \mathbf{I}$

and $ff^{-1} = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ b_1 & b_2 & \ldots b_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & \ldots b_n \\ a_1 & a_2 & \ldots a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \ldots b_n \\ b_1 & b_2 & \ldots b_n \end{pmatrix} = \mathbf{I}$

**Ex.4:** Find the inverse of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ ***(A.N.U. M98)***

**Sol.:** Inverse of $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$

**Note 1.** The set $\mathbf{S}_n$ of all permutations on $n$ symbols is a finite group of order $n!$ w.r.t. multiplication of permutations. For $n \leq 2$, the group is abelian and for $n \geq 3$, the group is non-abelian. This can be proved as in Ex. 15, Chapter 2, taking $f_1 f_2$ .... as permutations.

**2.** To write the inverse of a permutation, write the 2nd row as 1st row and 1st row as 2nd row.

**Ex.5 :** Find the order of the cycle $(1\ \ 4\ \ 5\ \ 7)$. ***(O. U. M. 08)***

**Sol.** Let $f = (1\ \ 4\ \ 5\ \ 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$

$$\therefore f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 1 & 6 & 4 \end{pmatrix},$$

$$f^3 = f^2 f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 1 & 6 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$$

$$f^4 = f^3 f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \mathbf{I}$$

$\therefore$ Order of the cycle = 4.

**Note.** The cycles of $f$ are $(1\ \ 4\ \ 5\ \ 7)\,(2)\,(3)\,(6)$.

## 7. 4. ORBITS AND CYCLES OF PERMUTATION

**Definition.** Consider a set $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ and a permutation $f$ on $\mathbf{S}$. If for $s \in \mathbf{S}$ there exists a smallest positive integer $l$ depending on $s$ such that $f^l(s) = s$, then the set $\{s, f^1(s), f^2(s), \ldots, f^{l-1}(s)\}$ is called the orbit of $s$ under the permutation $f$. The ordered set $\{s, f^1(s), f^2(s), \ldots, f^{l-1}(s)\}$ is called a cycle of $f$.

**e.g. 1.** Consider $\mathbf{S} = \{1, 2, 3, 4, 5, 6\}$ and a permutation on $\mathbf{S}$ be $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$.

We have $f^1(1) = 2, f^2(1) = f(2) = 1$. $\therefore$ orbit of 1 under $f = \{1, f(1)\} = \{1, 2\}$

We have $f^1(2) = 1, f^2(2) = f(1) = 2$. $\therefore$ orbit of 2 under $f = \{2, 1\}$

We have $f^1(3) = 3$. $\therefore$ orbit of 3 under $f = \{3\}$

We have $f^1(4) = 5, f^2(4) = f(5) = 6, f^3(4) = f(6) = 4$.

$\therefore$ orbit of 4 under $f = \{4, 5, 6\}$.

We have $f^1(5) = 6, f^2(5) = f(6) = 4$. $f^3(5) = f(4) = 5$.

$\therefore$ orbit of 5 under $f = \{5, 6, 4\}$.

We have $f^1(6) = 4, f^2(6) = 5, f^3(6) = 6$. $\therefore$ orbit of 6 under $f = \{6, 4, 5\}$.

Hence the cycles of $f$ are $(1, 2), (3), (4, 5, 6)$.

**e.g. 2.** Find the orbits of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix}$. Also find the order of $\sigma$.

***(K. U. M 07)***

**Sol.** Consider $\mathbf{S} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and a permutation on $\mathbf{S}$ be $\sigma = (\ldots\ldots)$

We have $\sigma^1(1) = 2, \sigma^2(1) = \sigma(2) = 3, \sigma^3(1) = \sigma(3) = 5, \sigma^4(1) = \sigma(5) = 4, \sigma^5(4) = 1$

$\therefore$ Orbit of 1 under $\sigma = \{1, \sigma^1(1), \sigma^2(1), \sigma^3(1), \sigma^4(1), \sigma^5(1)\} = \{1,2,3,5,4\}$

We have $\sigma^1(2) = 3, \sigma^2(2) = \sigma(3) = 5, \sigma^3(2) = \sigma(5) = 4, \sigma^4(2) = \sigma(4) = 1, \sigma(2) = \sigma(1) = 2$

$\therefore$ Orbit of 2 under $\sigma = \{2, \sigma^1(2), \sigma^2(2), \sigma^3(2), \sigma^4(2), \sigma^5(2)\} = \{2,3,5,4\}$

We have $\sigma^1(3) = 5, \sigma^2(3) = \sigma(5) = 4, \sigma^3(3) = \sigma(4) = 1, \sigma^4(3) = \sigma(1) = 2, \sigma^5(3) = \sigma(2) = 3$

$\therefore$ Orbit of 3 under $\sigma = \{3, \sigma^1(3), \sigma^2(3), \sigma^3(3), \sigma^4(3), \sigma^5(3)\} = \{3,5,4,1,2\}$

We have $\sigma^1(4) = 1, \sigma^2(4) = \sigma(1) = 2, \sigma^3(4) = \sigma(2) = 3, \sigma^4(4) = \sigma(3) = 5, \sigma^5(4) = \sigma^5(5) = 4$

$\therefore$ Orbit of 4 under $\sigma = \{4,1,2,3,5\}$

We have $\sigma^1(5) = 4, \sigma^2(5) = \sigma(4) = 1, \sigma^3(5) = \sigma(1) = 2, \sigma^4(5) = \sigma(2) = 3, \sigma^5(5) = \sigma(3) = 5$

$\therefore$ Orbit of 5 under $\sigma = \{5,4,1,2,3\}$

We have $\sigma^1(6) = 6$

$\therefore$ Orbit of 6 under $\sigma = \{6\}$

We have $\sigma^1(7) = 8, \sigma^2(7) = \sigma^1(8) = 7$

$\therefore$ Orbit of 7 under $\sigma = \{7,8\}$

We have $\sigma^1(8) = 7, \sigma^2(8) = \sigma(7) = 8$

$\therefore$ Orbit of 8 under $\sigma = \{8,7\}$

[Hence the cycles of $\sigma$ are $(1,2,3,5,4), (6), (7,8)$ ]

Again $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix}$

$\Rightarrow \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 6 & 7 & 8 \end{pmatrix}$

$\Rightarrow \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 3 & 2 & 6 & 7 & 8 \end{pmatrix}$

$\Rightarrow \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 5 & 3 & 6 & 7 & 8 \end{pmatrix}$

$\Rightarrow \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \mathbf{I}$ (Here $\sigma^m = \mathbf{I}$ where $m$ is least)

$\therefore$ Order of $\sigma$ is 5.

**Cyclic permutations**

**Definition.** Consider a set $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ and a permutation

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_k & a_{k+1} \ldots a_n \\ a_2 & a_3 & a_4 \ldots & a_1 & a_{k+1} \ldots a_n \end{pmatrix} \text{ on } \mathbf{S}.$$

i.e. $f(a_1) = a_2, f(a_2) = a_3, \ldots f(a_k) = a_1, f(a_{k+1}) = a_{k+1} \ldots f(a_n) = a_n$

This type of permutation $f$ is called a **cyclic permutation of length $k$ and degree $n$.** It is represented by $(a_1\ a_2\ \dots\ a_k)$ or $(a_1, a_2, a_3, \dots, a_k)$ which is a cycle of length $k$ or $k$-cycle. ***(K.U.M. 00, M.99)***

Thus : The number of elements permuted by a cycle is called its **length.**

In this type of notation we ignore elements that are mapped onto themselves. Also we can write the cycle $(a_1\ a_2\ a_3 \dots a_k)$ as $(a_2\ a_3 \dots a_k\ a_1)$ or $(a_3\ a_4 \dots a_k\ a_1\ a_2)$ etc.

**e.g. 1.** If $\mathbf{S} = \{1, 2, 3, 4, 5, 6\}$ then a permutation $f$ on $\mathbf{S}$ is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 5 & 2 \end{pmatrix}$. It can be written as $(1\ 3\ 4\ 6\ 2)$ since $f(1) = 3, f(3) = 4, f(4) = 6, f(6) = 2, f(2) = 1$ and $f(5) = 5$.

$f$ is a cycle of length 5. $f$ can also be written as $(3\ 4\ 6\ 2\ 1)$ or $(4\ 6\ 2\ 1\ 3)$ etc. following the cyclic order.

**e.g. 2.** If $\mathbf{S} = \{1, 2, 3, 4, 5, 6, 7\}$ then a permutation $f$ on $\mathbf{S}$ is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix}$. It can be written as $(1\ 3\ 5\ 7)$. $f$ is a cycle of length 4. $f$ can also be written as $(3\ 5\ 7\ 1)$ or $(5\ 7\ 1\ 3)$ or $(7\ 1\ 3\ 5)$.

**e.g. 3.** If $\mathbf{S} = \{1, 2, 3, 4, 5, 6\}$ then a permutation $f$ on $\mathbf{S}$ is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}$. $f$ is not a cyclic permutation since $f(1) = 4, f(4) = 1, f(2) = 3, f(3) = 5, f(5) = 2, f(6) = 6$.

**Note 1.** A cyclic permutation does not change by changing the places of its elements provided their cyclic order is not changed.

**2.** A cycle of length 1 is the identity permutation since $f(a_1) = a_1, f(a_2) = a_2, \dots$ $f(a_n) = a_n$.

**Transposition :**

**Definition.** A cycle of length 2 is called a **transposition.** ***(O.U. O 98)***

i.e. trasposition is a cycle $(a, b)$ where a and b are only interchanged keeping the rest of the elements unchanged.

**e.g.** If $\mathbf{S} = \{1, 2, 3, 4, 5\}$ and a permutation $f$ on $\mathbf{S}$ is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$ then $f = (2, 3)$ is a cycle of length 2 and degree 5.

Observe that $f(2) = 3, f(3) = 2$ and the image of each other element is itself.

Here $f^{-1} = (3\ 2)$ where $f = (2\ 3)$ i.e. $f^{-1} = f$. i.e. the inverse of a transposition is itself.

**Disjoint cycles.**

**Definition.** Let $\mathbf{S} = \{a_1, a_2, \dots\dots, a_n\}$. If $f, g$ be two cycles on $\mathbf{S}$ such that they have no common elements, then they are called **disjoint cycles.**

**e.g.** Let $\mathbf{S} = \{1, 2, 3, 4, 5, 6, 7\}$

(i) If $f = (1\ 3\ 7)$ and $g = (2\ 4\ 5)$ then $f, g$ are disjoint cycles.

(ii) If $f = (1\ 3\ 7)$ and $g = (2\ 3\ 4\ 5)$ then $f, g$ are not disjoint cycles.

**Product of two cycles over the same set $\mathbf{S} = \{1, 2, 3, 4, 5, 6\}$.**

**e.g. 1.** $f = (1\ 4\ 3), g = (2\ 5)$.

Now we find products $gf, fg$ .

$gf : 1 \to 4$ and $4 \to 4 \Rightarrow 1 \to 4$

(from $f$ ) (from $g$ )

$2 \to 2,$ $2 \to 5$ $\Rightarrow 2 \to 5;$

(from $f$ ) (from $g$ )

$3 \to 1$ and $1 \to 1 \Rightarrow 3 \to 1;\ 4 \to 3,\ 3 \to 3 \Rightarrow 4 \to 3$

$5 \to 5$ and $5 \to 2 \Rightarrow 5 \to 2;\ 6 \to 6,\ 6 \to 6 \Rightarrow 6 \to 6$

$\therefore\ gf = (2\ 5)(1\ 4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 2 & 6 \end{pmatrix}.$

Also $fg = (1\ 4\ 3)(2\ 5) = \begin{pmatrix} 1 & 4 & 2 & 3 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 2 & 6 \end{pmatrix}.$

**Note 1.** The multiplication is the multiplication of disjoint cycles and $fg = gf$ .

**2.** We leave identity permutation (s) while writing the product of cycles.

**e.g. 2.** $f = (2\ 3\ 6), g = (1\ 4\ 6)$ ***(N. U. 07)***

Now we find products $fg, gf$

$\therefore\ fg = (2\ 3\ 6)(1\ 4\ 6)$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 6 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 2 & 5 & 1 \end{pmatrix} = (1\ 4\ 2\ 3\ 6)$

and $gf = (1\ 4\ 6)(2\ 3\ 6)$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 6 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 5 & 2 \end{pmatrix} = (1\ 4\ 6\ 2\ 3).$

Observe that $f, g$ are not disjoint and $fg \neq gf$.

**e.g. 3.** $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 5 & 3 & 2 & 6 \end{pmatrix} = (1\ 5\ 2)\ (3\ 4)\ (6)$

$= (3\ 4)(1\ 5\ 2)$ . (1 5 2)(3 4) since (6) is the identity permutation and it need not be shown Observe that $(3\ 4)(1\ 5\ 3)$ are disjoint cycles.

**e.g. 4.** $(1\ 2)(1\ 3)(1\ 5) = (1\ 2) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix}$

$= (1\ 2) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 3 & 6 \end{pmatrix} = (1\ 2)(1\ 5\ 3) = (1\ 5\ 3\ 2)$

**e.g. 5.** $(3\ 4)(3\ 5)(3\ 6) = (3\ 4)(3\ 6\ 5) = (3\ 6\ 5\ 4)$

and $(3\ 4)(3\ 5\ 4)(3\ 6) = (3\ 5\ 4)(3\ 6) = (3\ 6\ 5\ 4)$

**e.g. 6.** $(1\ 5\ 3)(4\ 6) \neq (1\ 4)(5\ 3\ 6)$

since $(1\ 5\ 3)(4\ 6) = \begin{pmatrix}1&2&3&4&5&6\\5&2&1&4&3&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\1&2&3&6&5&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6\\5&2&1&6&3&4\end{pmatrix}$

and $(1\ 4)(5\ 3\ 6) = \begin{pmatrix}1&2&3&4&5&6\\4&2&6&1&3&5\end{pmatrix}$

**e.g. 7.** If $f = (1\ 3\ 4), g = (2\ 3), h = (5\ 4\ 2)$ then we have $(fg)h = f(gh)$

**Inverse of a cyclic permutation**

**e.g. 1.** If $f = (2\ 3\ 4\ 1)$ of degree 5, then $f^{-1} = (1\ 4\ 3\ 2)$

since $f = \begin{pmatrix}1&2&3&4&5\\2&3&4&1&5\end{pmatrix}$ and $f^{-1} = \begin{pmatrix}2&3&4&1&5\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\4&1&2&3&5\end{pmatrix} = (1\ 4\ 3\ 2)$

**e.g. 2.** If $f = (1\ 3\ 4\ 6)$ is a cyclic permutation on 6 symbols, its inverse $= f^{-1} = (6\ 4\ 3\ 1) = (1\ 6\ 4\ 3)$, etc. If $f = (3\ 5\ 6\ 1)$, then $f^{-1} = (1\ 6\ 5\ 3) = (3\ 1\ 6\ 5)$, etc.

**e.g. 3.** If $f = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 6), g = (4\ 1\ 5\ 6\ 7\ 3\ 2\ 8)$ are cyclic permutations, then show that $(fg)^{-1} = g^{-1}f^{-1}$. ***(N.U. A 95)***

**Sol.** $f = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 6) = \begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&5&8&1&6&7\end{pmatrix}$,

$g = (4\ 1\ 5\ 6\ 7\ 3\ 2\ 8) = \begin{pmatrix}1&2&3&4&5&6&7&8\\5&8&2&1&6&7&3&4\end{pmatrix}$.

$\therefore\quad fg = \begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&3&2&1&6&4&5\end{pmatrix}$ and $(fg)^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\5&4&3&7&8&6&2&1\end{pmatrix}$.

Also $f^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\6&1&2&3&4&7&8&5\end{pmatrix}$ and $g^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\4&3&7&8&1&5&6&2\end{pmatrix}$.

$\therefore\quad g^{-1}f^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\5&4&3&7&8&6&2&1\end{pmatrix}$. $\therefore\quad (fg)^{-1} = g^{-1}f^{-1}$.

**e.g. 4.** If $f = (1\ 3\ 4), g = (2\ 3), h = (5\ 4\ 2)$
then we have (i) $(fg)^{-1} = g^{-1}f^{-1}$ and (ii) $(fgh)^{-1} = h^{-1}g^{-1}f^{-1}$

**Order of a cyclic permutation**

**e.g. 1.** If $f = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ is a permutation in the permutation group $\mathbf{S}_3$, then

$f^2 = ff = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ and $f^3 = f^2 f = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \mathbf{I}$.

Thus the order of $f$ which is a 3-cycle in $\mathbf{S}_3$ is 3.

**e.g. 2.** $\mathbf{A} = \{1\ 2\ 3\ 4\}, f = (2\ 1\ 3)$, then

$$f^2 = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} = (1\ 2\ 3) = (2\ 3\ 1),$$

$$f^3 = f\ f^2 = (2\,1\,3)\,(2\,3\,1) = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = \mathbf{I}$$

Here $f$ is a cyclic permutation of length 3 and degree 4. Order of $f = 3$.

**e.g. 3.** If $f = (1\ 2\ 3\ 4\ 5)$, then

$$f^2 = \begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix} = (1\ 3\ 5\ 2\ 4),$$

$f^3 = ff^2 = (1\ 4\ 2\ 5\ 3), f^4 = (1\ 5\ 4\ 3\ 2)$ and $f^5 = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix} = \mathbf{I}$

If $f$ is a cycle of length 5 and degree5, then $f^5 = \mathbf{I}$ and hence the order of $f$ is 5.

**e.g. 4.** If $\mathbf{A} = \{1\ 2\ 3\ 4\ 5\ 6\ 7\}$ and $f = (7\ 3\ 2\ 5)$,

then $f^2 = \begin{pmatrix}1&2&3&4&5&6&7\\1&5&2&4&7&6&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\1&5&2&4&7&6&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6&7\\1&7&5&4&3&6&2\end{pmatrix} = (2\ 7)(3\ 5),$

$f^3 = \begin{pmatrix}1&2&3&4&5&6&7\\1&3&7&4&2&6&5\end{pmatrix}$ and $f^4 = \mathbf{I}$. Order of $f = 4$.

**Theorem 2.** ***The multiplication of disjoint cycles is commutative.***
***(A.N.U. S 01, S.K.U 097)***

**Proof.** Let $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ Let $f = (x_1, x_2, \ldots\ldots, x_k)$ and $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ be two disjoint cycles on $\mathbf{S}$.

To prove that $gf = fg$ i.e. to prove that $(gf)(x) = (fg)(x)$ for $x \in \mathbf{S}$.

For $x \in \mathbf{A}$, the following cases arise.

**Case (i).** Let $x \in \{x_1, x_2, \ldots x_k\}$ $\therefore$ $f(x) \in \{x_1, x_2, \ldots x_k\}$.

Since $f, g$ are disjoint cycles, $\{x_1, \ldots x_k\} \cap \{y_1, \ldots y_l\} = \phi$

$\therefore$ $x, f(x) \notin \{y_1, \ldots y_l\}$ $\therefore$ $g(x) = x$ and $g(f(x)) = f(x)$.

Now $(gf)(x) = g(f(x)) = f(x)$ and $(fg)(x) = f(g(x)) = f(x)$ and hence

$(gf)(x) = (fg)(x)$ for $x \in \mathbf{S}$.

**Case (ii).** Let $x \in \{y_1, y_2, \ldots y_l\}$ $\therefore$ $g(x) \in \{y_1, y_2, \ldots y_l\}$

$\therefore$ Since $f, g$ are disjoint cycles,

$\{x_1, x_2, \ldots x_k\} \cap \{y_1, y_2, \ldots y_l\} = \phi$

$\therefore$ $x, g(x) \notin \{x_1, x_2, \ldots x_k\}$. $\therefore$ $f(x) = x$ and $f(g(x)) = g(x)$.

Now $(gf)(x) = g(f(x)) = g(x)$ and $(fg)(x) = f(g(x)) = g(x)$.

and hence $(gf)(x) = (fg)(x)$ for $x \in \mathbf{S}$.

**Case (iii).** Let $x \notin \{x_1, x_2, \ldots x_k\}$ and $x \notin \{y_1, y_2, \ldots y_l\}$

$\therefore$ $f(x) = x$ and $g(x) = x$

Now $(gf)(x) = g(f(x)) = g(x) = x$ and $(fg)(x) = f(g(x)) = f(x) = x$

and hence $(gf)(x) = (fg)(x)$

$\therefore$ In all the cases $fg = gf$ for $x \in \mathbf{S}$.

**Theorem 3.** ***Every permutation can be expressed as a product of disjoint cycles, which is unique (apart from the order of the factors).*** ***(N. U. D 84)***

**Proof.** Let $f$ be a permutation on set $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$ and $a, b \in \mathbf{S}$. We note that $f \in \mathbf{S}_n$ the permutation group on $\mathbf{S}$. Then we define a relation $\sim$ on $\mathbf{S}$ by

$a \sim b \Rightarrow f^n(a) = b$ for some integer $n$.

The relation $\sim$ is

(i) Reflexive : $f^0(a) = \mathrm{I}(a) = a$ for $a \in \mathbf{S}$ and thus $a \sim a\ \forall\ a \in \mathbf{S}$.

(ii) Symmetric : $a \sim b \Rightarrow f^n(a) = b \Rightarrow a = (f^n)^{-1}(b)$

$\Rightarrow a = f^{-n}(b) \Rightarrow b \sim a$.

(iii) Transitive : $a \sim b, b \sim c \Rightarrow f^m(a) = b$ and $f^n(b) = c$ for some integers $m, n$.

$\Rightarrow f^n(f^m(a)) = c$

$\Rightarrow (f^n f^m)(a) = c$

$\Rightarrow f^{n+m}(a) = c$ for some integer $n + m$

$\Rightarrow a \sim c$

$\therefore$ The relation $\sim$ is an equivalence relation on $\mathbf{S}$. Then the set $\mathbf{S} = \{a_1, \ldots a_n\}$ is partitioned into mutually disjoint classes. Each class consists of elements which can be carried into each other by $f^n(a) = b$ and so $f$ generates a cycle on the elements of each class. Since every element of $\mathbf{S}$ is in someone of these classes, and cycles on disjoint classes of elements have no elements in common it follows that the permutation $f$ is a unique product (in any order) of the disjoint cycles associated with the equivalence classes.

**Ex. 1.** *Write down the following products as disjoint cycles.*

(i) $(1\ 3\ 2)(5\ 6\ 7)(2\ 6\ 1)(4\ 5)$ (ii) $(1\ 3\ 6)(1\ 3\ 5\ 7)(6\ 7)(1\ 2\ 3\ 4)$ ***(S.K.U. 2001/0)***

**Sol.** (i) $(1\ 3\ 2)(5\ 6\ 7)(2\ 6\ 1)(4\ 5)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 4 & 6 & 7 & 5 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 5 & 4 & 1 & 7 \end{pmatrix}$$

from the first two disjoint cycles from the last two disjoint cycles

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 6 & 4 & 3 & 5 \end{pmatrix} = (1)(2\ 7\ 5\ 4\ 6\ 3)$$

Since 7 is the maximum in any cycle, we take every cycle as a permutation of degree7.

(ii) $(1\ 3\ 6)(1\ 3\ 5\ 7)(6\ 7)(1\ 2\ 3\ 4)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 7 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 4 & 7 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 6 & 7 & 3 & 1 \end{pmatrix} = (1\ 2\ 5\ 7)(3\ 4\ 6)$$

**Ex. 2.** *Express the product* $(2\ 5\ 4)(1\ 4\ 3)(2\ 1)$ *as a product of disjoint cycles and find its inverse.*

**Sol.** $(2\ 5\ 4)(1\ 4\ 3)(2\ 1)$

$$= (2\ 5\ 4) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 5\ 4\ 3)(2)$$

**OR :** Cycle $1 : 2 \to 5,\ 5 \to 4,\ 4 \to 2.$

Cycle $2 : 1 \to 4,\ 4 \to 3,\ 3 \to 1.$

Cycle $3 : 2 \to 1,\ 1 \to 2.$

Start with cycle 3, then go into cycle 2 and end with cycle 1 while writing the image of every element.

$\therefore$ Required product $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 5\ 4\ 3)\,(2)$

(Since : from cycle 3, $1 \to 2$; from cycle 2, $2 \to 2$; from cycle 1, $2 \to 5$; etc.)

2nd part : $[(2\ 5\ 4)\ (1\ 4\ 3)\ (2\ 1)]^{-1}$

$= (1\ 2)\,(3\ 4\ 1)\,(4\ 5\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} = (1\ 3\ 4\ 5)\,(2) = (3\ 4\ 5\ 1)\,(2)$

**Note.** $(1\ 5\ 4\ 3)^{-1} = (3\ 4\ 5\ 1)$ and $(2)^{-1} = (2)$

**Ex. 3.** *Express the product* $(4\ 5)\,(1\ 2\ 3)\,(3\ 2\ 1)\,(5\ 4)\,(2\ 6)\,(1\ 4)$ *on 6 symbols as the product of disjoint cycles.*

**Sol.** $(4\ 5)\,(1\ 2\ 3)\,(3\ 2\ 1)\,(5\ 4)\,(2\ 6)\,(1\ 4)$

$= (4\ 5)\,(5\ 4)\,(2\ 6)\,(1\ 4)$ $[\because\ (3\ 2\ 1)^{-1} = (1\ 2\ 3)$ and $(3\ 2\ 1)^{-1}(3\ 2\ 1) = \mathbf{I}]$

$= (2\ 6)\,(1\ 4)$ $[\because\ (5\ 4)^{-1} = (4\ 5)]$

**Theorem 4.** ***Every cycle can be expressed as a product of transpositions.***

*The truth of the theorem is only verified here.*

**Ex. 1.** Let $f = (2\ 4\ 3)$ of degree 4.

Then $f = (2\ 3)\,(2\ 4)$ $\left[\because\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)\right]$

Also we have : $f = (2\ 3)\,(1\ 2)\,(2\ 1)\,(2\ 4)$, $f = (1\ 3)\,(3\ 1)\,(2\ 3)\,(2\ 4)$,

$f = (1\ 3)\,(3\ 1)\,(2\ 3)\,(1\ 4)\,(4\ 1)\,(2\ 4)$, etc.

Also $f = (4\ 3\ 2)$. $\therefore$ We can have

$f = (4\ 2)\,(4\ 3)$, $f = (3\ 1)\,(1\ 3)\,(4\ 2)\,(1\ 2), (2\ 1)\,(4\ 3)$, etc.

Thus every cycle can be expressed as a product of transpositions in many ways.

**Ex. 2.** Let $f = (1\ 2\ 3\ 4)$. We can have $f = (1\ 4)\,(1\ 3)\,(1\ 2)$

Also $f = (2\ 3\ 4\ 1)$. $\therefore$ We can have $f = (2\ 1)\,(2\ 4)\,(2\ 3)$, etc.

**Ex. 3.** Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$. ***(S.V.U. S 93)***

Then $f = (1\ 2\ 3)\,(4)\,(5\ 6) = (1\ 3)\,(1\ 2)\,(5\ 6)$

or $f = (3\ 1\ 2)\,(4)\,(5\ 6) = (3\ 2)\,(3\ 1)\,(5\ 6)$

$= (4\ 5)\,(5\ 4)\,(3\ 2)\,(3\ 1)\,(5\ 6)$, etc.

**Ex. 4.** Let $f = (a_1, a_2, \ldots a_n)$.

We can have $f = (a_1\ a_n)\,(a_1\ a_{n-1})\ldots(a_1\ a_3)\,(a_1\ a_2)$ i.e. a cycle of length $n$ may be expressed as a product of $(n-1)$ transpositions.

**Note.** In the case of any cycle the number of transpositions is either always odd or always even.

**Theorem 5.** ***Every permutation can be expressed as a product of transpositions in many ways.***

It is a consequence of Theorems 3 and 4.

## 7.5. EVEN AND ODD PERMUTATIONS

**Definition.** A permutation is said to be an **even (odd) permutation** if it can be expressed as a product of an even (odd) number of transpositions.

To study the theorem that ensures it is worthwhile to consider the following illustration.

We consider a polynomial $P_5(x)$ in 5 distinct symbols $x_1, x_2, x_3, x_4, x_5$ defined as the product of all factors of the type $x_i - x_j$ where $1 \le i \le 4$ and $2 \le j \le 5$

Consider $\mathbf{P_5}(x) = (x_1 - x_2)\,(x_1 - x_3)\,(x_1 - x_4)\,(x_1 - x_5)\,(x_2 - x_3)$

$(x_2 - x_4)\,(x_2 - x_5)\,(x_3 - x_4)\,(x_3 - x_5)\,(x_4 - x_5)$

$= \pi (x_i - x_j)$ where $i < j,\ 1 \le i \le 4$ and $2 \le j \le 5$

$\left(\dfrac{4 \times 5}{2} = 10 \text{ factors}\right)$

Consider a transposition $(2\ 5)$ on $\mathbf{P}_5(x)$.

We can have $\mathbf{P}_5(x) = +\mathbf{LM}\,(x_2 - x_5)$ where

$\mathrm{L} = \underset{i, j \ne 2,5}{\pi} (x_i - x_j) = (x_1 - x_3)\,(x_1 - x_4)\,(x_3 - x_4)$

[factors which do not contain $x_2, x_5$ ]

$\mathrm{M} = \underset{i \ne 2,5}{\pi} (x_i - x_2)(x_j - x_5)$

$= (x_1 - x_2)\,(x_1 - x_5)\,(x_3 - x_2)\,(x_3 - x_5)\,(x_4 - x_2)\,(x_4 - x_5)$

$= (x_1 - x_2)\,(x_1 - x_5)\,(x_2 - x_3)\,(x_3 - x_5)\,(x_2 - x_4)\,(x_4 - x_5)$

Then $(2,5)\,\mathbf{L} = \mathbf{L}$, $(2,5)\,\mathbf{M} = \mathbf{M}$ and $(2,5)[(x_2 - x_5)] = x_5 - x_2 = -(x_2 - x_5)$

$\therefore$ $(2,5)\,\mathrm{P}_5(x) = (2,5)[+\mathrm{LM}\,(x_2 - x_5)]$

$= +(2,5)\,\mathbf{L}.(2,5)\,\mathbf{M}.(2,5)[x_2 - x_5]$

$= +\mathrm{LM}\,[-(x_2 - x_5)] = -[+\mathrm{LM} - (x_2 - x_5)] = -\mathbf{P}_5(x)$

Again consider a transposition $(2,4)$ on $\mathbf{P}_5(x)$. We can have -- where

$\mathrm{P}_5(x) = -\mathrm{LM}\,(x_2 - x_4)$

$\mathbf{L} = \underset{i, j \ne 2,4}{\pi} (x_i - x_j) = (x_1 - x_3)\,(x_1 - x_5)\,(x_3 - x_5)$

[factors which do not contain $x_2, x_4$ ]

$\mathbf{M} = \underset{i \ne 2,4}{\pi} (x_i - x_2)\,(x_i - x_4) = (x_1 - x_2)\,(x_3 - x_2)\,(x_5 - x_2)$

$(x_1 - x_4)\,(x_3 - x_4)\,(x_5 - x_4)$

$= -(x_1 - x_2)\,(x_1 - x_4)\,(x_2 - x_3)\,(x_2 - x_5)\,(x_3 - x_4)\,(x_4 - x_5)$

Then $(2,4)\,\mathbf{L} = \mathbf{L}$, $(2,4)\,\mathbf{M} = \mathbf{M}$ and $(2,4)[(x_2 - x_4)] = x_4 - x_2 = -(x_2 - x_4)$

$\therefore$ $(2,4)\,\mathrm{P}_5(x) = (2,4)\,[-\mathbf{LM}\,(x_2 - x_4)]$

$= -(2,4)\,\mathbf{L}.(2,4)\,\mathbf{M}.(2,4)[x_2 - x_4]$

$= -\mathbf{LM}\,[(x_4 - x_2)] = -\mathbf{LM}.[-(x_2 - x_4)] = -[-\mathbf{LM}\,[(x_2 - x_4)] = -\mathrm{P}_5(x)$

$\therefore$ A transposition changes $\mathbf{P}_5(x)$ to $-\mathbf{P}_5(x)$.

**Note:** $\mathbf{P}_5(x) = \pm \mathbf{LM}(x_2 - x_4) \Rightarrow (r, s)\,\mathbf{P}_5(x) = -\mathbf{P}_5(x)$ where $1 \le r,\ s \le 5$.

**Theorem 6.** *Let* $\mathbf{S} = \{a_1, a_2, \ldots, a_n\}$ *. If* $f$ *is a permutation on* $\mathbf{S}$ *which can be expressed as a product of* $\mathbf{r}$ *transpositions and again as a product of s transpositions, then both r, s are even or odd.*

**Proof.** To prove the theorem we take a polynomial in $x$ corresponding to $\mathbf{S}$.

Let $\mathbf{P}_n(x) = (x_1 - x_2)(x_1 - x_3)\ldots\ldots(x_1 - x_n)$

$(x_2 - x_3)\ldots\ldots(x_2 - x_n)$

$\ldots\ldots\ldots\ldots\ldots\ldots$

$\ldots\ldots\ldots\ldots\ldots\ldots$

$(x_{n-1} - x_n)$

$= \pi(x_i - x_j)$ where $i < j,\ 1 \le i \le n-1$ and $2 \le j \le n$

$\left(\text{product of } \dfrac{(n-1)\,n}{2} \text{ factors}\right)$

Now $\mathbf{P}_n(x)$ can be split into the following three types of products corresponding to a transposition $(r, s)$.

(i) $\mathbf{L} = \underset{i, j \ne r, s}{\pi} (x_i - x_j)$ [factors that do not contain $x_r$ or $x_s$]

(ii) $\mathbf{M} = \underset{i \ne r, s}{\pi} (x_i - x_r)(x_i - x_s)$ [$x_i$ takes all values but not $x_r$ or $x_s$]

(iii) $x_r - x_s$

$\therefore\ \mathbf{P}_n(x) = \pm\, \mathbf{LM}(x_r - x_s)$

We consider the effect of transposition $(r, s)$ on $\mathbf{P}_n(x)$

Then $(r, s)\,\mathbf{L} = \mathbf{L}$ ($\because$ any factor $\mathbf{I}$ does not contain either ($x_r$ or $x_s$))

$(r, s)\,\mathbf{M} = (r, s)[\pm \underset{i \ne r, s}{\pi} (x_i - x_r)(x_i - x_s)] = \mathbf{M}$

$(r, s)[(x_r - x_s)] = x_s - x_r = -(x_r - x_s)$.

$(r, s)[\mathbf{P}_n(x)] = (r, s)[\pm\, \mathbf{LM}(x_r - x_s)]$

$= \pm (r, s)\,\mathbf{L}.(r, s)\,\mathbf{M}.(r, s)\ (x_r - x_s)$

$= \pm[\mathbf{LM}\ \{(x_r - x_s)\}] = \pm[\mathbf{LM}\ \{-(x_r - x_s)\}] = -\mathrm{P}_n(x)$.

$\therefore$ A transposition $(r, s)$ changes $\mathbf{P}_n(x)$ to $-\mathbf{P}_n(x)$

Let $f$ be a permutation on $\mathbf{S}$. If $f$ can be expressed as a product of $r$ permutations, say $f_1, f_2, \ldots, f_r$ then

$f(\mathbf{P}_n(x)) = f_1, f_2, \ldots, f_r\,[\mathbf{P}_n(x)]$

$= f_1, f_2, \ldots, f_{r-1}\,((-1)^1 \mathbf{P}_n(x)) = (-1)^r \mathbf{P}_n(x)$

Again if $f$ can be expressed as a product of $s$ transpositions, then $f(\mathbf{P}_n(x)) = (-1)^r \mathbf{P}_n(x)$.

Since $f$ is a permutation (bijection), $f(\mathbf{P}_n(x))$ is unique.

$\therefore\ (-1)^r \mathbf{P}_n(x) = (-1)^s \mathbf{P}_n(x)$.

For this to be true, both $r, s$ must be even or odd.

**Note 1.** *If $f$ is expressed as a product on $n$ transpositions then either $n$ is even or $n$ is odd but cannot be both and $n$ is not unique.*

*In other words, a permutation can be expressed as a product of an even number of transpositions or an odd number of transpositions.*

*Hence the permutation group $\mathbf{S}_n$ on $n$ symbols can be split up into two disjoint sets, namely, the set of even permutations and the set of odd permutations.*

**2.** *Every transposition is an odd permutation.*

**Cor. 1.** Identity permutation $\mathbf{I}$ is always an even permutation since $\mathbf{I}$ can be expressed as a product of two transpositions.

**e.g.** $\mathbf{I} = (1\ 2)(2\ 1) = (1\ 2)(2\ 1)(3\ 1)(1\ 3)$ etc.

**Cor. 2.** A cycle of length $n$ can be expressed as a product of $(n-1)$ transpositions. If $n$ is odd, then the cycle can be expressed as a product of even number of transpositions. If $n$ is even, then the cycle can be expressed as a product of odd number of transpositions.

**Cor. 3.** The product of two odd permutations is an even permutation.

**Proof.** Let $f, g$ be two odd permutations. Let $f$ can be expressed as a product of $r$ (odd) transpositions and $g$ can be expressed as a product of $s$ (odd) transpositions.

$\therefore$ $gf$ can be expressed as $r+s$ i.e. even number of transpositions. Hence $gf$ is even.

**Cor. 4.** The product of two even permutations is an even permutation.

**Cor. 5.** The product of an odd permutation and an even permutation is an odd permutation is an odd permutation.

**Cor. 6.** The inverse of an odd permutation is an odd permutation. ***(A.N.U. 97)***

**Proof.** Let $f$ be an odd permutation and $\mathbf{I}$ be the identity permutation.

$\therefore$ $f^{-1}$ is also a permutation and $f^{-1}f = ff^{-1} = \mathbf{I}$.

Since $\mathbf{I}$ is an even and $f$ is an odd permutation, we must have $f^{-1}$ to be an odd permutation.

**Cor. 7.** The inverse of an even permutation is an even permutation.

**Proof.** Let $f$ be an even permutation and $\mathbf{I}$ be the identity permutation.

$\therefore$ $f^{-1}$ is also a permutation and $f^{-1}f = ff^{-1} = \mathbf{I}$

Since $\mathbf{I}$ is an even and $f$ is an even permutation, we must have $f^{-1}$ to be an even permutation.

**Theorem 7.** ***Let $\mathbf{S}_n$ be the permutation group on $\mathbf{n}$ symbols. Then of the $\mathbf{n}!$ permutations (elements) in $\frac{1}{2}\mathbf{n}!$ are even permutations and $\frac{1}{2}\mathbf{n}!$ are odd permutations.***

**Proof.** Let $\mathrm{S}_n = (e_1, e_2 \ldots, e_p, 0_1, 0_2, \ldots, 0_q)$ be the permutation group on $n$ symbols where $e_1, \ldots, e_p$ are even permutations and $0_1, \ldots, 0_q$ are odd permutations.($\because$ any permutation can be either even or odd but not both).

$\therefore$ $p + q = n!$

Let $t \in \mathbf{S}_n$ and $t$ be a transposition.

Since permutation multiplication follows closure law in $\mathbf{S}_n$, we have $te_1, te_2 \ldots, te_p, t0_1, t0_2 \ldots, t0_q$ as elements of $\mathbf{S}_n$.

Since $t$ is an odd permutation.

$te_1, te_2 \ldots, te_p$ are all odd and $t0_1, t0_2 \ldots, t0_q$ are all even.

Let $te_i = te_j$ for $i \le p, j \le p$.

Since $\mathbf{S}_n$ is a group, by left cancellation law $e_i = e_j$ which is absurd.

$\therefore$ $te_i \neq te_j$ and hence the $p$ permutations $te_1, te_2 \ldots, te_p$ are all distinct in $\mathbf{S}_n$. But $\mathbf{S}_n$ contains exactly $q$ odd permutations.

$\therefore$ $p \le q$ ...(1)

Similarly we can show that $q$ even permutations $t0_1, t0_2 \ldots, t0_q$ are all distinct even permutations in $\mathbf{S}_n$.

$\therefore$ $q \le p$ ...(2)

$\therefore$ From (1) and (2) $p = q = \frac{1}{2}n!$ $(\because\ p + q = n!)$

$\therefore$ Number of even permutations in $\mathbf{S}_n$ = Number of odd permutation sin $\mathbf{S}_n = \frac{1}{2}n!$.

**Definition.** Let $\mathbf{S}_n$ be the permutation group on $n$ symbols. The set of all $\frac{1}{2}n!$ even permutations of $\mathbf{S}_n$, denoted by $\mathbf{A}_n$ is called the alternating set of permutations of degree $n$.

**Theorem 8.** ***The set $\mathbf{A}_n$ of all even permutations of degree n forms a group of order $\mathbf{1/2}\, n!$ w.r.t. permutation multiplication.*** ***(A. U. M11, N.U. 00)***

**Proof. Closure.** Let $f, g \in \mathbf{A}_n$ are even permutations.

$\therefore$ $gf$ is an even permutation and hence $gf \in \mathbf{A}_n$.

**Associativity.** Since a permutation is a bijection, multiplication of permutations (composition of mappings) is associative.

**Existence of identity.** Let $f \in \mathbf{A}_n$. Let $\mathbf{I}$ be the identity permutation on the $n$ symbols, then $\mathbf{I} \in \mathbf{A}_n$, since $\mathbf{I}$ is an even permutation.

$\therefore$ $f\mathbf{I} = \mathbf{I}f$ for $f \in \mathbf{A}_n$ $\therefore$ Identity exists in $\mathbf{A}_n$ and $\mathbf{I}$ is the identity in $\mathbf{A}_n$.

**Existence of inverse.** Let $f \in \mathbf{A}_n$. $\therefore$ $f$ is an even permutation and $f^{-1}$ is also an even permutation on the $n$ symbols such that $f^{-1}f = ff^{-1} = \mathbf{I}$ for $f \in \mathbf{A}_n$.

$\therefore$ Every element of $\mathbf{A}_n$ is invertible and the inverse of $f$ is $f^{-1}$.

$\therefore$ $\mathbf{A}_n$ forms a group of order $\frac{1}{2}n!$ since the number of permutations on $n$ symbols is $\frac{1}{2}n!$

**Note 1.** The group $\mathbf{A}_n$ is called alternative group or alternating group of degree $n$ and the number of elements in $\mathbf{A}_n$ is $\frac{1}{2} \angle n$.

**2.** The product of two odd permutations is an even permutation and hence the set of odd permutations w.r.t. permutation multiplication is not a group.

**Theorem 9.** ***The set $\mathbf{A}_n$ of all even permutations on n symbols is a normal subgroup of the permutation group $\mathbf{S}_n$ on the n symbols.***

***(A. U. M11, A.N.U. M03, S93, A93, S.V.U. M03, O01, O99)***

**Proof.** $\mathbf{S}_n$ is a group on $n$ symbols w.r.t. permutation multiplication and $\mathbf{A}_n (\subset \mathbf{S}_n)$ is the set of even permutations. Also $\mathbf{A}_n$ is a group w.r.t. permutation multiplication.

Let $f \in \mathbf{S}_n$ and $g \in \mathbf{A}_n$.

$\therefore$ $g$ is an even permutation and $f$ is an even or odd permutation.

If $f$ is an odd permutation then $f^{-1}$ is also an odd permutation.

Also $fg$ is an odd permutation.

$\therefore$ $fgf^{-1}$ is an even permutation and hence $fgf^{-1} \in \mathbf{A}_n$

If $f$ is an even permutation, then $f^{-1}$ is also an even permutation. Also $fg$ is an even permutation.

$\therefore$ $fgf^{-1}$ is an even permutation and hence $fgf^{-1} \in \mathbf{A}_n$.

Thus $f \in \mathbf{S}_n, g \in \mathbf{A}_n \Rightarrow fgf^{-1} \in \mathbf{A}_n$

$\therefore$ $\mathbf{A}_n$ is a normal subgroup of $\mathbf{S}_n$

**Ex.** *Find $\mathbf{A}_3$ the normal subgroup of $\mathbf{P}_3$.* ***(K.U.S. 00, O.U. 01/0)***

**Sol.** Let $\mathbf{S} = \{a, b, c\}$ and $\mathbf{P}_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ be the permutation group on $\mathbf{S}$.

Now $f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = (a\ b)(b\ a)$ $\therefore$ $f_1$ is an even permutation.

$f_2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = (a\ b)$ $\therefore$ $f_2$ is an odd permutation.

$f_3 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = (b\ c)$ $\therefore$ $f_3$ is an odd permutation.

$f_4 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = (a\ c)$ $\therefore$ $f_4$ is an odd permutation.

$f_5 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = (a\ b\ c) = (a\ c)(a\ b)$ $\therefore$ $f_5$ is an even permutation.

$f_6 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = (a\ c\ b) = (a\ b)(a\ c)$ $\therefore$ $f_6$ is an even permutation.

$\mathbf{A}_3 = \{f_1, f_5, f_6\}$ is a normal subgroup of $\mathbf{P}_3$.

## 7.6. CAYLEY'S THEOREM

**Theorem 10.** ***Every finite group $\mathbf{G}$ is isomorphic to a permutation group.***

***(K. U. 07, A.N.U. M 01, S 00, S98, S97, S96, S93, A90, A89, A.V.O. 01, A 01, M 00, S96, S.K.U. M 03, O 02, M 01, O 00, A 00, A99, S.V.U. S 03, O 02, O 01, A98, O97, A97)***

**Proof.** Let $\mathbf{G}$ be a finite group. Let $a \in \mathbf{G}$. Then for every $x \in \mathbf{G}, ax \in \mathbf{G}$.

Now consider $f_a : \mathbf{G} \to \mathbf{G}$ defined by $f_a(x) = ax$ for $x \in \mathbf{G}$.

For $x, y \in \mathbf{G}$, $ax, ay \in \mathbf{G}$, $\therefore$ $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

$\therefore$ $f_a$ is well defined.

$f_a$ is one-one since for $x, y \in \mathbf{G}$ we have $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$.

$f_a$ is also onto since for $x \in \mathbf{G}$, $\exists\ a^{-1}x \in \mathbf{G}$

such that $f_a(a^{-1}x) = a\ (a^{-1}x) = (aa^{-1})\ x = ex = x$.

Thus $f_a : \mathbf{G} \to \mathbf{G}$ is one-one and onto.

$\therefore$ $f_a$ is a permutation on $\mathbf{G}$.

Let $\mathbf{G}' = \{f_a \mid a \in \mathbf{G}\}$ i.e., let $\mathbf{G}'$ be the set of all permutations (one-one and onto mappings defined on $\mathbf{G}$) defined on $\mathbf{G}$ corresponding to every element of $\mathbf{G}$. We shall show that $\mathbf{G}'$ is a group w.r.t. permutation multiplication.

**Closure.** For $a, b \in \mathbf{G}, f_a, f_b \in \mathbf{G}'$.

For $x \in \mathbf{G}, (f_a f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx)$

$= (ab)\,x = f_{ab}(x)$ since $ab \in \mathbf{G}$.

$\therefore$ $f_a f_b = f_{ab}$ and $f_{ab} \in \mathbf{G}'$. Hence $f_a f_b \in \mathbf{G}'$

**Associativity.** For $a, b, c \in \mathbf{G}, f_a, f_b, f_c \in \mathbf{G}'$.

For $x \in \mathbf{G}, ((f_a f_b) f_c)(x) = f_a((f_b) f_c(x)) = f_a f_b(f_c)(x)$

$= f_a f_b(f_c(x)) = f_a(f_b f_c(x))$

$\Rightarrow$ $(f_a f_b) f_c = f_a(f_b f_c)$

**Existence of identity.** Let $e$ be the identity in $\mathbf{G}$.

$\therefore$ $f_e \in \mathbf{G}$ and $f_e f_a = f_{ea} = f_{a'}$ $f_a f_e = f_{ae} = f_{a'}$.

$\therefore$ Identity in $\mathbf{G}'$ exists and it is $f_e$.

**Existence of inverse.** If $a \in \mathbf{G}$, then $a^{-1} \in \mathbf{G}$.

$\therefore$ $f_{a^{-1}} \in \mathbf{G}'$ and $f_{a^{-1}} f_a = f_{a^{-1}a} = f_{e'} f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$.

$\therefore$ Every element in $\mathbf{G}'$ is invertible and $[f_a]^{-1} = f_{a^{-1}}$

$\therefore$ $\mathbf{G}'$ is a group.

Finally we show that $\mathbf{G} \cong \mathbf{G}'$.

Consider $\phi : \mathbf{G} \to \mathbf{G}'$ defined by $\phi(a) = f_a$ for $a \in \mathbf{G}$.

$\phi$ is one-one since $\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow ax = bx \Rightarrow a = b$

for $x \in \mathbf{G}$ and $a, b \in \mathbf{G}$.

$\phi$ is onto since for $f_a \in \mathbf{G}', a \in \mathbf{G}$ such that $\phi(a) = f_a$.

$\phi$ is structure preserving since for $a, b \in \mathbf{G}$ and $ab \in \mathbf{G}$ and

$\phi(ab) = f_{ab} = f_a f_b = \phi(a)\,\phi(b)$.

$\therefore$ $\mathbf{G} \cong \mathbf{G}'$. $\mathbf{G}'$ is called a **regular permutation group.**

**Note 1.** The above theorem can also be stated as :

**Any finite group of order $n$ is isomorphic to a sub-group of the symmetric group $\mathbf{S}_n$** ***(A.U. M 74)***

**2.** Cayley's theorem is true even if the group $\mathbf{G}$ is **not** finite. If $\mathbf{G}$ is infinite then the statement of the theorem is : Every group is isomorphic to a group of one-one onto functions. ***(N.U. O 88, S 93)***

Above proof holds even here with the exception that the word permutation must be replaced by one-one onto function.

**Ex. 1.** *Examine whether the following permutations are even or odd.*

(i) $\begin{pmatrix}1&2&3&4&5&6&7\\3&2&4&5&6&7&1\end{pmatrix}$ ***(A. U. M11,N.U. 99, 2K)*** (ii) $\begin{pmatrix}1&2&3&4&5&6&7&8\\7&3&1&8&5&6&2&4\end{pmatrix}$

(iii) $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ 5)$ ***(N.U. 99, S2000, O91)***

(iv) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&1&4&3&2&5&7&8&9\end{pmatrix}$ ***(A.N.U. A91, 89, S.K.V. 2003)***

**Sol.** (i) $\begin{pmatrix}1&2&3&4&5&6&7\\3&2&4&5&6&7&1\end{pmatrix} = (1\ 3\ 4\ 5\ 6\ 7)(2)$

$= (1\ 3\ 4\ 5\ 6\ 7) = (1\ 7)(1\ 6)(1\ 5)(1\ 4)(1\ 3)$ [Product of 5 transpositions]

$\therefore$ The permutation is odd.

(ii) $\begin{pmatrix}1&2&3&4&5&6&7&8\\7&3&1&8&5&6&2&4\end{pmatrix} = (1\ 7\ 2\ 3)(4\ 8)(5)(6)$

$= (1\ 3)(1\ 2)(1\ 7)(4\ 8)$ [Product of 4 transpositions]

$\therefore$ The permutation is even.

(iii) $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ 5) = (1\ 2)(1\ 3)(1\ 4)(1\ 5)(1\ 2)(1\ 3)(4\ 5)$

$= (1\ 2)(1\ 3)(1\ 4)(1\ 5)(4\ 5)$ Product of 5 transpositions.

$\therefore$ The permutation is odd.

(iv) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&1&4&3&2&5&7&9&8\end{pmatrix} = (1652)\ (34)\ (7)(89) = (12)\ (15)\ (16)\ (34)\ (89)$

$\therefore$ The permutation is odd.

**Ex.2.** *Find the regular permutation group isomorphic to the multiplicative group* $\{1, \omega, \omega^2\}$. ***(A.N.M99, M98, S.K.V. M2001)***

**Sol.** We use Cayley's Theorem.

$\mathbf{G} = \{1, \omega, \omega^2\}$ and $f_a : \mathbf{G} \to \mathbf{G}$ be a mapping defined by $f_a(x) = ax$ for each $a \in \mathbf{G}$ and $x$ is any element of $\mathbf{G}$.

The regular permutation group $= \{f_1, f_\omega, f_{\omega^2}\}$

where $f_1 = \begin{pmatrix}1&\omega&\omega^2\\1.1&1.\omega&1.\omega^2\end{pmatrix} = \begin{pmatrix}1&\omega&\omega^2\\1&\omega&\omega^2\end{pmatrix}$ (identity permutation)

$$f_\omega = \begin{pmatrix}1&\omega&\omega^2\\\omega.1&\omega\omega&\omega.\omega^2\end{pmatrix} = \begin{pmatrix}1&\omega&\omega^2\\\omega&\omega^2&\omega^3\end{pmatrix} = \begin{pmatrix}1&\omega&\omega^2\\\omega&\omega^2&1\end{pmatrix}$$

and $$f_{\omega^2} = \begin{pmatrix}1&\omega&\omega^2\\\omega^2.1&\omega^2\omega&\omega^2.\omega^2\end{pmatrix} = \begin{pmatrix}1&\omega&\omega^2\\\omega^2&\omega^3&\omega^4\end{pmatrix} = \begin{pmatrix}1&\omega&\omega^2\\\omega^2&1&\omega\end{pmatrix}$$

**Ex. 3.** *Find the regular permutation group isomorphic to the multiplicative group* $\{1, -1, i, -i\}$. ***(A.V.S. 00, S99, S98, S97, A.N.V.M97, S.V.U. O98)***

**Sol.** We use Cayley's theorem,

Let $\mathbf{G} = \{1, -1, i, -i\}$ and $f_a : \mathbf{G} \to \mathbf{G}$ be a mapping defined by $f_0(x) = ax$ for each $a \in \mathbf{G}$ and $x$ is any element of $\mathbf{G}$.

Then the regular permutation group $= \{f_1, f_{-1}, f_i, f_{-i}\}$ where

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1.1 & 1.-1 & 1.i & 1.-i \end{pmatrix} = \begin{pmatrix} -1 & 1 & i & -i \\ -1 & 1 & i & -i \end{pmatrix} = \mathbf{I} \text{ (identity permutation)}$$

$$f_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ -1.1 & -1.-1 & -1.i & -1.-i \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix},$$

$$f_i = \begin{pmatrix} 1 & -1 & i & -i \\ i.1 & i.-1 & i.i & i.-i \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix},$$

$$f_{-i} = \begin{pmatrix} 1 & -1 & i & -i \\ -i.1 & -i.-1 & -i.i & -i.-i \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$$

**Ex. 4.** $\mathbf{G} = \{e, x, y, xy\}$. $'o'$ *is an operation defined on* $\mathbf{G}$ *such that* $x^2 = y^2 = e$ *and* $xy = yx$. *Find the regular permutation group isomorphic to the group* $(\mathbf{G}, o)$.

**Sol.** We use Cayley's theorem. $e$ is the identity of $\mathbf{G}$ let $f_a : \mathbf{G} \to \mathbf{G}$ be a mapping defined by $f_a(x) = ax$ for each $a \in \mathbf{G}$ and $x$ is any element of $\mathbf{G}$.

Then the regular permutation group $= \{f_e, f_x, f_y, f_{xy}\}$

where $f_e = \begin{pmatrix} e & x & y & xy \\ ee & ex & ey & exy \end{pmatrix} = \begin{pmatrix} e & x & y & xy \\ e & x & y & xy \end{pmatrix} = \mathbf{I}$,

$$f_x = \begin{pmatrix} e & x & y & xy \\ xe & xx & xy & xxy \end{pmatrix} = \begin{pmatrix} e & x & y & xy \\ x & e & xy & y \end{pmatrix} \text{ since } xxy = x^2y = ey = y,$$

$$f_y = \begin{pmatrix} e & x & y & xy \\ ye & yx & yy & yxy \end{pmatrix} = \begin{pmatrix} e & x & y & xy \\ y & xy & e & x \end{pmatrix} \text{ since } yxy = xyy = xy^2 = xe = x,$$

$$f_{xy} = \begin{pmatrix} e & x & y & xy \\ xye & xyx & xyy & xyxy \end{pmatrix} = \begin{pmatrix} e & x & y & xy \\ xy & y & x & e \end{pmatrix}$$

since $xyx = yxx = yx^2 = ye = y$, $xyy = xy^2 = xe = x$,

$$xyxy = xyyx = xy^2x = xex = x^2 = e.$$

**Ex. 5.** *Write down all the permutations on four symbols* 1, 2, 3, 4. *Which of these permutations are even permutations?*

**Sol.** Let $\mathbf{S} = \{1, 2, 3, 4\}$. Let $\mathbf{S}_4$ be the set of all permutations on $\mathbf{S}$.

Then $\mathbf{S}_4 = \{(1)(1\ 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)$.

$(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4)$,

$(1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3)$

$(1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2),$
$(1\ 2)(3\ 4), (2\ 3)(1\ 4), (3\ 1)(2\ 4).\}$

Now $\mathbf{S}_4$ is a non-abelian group under permutation multiplication.

Let $\mathbf{A}_4$ be the set of all even permutations in $\mathbf{S}$. $\mathbf{A}_4$ contains $\frac{1}{2}(4!)$ elements i.e. 12 elements.

Then $\mathbf{A}_4 = \{(1)\,(1\ 2\ 3), (1\,3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4)$

$(1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2)\,(3\ 4), (2\ 3)\,(1\ 4), (3\ 1)\,(2\ 4).\}$

**Note.** $\mathbf{S}_4$ is a non-abelian group i.e. $\mathbf{A}_4$ is a non-abelian sub-group of the non-abelian group $\mathbf{S}_4$. Hence a non-abelian group can have a non-abelian subgroup.

**Ex.6.** *Find the order of n-cycle in the permutation group* $\mathbf{S}_n$. ***(N.U. 89)***

**Sol.** Let $\mathbf{S}_n$ be a permutation group on $\mathbf{S} = \{a_1, a_2, \ldots\ldots, a_n\}$

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 \ldots & a_n & a_1 \end{pmatrix}$ be n-cycle in $\mathbf{S}_n$.

Then $f^2 = ff = \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 \ldots & a_n & a_1 \end{pmatrix}\begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 \ldots & a_n & a_1 \end{pmatrix}$

$= \begin{pmatrix} a_1 & a_2 & a_3 \ldots & a_{n-2} & a_{n-1} & a_n \\ a_3 & a_4 & a_5 \ldots & a_n & a_1 & a_2 \end{pmatrix}$

Thus in $f^2 : a_1 \to a_3,\ a_2 \to a_4,\ \ldots,\ a_n \to a_2;$

in $f^3 : a_1 \to a_4,\ a_2 \to a_5,\ \ldots,\ a_n \to a_3;$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

in $f^{n-1} : a_1 \to a_n,\ a_2 \to a_1,\ \ldots,\ a_n \to a_1;$

in $f^n : a_1 \to a_1,\ a_2 \to a_2,\ \ldots,\ a_n \to a_n$

$\therefore$ $f^n = \mathrm{I}$, the identity permutation in $\mathbf{S}_n$.

$\therefore$ Order of $n$ - cycle $f$ in $\mathbf{S}_n$ is $n$.

**Ex. 7.** $\mathbf{S}_n$ *be a symmetric group of* $n$ *symbols and let* $\mathbf{A}_n$ *be the group of even permutations. Then show that* $\mathbf{A}_n$ *is normal in* $\mathbf{S}_n$ *and* $\mathbf{O}(\mathbf{A}_n) = \frac{1}{2}n!$.

***(A.N.U.M 03, N.U. S 93, A93, S.V.U. M, O 96, O 01, O99, M 03)***

**Sol.** Let the $n$ symbols be 1, 2, 3, $\ldots n$. $\mathbf{S}_n$ is the symmetric group of the $n$ symbols w.r.t. permutation multiplication and $\mathbf{A}_n (\subset \mathbf{S}_n)$ is the set of all even permutations.

We know that $\mathbf{G} = \{1, -1\}$ is a group under usual multiplication and 1 is the identity in $\mathbf{G}$.

Define a mapping $f : \mathbf{S}_n \to \mathbf{G}$ such that $\phi \in \mathbf{S}_n$,

$$f(\phi) = \begin{cases} 1, & \text{when } \phi \text{ is an even permutation} \\ -1, & \text{when } \phi \text{ is an odd permutation} \end{cases}$$

Thus all the even permutations of $\mathbf{S}_n$ under $f$ are mapped into 1 and all the odd permutations of $\mathbf{S}_n$ under $f$ are mapped into $-1$. now we prove that $f : \mathbf{S}_n \to \mathbf{G}$ is an onto homomorphism with $\mathbf{A}_n$ as Kernel.

Let $\phi_1, \phi_2$ be even $\Rightarrow$ $\phi_1 \phi_2$ is even. (ii) both $\phi_1, \phi_2$ are odd (iii) one is even and the other is odd.

(i) $\phi_1, \phi_2$ are even $\Rightarrow$ $\phi_1 \phi_2$ is even

$\therefore$ $f(\phi_1) = 1, f(\phi_2) = 1$ and $f(\phi_1 \phi_2) = 1$

and hence $f(\phi_1 \phi_2) = 1 = 1.1 = f(\phi_1) . f(\phi_2)$.

(ii) $\phi_1, \phi_2$ are odd $\Rightarrow$ $\phi_1 \phi_2$ is even.

$\therefore$ $f(\phi_1) = -1, f(\phi_2) = -1$ and $f(\phi_1 \phi_2) = 1$

and hence $f(\phi_1 \phi_2) = (-1)(-1) = f(\phi_1) . f(\phi_2)$.

(iii) $\phi_1$ is even and $\phi_2$ odd (say) $\therefore$ $\phi_1 \phi_2$ is odd

Also $f(\phi_1) = 1, f(\phi_2) = -1$ and $f(\phi_1 . \phi_2) = -1$

and hence $f(\phi_1 \phi_2) = -1 = (1)(-1) = f(\phi_1) . f(\phi_2)$

$\therefore$ In all the cases (i), (ii) and (iii) $f(\phi_2 \phi_2) = f(\phi_1) . f(\phi_2)$

$\therefore$ $f : \mathbf{S}_n \to \mathbf{G}$ is a homomorphism.

Also from the definition $f$ is onto.

Since all the pre-images of 1 of $\mathbf{G}$ are even permutations of $\mathbf{S}_n$ and since no other permutation of $\mathbf{S}_n$ has its image as 1, $\ker f = \mathbf{A}_n$ (the set of all even permutations)

But $\ker f$ is a normal subgroup of $\mathbf{S}_n$

$\therefore$ By the fundamental theorem on homomorphism, $\dfrac{\mathbf{S}_n}{\mathbf{A}_n} \cong \mathbf{G}$.

$$O\left(\frac{S_n}{A_n}\right) = O(G) = 2 \Rightarrow \frac{O(S_n)}{O(A_n)} = 2 \Rightarrow O(A_n) = \frac{1}{2} O(S_n) = \frac{1}{2} n!.$$

## EXERCISE 7

**1.** Express $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ as a product of transpositions. ***(S.V.U. A 93)***

**2.** Write down the inverses of the following permutations.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$ (ii) $\begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ (iii) $(2\ 5\ 1\ 6)(3\ 7)$

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ ***(O.U.A2000, A93)*** (v) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ ***(O.U. O99)***

**3.** Find whether the permutation is odd or even..

$$\begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 6&1&4&3&2&5&7&9&8 \end{pmatrix}$$

Also show that the inverse of the permutation is odd.

**4.** Write down the following permutations are products of disjoint cycles.

(i) $\begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 3&7&1&4&8&2&6&5 \end{pmatrix}$ (ii) $(4\ 3\ 1\ 2\ 5)(1\ 4\ 5\ 2)$ (on 5 symbols)

(iii) $(1\ 3\ 2\ 5).(1\ 4\ 3).(2\ 5\ 1)$ ***(K.V.M. 04, O.U.A. 01, O 01, S.V.U. A 93)***

**5.** If $f = (1\ 2\ 3\ 4\ 5\ 6)$ show that $f^2 = (2\ 4\ 6)(1\ 3\ 5)$ and $f^3 = (1\ 4)(2\ 5)(3\ 6)$.

***(S.V.U. O 93)***

**6.** Prove that $(1\ 2\ 3\ 4\ \ldots\ n)^{-1} = (n(n-1)\ldots 4\ 3\ 2\ 1)$.

**7.** (i) Express $(1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$ as the product of disjoint cycles and find its inverse. ***(O.U. 91)***

(ii) Express $(1\ 2\ 3)(4\ 5\ 6)(1\ 6\ 7\ 8\ 9)$ as a product of disjoint cycles. Find its inverse.

***(O. U. O 98)***

**8.** If $\mathbf{A} = \begin{pmatrix} 1&2&3&4&5 \\ 2&3&1&5&4 \end{pmatrix}$ $\mathbf{B} = \begin{pmatrix} 1&2&3&4&5 \\ 1&3&4&5&2 \end{pmatrix}$ calculate $\mathbf{AB, BA, A^{-1}, A^2B, B^{-1}A^2}$

**9.** If $f = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 6)$, $g = (4\ 1\ 5\ 6\ 7\ 3\ 2\ 8)$ are cyclic permutations then show that $(fg)^{-1} = g^{-1}f^{-1}$.

**10.** Verify whether the following permutation is even or odd.

(i) $\begin{pmatrix} 1&2&3&4&5&6&7 \\ 3&1&4&7&6&2&5 \end{pmatrix}$ ***(S.K.U. O2003)***

(ii) $\begin{pmatrix} 1&2&3&4&5&6 \\ 2&3&1&4&6&5 \end{pmatrix}$ ***(S.V.O. S93)***

(iii) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 2&5&4&3&6&1&7&9&8 \end{pmatrix}$ ***(K.U.M. 2004, O99)***

(iv) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 5&8&2&1&9&6&3&7&4 \end{pmatrix}$ ***(K.U.M. 96)***

(v) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 2&9&4&8&3&5&1&6&7 \end{pmatrix}$ ***(K.U.M. 96)***

(vi) $\begin{pmatrix} 1&2&3&4&5&6 \\ 3&1&2&4&6&5 \end{pmatrix}$ ***(S.K.U.A.99)***

## ANSWERS

**1.** (1 2) (1 3) (5 6)

**2.** (i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ (iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 4 & 2 & 1 & 3 \end{pmatrix}$ (iv) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ (v) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

**3.** odd **4.** (i) (1 3) (2 7 6) (5 8) (ii) (1 3) (iii) (1 5 4 2)

**7.** (i) (2 3 4 5 6 7 8 9) (ii) (1 4 5 6 7 8 9 2 3), (3 2 9 8 7 6 5 4 1)

**8.** $\mathbf{AB} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$, $\mathbf{BA} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$, $\mathbf{A}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$,

$\mathbf{A}^2\mathbf{B} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$, $\mathbf{B}^{-1}\mathbf{A}^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$

**10.** (i) even (ii) odd (iii) odd (iv) even (v) odd (vi) odd.

# Cyclic Groups

**8.1.** Before defining a cyclic group, we prove a theorem that serves as a motivation for the definition of cyclic group.

**Theorem.** *Let* $\mathbf{G}$ *be a group and* $a$ *be an element of* $\mathbf{G}$. *Then* $\mathbf{H} = \{a^n / n \in \mathbf{Z}\}$ *is a subgroup of* $\mathbf{G}$. *Further* $\mathbf{H}$ *is the smallest of subgroups of* $\mathbf{G}$ *which contain the element* $a$. *(N.U. 92)*

**Proof.** Let $(\mathbf{G}, .)$ be a group and $a \in \mathbf{G}$.

For $1 \in \mathbf{Z}$ we have $a^1 = a \in \mathbf{H}$ which shows that $\mathbf{H}$ is non empty.

Suppose now that $a^r, a^s \in \mathbf{H}$. We will show that (i) $a^r a^s \in \mathbf{H}$ and $(a^r)^{-1} \in \mathbf{H}$ which will prove that $\mathbf{H}$ is a subgroup of $\mathbf{G}$.

$$a^r, a^s \in \mathbf{H} \Rightarrow r, s \in \mathbf{Z} \Rightarrow r + s, -r \in \mathbf{Z}$$

$\therefore\ a^r . a^s = a^{r+s} \in \mathbf{H}$ and $(a^r)^{-1} = a^{-r} \in \mathbf{H}$

$\therefore\ \mathbf{H}$ is a subgroup of $\mathbf{G}$.

(ii) Suppose $\mathbf{K}$ is any other subgroup of $\mathbf{G}$ such that $a \in \mathbf{K}$. Then $a^n \in \mathbf{K}\ \forall\ n \in \mathbf{Z}$.

$\therefore\ \mathbf{H} \subset \mathbf{K}$ which shows that $\mathbf{H}$ is the subset of every subgroup of $\mathbf{G}$ which contains $a$.

Thus $\mathbf{H}$ is the smallest of subgroups of $\mathbf{G}$ which contain $a$.

## 8.2. CYCLIC SUBGROUP GENERATED BY $a$

**Definition.** Suppose $\mathbf{G}$ is a group and $a$ is an element of $\mathbf{G}$. Then the subgroup $\mathbf{H} = \{a^n / n \in \mathbf{Z}\}$ is called a cyclic subgroup generated by $a$. $a$ is called a generator of $\mathbf{H}$. This will be written as $\mathbf{H} = < a >$ or $(a)$ or $\{a\}$.

**Cyclic group.**

**Definition.** Suppose $\mathbf{G}$ is a group and there is an element $a \in \mathbf{G}$ such that $\mathbf{G} = \{a^n \mid n \in \mathbf{Z}\}$. Then $\mathbf{G}$ is called a **cyclic** group and $a$ is called a generator of $\mathbf{G}$.

We denote $\mathbf{G}$ by $< a >$. ***(A.N.U.J 04, M99, O91, A90, A89, A.U.M. 05, S 00, K.U.O96, O.U. M12, O 02, A 01, A99, S.K.U.O98, A97, S.V.M. 03, O 01, S 03, A99)***

Thus a group consisting of elements which are only the power of a single element belonging to it is a cyclic group. ***(O.U. O 98, S.V.U. S 01)***

Let $\mathbf{G}$ be a group and $a \in \mathbf{G}$. If the cyclic subgroup of G generated by $a$ *i.e.* $< a >$ is finite, then the order of the subgroup i.e. $|< a >|$ is the order of $a$. If $< a >$ is infinite then we say that the order of $a$ is infinite.

**Note.** If $\mathbf{G}$ is a cyclic group generated by $a$, then the elements of $\mathbf{G}$ will be $\ldots a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots$ in multiplicative notation and the elements of $\mathbf{G}$ will be $\ldots -2a, -a, 0a = 0, a, 2a, \ldots$ in additive notation. The elements of $\mathbf{G}$ are not necessarily distinct. There exist finite and infinite cyclic groups.

**e.g. 1.** $\mathbf{G} = \{1, -1\}$ is a multiplicative group. Since $(-1)^0 = 1, (-1)^1 = -1, (\mathbf{G}, .)$ is a cyclic group generated by $-1$ i.e. $\mathbf{G} = <-1>$. It is a finite cyclic group of order 2 and $O(-1) = 2$.

**e.g. 2.** $\mathbf{G} = \{\ldots -4, -2, 0, 2, 4, \ldots\}$ is an additive group.

Since $\mathbf{G} = \{2m / m = \ldots -1, 0, 1, 2, \ldots\}$, $\mathbf{G}$ is a cyclic group generated by 2 i.e. $\mathbf{G} = <2>$. It is an infinite cyclic group.

**e.g. 3.** $(\mathbf{Q}, +), (\mathbf{Q}^+, \cdot)$ are groups but are not cyclic.

**e.g. 4.** $\{12^n / n \in \mathbf{Z}\}$ is a cyclic group w.r.t. usual multiplication.

Its generators are $12, 1/12$.

**e.g. 5.** $<18>$ is a cyclic subgroup of the cyclic group $(\mathbf{Z}_{36}, +_{36})$ and since

$18^1 = 18, 18^2 = 18 +_{36} 18 = 0,\ 18^3 = 18^2 +_{36} 18 = 18, 18^4 = 18^3 +_{36} 18 = 18 +_{36} 18 = 0, \ldots\ldots,$

we have $<18> = \{0, 18\}$.

**e.g. 6.** Let $\mathbf{G} = \mathbf{S}_3$ and $\mathbf{H} = \{(1), (1\,3)\}$.

Then the left cosets of H in G are :

$$(1)\,\mathbf{H} = \mathbf{H}, (1\,2)\,\mathbf{H} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3\,2)\,\mathbf{H},$$

$(1\,3)\,\mathbf{H} = \mathbf{H}, (2\,3)\,\mathbf{H} = (1\,2\,3)\,\mathbf{H}$. (Analogous results hold for right cosets)

**Theorem 1.** *Let $(\mathbf{G}, \cdot)$ be a cyclic group generated by a. If $O(a) = n$, then $a^n = e$ and $\{a, a^2, \ldots\ldots, a^{n-1}, a^n = e\}$ is precisely the set of distinct elements belonging to G where e is the identity in the group $(\mathbf{G}, \cdot)$.*

(For proof, vide Theorem 13 of Art 8.5)

**Theorem 2.** *If $\mathbf{G}$ is a finite group and $a \in \mathbf{G}$, then $o(a) / o(\mathbf{G})$*

*(N. U. O 91, A. U. M. 98, K. U. J. 02, O.U. 01/0)*

**Proof.** $\mathbf{G}$ is a finite group. Let $o(\mathbf{G}) = m$.

Let $\mathbf{H}$ be the cyclic subgroup of $\mathbf{G}$ generated by $a$.

Let $o(a) = n$ $\quad\therefore\quad o(\mathbf{H}) = n$ (Vide Theorem 25, Art. 2.17.)

But by Lagrange's Theorem, $o(\mathbf{H}) / o(\mathbf{G})$.

$n / o(\mathbf{G})$ i.e. $o(a) / o(\mathbf{G})$.

**Note.** If $o(a) = n$ and $a \in \mathbf{G}$, then $o(\mathbf{H}) \le o(\mathbf{G})$.

**Theorem 3.** *If $\mathbf{G}$ is a finite group of order $n$ and if $a \in \mathbf{G}$, then $a^n = e$ (identity in $\mathbf{G}$).* *(N.U. S 99)*

**Proof.** Let $o(a) = d$ and $a^d = e$ and $d \le n$.

If $\mathbf{H}$ is a cyclic subgroup generated by $a$, then $o(\mathbf{H}) = d = o(a)$.

But by Lagrange's Theorem, $o(\mathbf{H}) / o(\mathbf{G})$ i.e. $d / n$.

$\therefore\ \exists a$ positive integer $q$ such that $n = dq$. $\quad\therefore\ a^n = a^{dq} = (a^d)^q = e^q = e$.

**Note.** The statement of the above theorem may be : If $\mathbf{G}$ is a finite group, then for any $a \in \mathbf{G}$, $a^{0(G)} = e$.

**Ex. 1.** *Let* $\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $\mathbf{C} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ *and* $\mathbf{D} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

*We have that* $\mathbf{G} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}\}$ *with matrix multiplication as operation is a group whose composition table is given below.*

**Sol.** Here $\mathbf{O(G)} = 4, \mathbf{A}$ is the identity element in $\mathbf{G}$. Now we can see that

$\mathbf{B}^1 = \mathbf{B}, \mathbf{B}^2 = \mathbf{B}.\mathbf{B} = \mathbf{C}$,

$\mathbf{B}^3 = \mathbf{B}^2.\mathbf{B} = \mathbf{C}.\mathbf{B} = \mathbf{D}$,

$\mathbf{B}^4 = \mathbf{B}^3.\mathbf{B} = \mathbf{D}.\mathbf{B} = \mathbf{A}$.

Thus $\mathbf{B} \in \mathbf{G}$ generated the group $\mathbf{G}$ and hence $\mathbf{G}$ is a cyclic group with $\mathbf{B}$ as generator i.e. $\mathbf{G} = <\mathbf{B}>$.

Note that $\mathbf{O(B)} = 4 = \mathbf{O(G)}$ and $\mathbf{B}^{\mathbf{O(G)}} = \mathbf{A}$.

Also $\mathbf{G}$ is abelian.

**Note :** A, C, D are not generators of the group $\mathbf{G}$.

| | A | B | C | D |
|---|---|---|---|---|
| A | A | B | C | D |
| B | B | C | D | A |
| C | C | D | A | B |
| D | D | A | B | C |

**Ex. 2.** *Prove that* $(\mathbf{Z}, +)$ *is cyclic group.* ***(S.V.U. S 93)***

**Sol.** $(\mathbf{Z}, +)$ is a group and $1 \in \mathbf{Z}$.

When we take additive notation in $\mathbf{Z}$, $a^n$ becomes $na$.

$1^0 = 0.1 = 0$, $1^1 = 1.1 = 1$, $1^2 = 2.1 = 2$, etc.

Also $1^{-1} = -1$, $1^{-2} = -2.1 = -2$, etc.

$\therefore$ 1 is a generator of the cyclic group $(\mathbf{Z}, +)$ i.e. $\mathbf{Z} = <1>$.

Similarly we can prove that $\mathbf{Z} = <-1>$.

**Note 1.** $(\mathbf{Z}, +)$ has no generators except 1 and $-1$.

For: Let $r = 4 \in \mathbf{Z}$.

We cannot write every element $m$ of $z$ in the form $m = 4n$. For example, $7 = 4n$ is not possible for $n \in \mathbf{Z}$. Thus when $r$ is an integer greater than 1, $r$ is not a generator of $\mathbf{Z}$.

Similarly when $r$ is an integer less than $-1$ also, $r$ is not a generator of $\mathbf{Z}$.

Thus $(\mathbf{Z}, +)$ is a cyclic group with only two generators 1 and $-1$.

**2.** $(\mathbf{Z}, +)$ is an infinite abelian group and it is a cyclic group.

**Ex. 3.** *Show that* $\mathbf{G} = \{1, -1, i, -i\}$ *the set of all fourth roots of unity, is a cyclic group w.r.t. multiplication.* ***(S.K. U 02, O.U. O 99)***

**Sol.** Clearly $(\mathbf{G}, \cdot)$ is a group. We see that $(i)^1 = i$, $i^2 = i.i = -1$, $i^3 = i^2.i = -1.i = -i$.

$i^4 = i^3.i = (-i)\,i = 1$

Thus all the elements of $\mathbf{G}$ are the powers of $i \in \mathbf{G}$ i.e. $\mathbf{G} = <i>$. Similarly we can have $\mathbf{G} = <-i>$. Note that $0(\mathbf{G}) = 0(i) = 0(-i) = 4$. Also $\mathbf{G}$ is abelian.

**Note.** $(\mathbf{G}, .)$ is a finite abelian group which is cyclic.

**Ex. 4.** *Show that the set of all cube roots of unity is a cyclic group w.r.t. multiplication.* ***(N.U. 99)***

**Sol.** If $\omega$ is one of the complex cube roots of unity, we know that $\mathbf{G} = \{1, \omega, \omega^2\}$ is a group w.r.t. multiplication. We see that $\omega^1 = \omega, \omega^2 = \omega\omega = \omega^2, \omega^3 = 1$.

$\therefore$ Then elements of $\mathbf{G}$ are the powers of the single element $\omega \in \mathbf{G}$.

$\therefore$ $\mathbf{G} = <\omega>$

We can also have $\mathbf{G} = <\omega^2>$. $(\because (\omega^2)^1 = \omega^2, (\omega^2)^2 = \omega, (\omega^2)^3 = 1)$

**Ex. 5.** *Prove that the group* $(\{1,2,3,4\}, \times_5)$ *is cyclic and write its generators.*

**Sol.** $2 \times_5 2 = 4, 2 \times_5 2 \times_5 2 = 4 \times_5 2 = 3, 2 \times_5 2 \times_5 2 \times_5 2 = 1, \; 2 \times_5 2 \times_5 2 \times_5 2 \times_5 2 = 2$

$\Rightarrow$ 2 is a generator of the group $\Rightarrow$ the group is cyclic.

Also for the group 3 is a generator.

1, 4 are not generators of the cyclic group.

**Ex. 6 (*a*).** *Show that* $(\bar{\mathbf{Z}}_5, +)$ *where* $\bar{\mathbf{Z}}_5$ *is the set of all residue classes modulo 5, is a cyclic group w.r.t. addition* $(+)$ *of residue classes.*

**Sol.** The composition table for the group $(\bar{\mathbf{Z}}_5, +)$ is;

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

We can have

$\bar{1} = \bar{1}, \; (\bar{1})^2 = 2(\bar{1}) = \bar{1} + \bar{1} = \bar{2}$

$(\bar{1})^3 = (\bar{1}^2) + (\bar{1}) = \bar{2} + \bar{1} = \bar{3}$

$(\bar{1})^4 = (\bar{1})^3 + (\bar{1}) = \bar{3} + \bar{1} = \bar{4}$

Thus $(\bar{\mathbf{Z}}_5, +)$ is a cyclic group with $\bar{1}$ as generator.

$\therefore$ $(\bar{\mathbf{Z}}_5, +) = <\bar{1}>$.

Similarly we can prove that $\bar{2}, \bar{3}, \bar{4}$ are also generators of this cyclic group.

**Ex. 6 (*b*).** *Show that* $(\bar{\mathbf{Z}}_m, +)$, *where* $\bar{\mathbf{Z}}_m$ *is the set of all residue classes modulo-m and + is the residue class addition, is a cyclic group.*

**Sol.** We have $(\bar{\mathbf{Z}}_m, +)$ as an abeian group.

We can have $(\bar{1})^1 = 1, (\bar{1})^2 = 2(\bar{1}) = \bar{1} + \bar{1} = \bar{2}$

$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$

$(\bar{1})^{m-1} = (\bar{1})^{m-2} + (\bar{1})^1 = (m-2)\bar{1} + \bar{1} = \overline{m-1}$

and $(\bar{1})^m = (\bar{1})^{m-1} + (\bar{1})^1 = (m-1)\bar{1} + \bar{1} = \bar{m} = \bar{0}$

Thus $\bar{1}$ is a generator of $(\bar{\mathbf{Z}}_m, +)$ i.e. $(\bar{\mathbf{Z}}_m, +) = <\bar{1}>$

**Note.** We can prove that $\overline{m-1}$ is also a generator of $(\bar{\mathbf{Z}}_m, +)$.

**Ex. 7.** *If* $\mathbf{G}$ *is the group of all symmetries of an equilateral triangle (vide Ex. 16, Chapter 2) we have that* $\mathbf{H} = \{r_0, r_1, r_2\}$ *is again a group w.r.t. the composition of maps. Show that* $(\mathbf{H}, o)$ *is a cyclic group.*

**Sol.** The composition table for the group $(\mathbf{H}, o)$ is :

We can have

$r_1 = r_1,\ r_1^2 = r_1 o r_1 = r_2,\ r_1^3 = r_1^2 o r_1 = r_2 o r_1 = r_0$

Thus $r_1$ is a generator for the group $(\mathbf{H}, o)$.

$\therefore$ $(\mathbf{H}, o)$ is cyclic group.

Similarly we can prove that

$r_2$ is also a generator of the group $(\mathbf{H}, o)$.

| | | | |
|---|---|---|---|
| 0 | $r_0$ | $r_1$ | $r_2$ |
| $r_0$ | $r_0$ | $r_1$ | $r_2$ |
| $r_1$ | $r_1$ | $r_2$ | $r_0$ |
| $r_2$ | $r_2$ | $r_0$ | $r_1$ |

**Ex. 8.** *Show that the set of all $n^{th}$ roots of unity w.r.t. multiplication is a cyclic group.* ***(O.U. A 2001, N.U. A 92, A.U. A 76)***

**Sol.** We know that (vide Ex. 8, Chapter 2)

$$G = \{\omega^0 = 1, \omega^1, \omega^2, \ldots \omega^{n-1}\}$$

where $\omega^k = e^{\frac{2k\pi i}{n}}$, $k = 0, 1, 2, \ldots, (n-1)$ is a group under multiplication.

We can have $\omega^0 = 1 = e, \omega^1 = \omega, \omega^2 = \omega.\omega = \omega^2, \omega^3 = \omega^2.\omega = \omega^3, \ldots \omega^{n-1} = \omega^{n-1}$.

Thus every element of $\mathbf{G}$ is some power of $\omega$ i.e. $(\mathbf{G}, .) = <\omega>$

**Ex. 9 (*a*).** *$\mathbf{Z}_n$ is the set of residues under addition modulo n. Show that $(\mathbf{Z}_n, +_n)$ is an abelian cyclic group.*

**Sol.** Clearly $\mathbf{Z}_n = \{0, 1, 2, 3, \ldots, (n-1)\}$ is an abelian group under $+_n$ (Theorem. 14, Art. 2.12)

Now $1^1 = 1, 1^2 = 1 +_n 1 = 2, \ldots,$

$1^{n-1} = 1 +_n 1 +_n 1 +_n \ldots +_n 1$ $(n-1$ times$) = n-1,$

$1^n = 1 +_n 1 +_n 1 +_n \ldots n$ times $= 0$

$\therefore$ 1 is a generator of $(\mathbf{Z}_n, +_n)$ and hence $(\mathbf{Z}_n, +_n)$ is a cyclic group which is abelian.

The other generator is $n-1$. (Theorem. 4, Art 8.3)

Thus $\mathbf{Z}_n = <1> = <n-1>$.

**Ex. 9 (*b*).** *Show that $(n\mathbf{Z}, +)$ is a cyclic subgroup of $(\mathbf{Z}, +)$ where $n$ is a positive fixed integer.* ***(A.N.U. S 00)***

**Sol.** We have to prove that $(n\mathbf{Z}, +)$ is a subgroup of $(\mathbf{Z}, +)$. (vide Ex.1 of Chapter 2)

We have $n\mathbf{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$

$\therefore$ $(n\mathbf{Z}, +) = <n>$ and $(n\mathbf{Z}, +) = <-n>$.

**Note.** $(n\mathbf{Z}, +)$ is a subgroup of the group $(\mathbf{Z}, +)$ and $(n\mathbf{Z}, +)$ is cyclic.

## 8. 3. SOME PROPERTIES OF CYCLIC GROUPS

**Theorem 4.** ***Every cyclic group is an abelian group.*** ***(K. U. M11, S.V.U. 92, N.U. S 93, A 92, O 89, M99, M98, O.U. M12, 93, A99, O 00, A 02, 03, 08 )***

**Proof.** Let $\mathbf{G} = <a>$ by a cyclic group.

We have $\mathbf{G} = \{a^n / n \in \mathbf{Z}\}$. Let $a^r, a^s \in \mathbf{G}$ $\therefore$ $a^r.a^s = a^{r+s}$ since $r, s \in \mathbf{Z}$

$= a^{s+r} = a^s.a^r$ $\therefore$ $\mathbf{G}$ is abelian.

**Note.** Converse is not true i.e. every abelian group is not cyclic. Klein's group of 4 is an example. (Ex. 11, Chapter 2) ***(O.U.A. 02, 08, N.V.S93)***

$$e = e^2 = e^3 = e^4; a = a, a^2 = e, a^3 = a, a^4 = e$$
$$b = b, b^2 = e, b^3 = b, b^4 = e, c = c, c^2 = e, c^3 = c, c^4 = e$$

None of the elements of $\mathbf{G}$ generates $\mathbf{G}$ even though $\mathbf{G}$ is abelian i.e. $\mathbf{G}$ is abelian but not cyclic. ***(N.U. S 93)***

**e. g.** Consider the set $\mathbf{G} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}\}$ where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \mathbf{D} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

and the matrix multiplication as the binary composition on $\mathbf{G}$.

Composition table is :

| | A | B | C | D |
|---|---|---|---|---|
| A | A | B | C | D |
| B | B | A | D | C |
| C | C | D | A | B |
| D | D | C | B | A |

Clearly $\mathbf{G}$ is a finite abelian group (of order 4) with identity element $\mathbf{A}$.

Also $\mathbf{B}^2 = \mathbf{A}, \mathbf{C}^2 = \mathbf{A}$ and $\mathbf{D}^2 = \mathbf{A}$

i.e. each element is of order 2 (except the identity $\mathbf{A}$)

$\therefore$ $\mathbf{G}$ is abelian.

Hence there is no element of order 4 in $\mathbf{G}$.

$\therefore$ $\mathbf{G}$ is not cyclic and hence every finite abelian group is not cyclic.

**Theorem 5.** ***If $a$ is a generator of a cyclic group $\mathbf{G}$, then $a^{-1}$ is also a generator of $\mathbf{G}$.***

***OR***

***If $\mathbf{G} = <a>$, then $\mathbf{G} = <a^{-1}>$.*** ***(A.N.U.M. 00, S99, S98, M96, O.U.A.99)***

**Proof.** Let $\mathbf{G} = <a>$ be a cyclic group generated by $a$. Let $a^r \in \mathbf{G}, r \in \mathbf{Z}$. We have $a^r = (a^{-1})^{-r}$ since $-r \in \mathbf{Z}$.

$\therefore$ Each element of $\mathbf{G}$ is generated by $a^{-1}$. Thus $a^{-1}$ is also a generator of $\mathbf{G}$ i.e. $\mathbf{G} = <a^{-1}>$.

**Theorem 6.** ***Every subgroup of cyclic group is cyclic.***
***(K. U. M12, 07, S.K.U. A 01, S.V.U. O 01, A 00, A.N.U. J 04, M 03, M 01, M 00, S98, M96, A92, O91, A90, O89, A.U.M. 05, M 00, S99, S98, S97, M97, A96, K.U.M. 05, M 04, M 03, O99, A98, O97, M96, O.U. M12, O 02, O 01)***

**Proof.** Let $\mathbf{G} = <a>$. Let $\mathbf{H}$ be a subgroup of $\mathbf{G}$. Since $\mathbf{H}$ is a subgroup of $\mathbf{G}$, we take that every element of $\mathbf{H}$ is an element of $\mathbf{G}$. Thus it can be expressed as $a^n$ for some $n \in \mathbf{Z}$. Let $d$ be the smallest of the positive integers such that $a^n \in \mathbf{H}$. We will now prove that $\mathbf{H} = <a^d>$.

Let $a^m \in \mathbf{H}$ where $m \in \mathbf{Z}$.

By division algorithm we can find integers $q$ and $r$ such that $m = dq + r$, $0 \le r < d$.

$\therefore$ $a^m = a^{dq+r} = a^{dq} a^r = (a^d)^q . a^r$

But $a^d \in \mathbf{H} \Rightarrow (a^d)^q \in \mathbf{H} \Rightarrow a^{dq} \Rightarrow a^{-dq} \in \mathbf{H}$

Now $a^m, a^{-dq} \in \mathbf{H} \Rightarrow a^m . a^{-dq} \in \mathbf{H} \Rightarrow a^{m-dq} \in \mathbf{H} \quad \Rightarrow a^r \in \mathbf{H}$.

But $0 < r < d$ and $a^r \in \mathbf{H}$ is a contradiction to our assumption that of smallest integer such that $a^d \in \mathbf{H}$. $\therefore \quad r = 0 \quad \therefore \quad m = dq$

i.e. $a^m = (a^d)^q$ which shows that every $a^n \in \mathbf{H}$ can be written as $(a^d)^q, q \in \mathbf{Z}$.

$\therefore \mathbf{H} = <a^d>$

Hence a subgroup $\mathbf{H}$ of $\mathbf{G}$ is cyclic and $a^d$ is a generator of $\mathbf{H}$.

**Note :** The converse of the above theorem is not true. ***(S.V.U. O 2001)***

That is though the subgroup of a group is cyclic, the group need not be cyclic.

**e.g.** We know that $(\mathbf{Z}, +)$ is a subgroup of $(\mathbf{R}, +)$. We also have that $(\mathbf{Z}, +)$ is a cyclic group generated by 1 and $-1$. But $(\mathbf{R}, +)$ is not a cyclic group since it has no generators.

**Cor.** Every subgroup of a cyclic group is a normal subgroup. ***(O.U. 93)***

**Proof.** Every cyclic group is abelian (vide Theorem 4) and every subgroup of a cyclic group is cyclic (vide Theorem 6).

$\therefore$ Every subgroup of a cyclic group is abelian. Hence every subgroup of a cyclic group is a normal subgroup.

## 8. 4. CLASSIFICATION OF CYCLIC GROUPS

Let $\mathbf{G} = <a>$. Then

(i) $\mathbf{G}$ is a finite cyclic group if there exist two unequal integers $l$ and $m$ such that $a^l = a^m$.

If a group $\mathbf{G}$ of order $n$ is cyclic, then $\mathbf{G}$ is a cyclic group of order $n$.

(ii) $\mathbf{G}$ is an infinite cyclic group if for every pair of unequal integers $l$ and $m$, $a^l \neq a^m$.

**Theorem 7.** ***The quotient group of a cyclic group is cyclic.*** ***(S.V.U. S 89, A.U.11)***

**Proof.** Let $\mathbf{G} = <a>$ be a cyclic group with $a$ as generator.

Let $\mathbf{N}$ be a subgroup of $\mathbf{G}$. Since $\mathbf{G}$ is abelian (Th.14, Art 5.4).

we take that $\mathbf{N}$ is normal in $\mathbf{G}$. We know that $\dfrac{\mathbf{G}}{\mathbf{N}} = \{\mathbf{N}x / x \in \mathbf{G}\}$

Now $a \in \mathbf{G} \Rightarrow \mathbf{N}a \in \mathbf{G/N} \Rightarrow <\mathbf{N}a> \subseteq \mathbf{G/N}$ …(1)

Also $\mathbf{N}x \in \mathbf{G/N} \Rightarrow x \in \mathbf{G} = <a> \quad \therefore x = a^n$ for some $n \in \mathbf{Z}$.

$\therefore \quad \mathbf{N}x = \mathbf{N}a = \mathbf{N}(a \ a \ a \ \ldots\ldots n \text{ times})$ when $n$ is a +ve integer

$= \mathbf{N}a\,\mathbf{N}a \ldots\ldots n \text{ times} = (\mathbf{N}a)^n$

We can prove that $\mathbf{N}x = (\mathbf{N}a)^n$ when $n = 0$ or a negative integer.

$\therefore \quad \mathbf{N}x \in \mathbf{G/N} \Rightarrow \mathbf{N}(x) \in <\mathbf{N}a>$

$\therefore \quad \mathbf{G/N} \subseteq <\mathbf{N}a>$ …(2)

$\therefore$ From (1) and (2) $\mathbf{G/N} = <\mathbf{N}a>$ which shows that $\mathbf{G/N}$ is cyclic.

**Theorem 8.** ***If $p$ is a prime number then every group of order $p$ is a cyclic group i.e. a group of prime order is cyclic.***

***(A.U. O 75, N.U. 92, A 93, 95, O.U. O 99, A.N.U. M 04, S96, A93, O92, O90, A89, O.U. M 06, O 01, O 00, O99, A.U. A 01, S00, M99, K.U.M. 08, 05, A 03, A 02, A 00, M99, O97, A.97, O96, S.K.U. M 05, O 01, O 00, A97, S.V.U. S 03, O98)***

**Proof.** Let $p \geq 2$ be a prime number and $\mathbf{G}$ be a group such that $\mathbf{O}(\mathbf{G}) \geq p$. Since

the number elements is at least 2, one of the elements of $\mathbf{G}$ will be different from the identity $e$ of $\mathbf{G}$. Let that element be $a$.

Let $<a>$ be the cyclic subgroup of $\mathbf{G}$ generated by $a$. $\therefore$ $a \in <a> \Rightarrow <a> \neq \{e\}$.

Let $<a>$ have order $h$, $\therefore$ By Langrange's Theorem $h \mid p$

But $p$ is a prime number. $\therefore$ $h = 1$ or $h = p$

But $<a> \neq \{e\}$. $\therefore$ $h \neq 1$ and hence $h = p$

$\therefore$ $\mathbf{O}(<a>) = p$ i.e. $<a> = \mathbf{G}$ which shows that $\mathbf{G}$ is a cyclic group.

**Note 1.** We have by the above theorem if $\mathbf{O}(\mathbf{G}) = p$, a prime number, then every element of $\mathbf{G}$ which is not an identity is a generator of $\mathbf{G}$. Thus the number of generators of $\mathbf{G}$ having $p$ elements is equal to $p - 1$.

**2.** Every group $\mathbf{G}$ of order less than 6 is abelian. For : We know that every group $\mathbf{G}$ of order less than or equal to 4 is abelian.

Also we know that every group of prime order is cyclic and every cyclic group is abelian. If $\mathbf{O}(\mathbf{G}) = 5$, then $\mathbf{G}$ is abelian. ***(S.V.U. A 01)***

Thus the smallest non-abelian group is of order 6.

**3.** Is the converse of the theorem "Every group of prime order is cyclic" true ? Not true.

For $4^{th}$ roots of unity w.r.t. multiplication form a cyclic group and 4 is not a prime number. Thus a cyclic group need not be of prime order.

## 8. 5. SOME MORE THEOREMS ON CYCLIC GROUPS

**Theorem 9.** ***If a finite group of order $n$ contains an element of order $n$, then the group is cyclic.*** ***(B.A.) (N.U. O 90)***

**Proof.** Let $\mathbf{G}$ be finite group of order $n$. Let $a \in \mathbf{G}$ such that $\mathbf{O}(a) = n$ i.e. $a^n = e$ where $n$ is the least positive integer.

If $\mathbf{H}$ is a cyclic subgroup of $\mathbf{G}$ generated by $a$ i.e. if $\mathbf{H} = \{a^r / r \in \mathbf{Z}\}$ then $\mathbf{O}(\mathbf{H}) = n$ because the order of the generator $a$ of $\mathbf{H}$ is $n$. Thus $\mathbf{H}$ is a cyclic subgroup of $\mathbf{G}$ and $\mathbf{O}(\mathbf{H}) = \mathbf{O}(\mathbf{G})$.

Hence $\mathbf{H} = \mathbf{G}$ and $\mathbf{G}$ itself is a cyclic group with $a$ as a generator.

**Note.** Suppose $\mathbf{G}$ is a finite group of order $n$ and we are to determine whether $\mathbf{G}$ is cyclic or not. For this we find the orders of the elements of $\mathbf{G}$ and if $a \in \mathbf{G}$ exists such that $\mathbf{O}(a) = n$ then $\mathbf{G}$ will be a cyclic group with $a$ as a generator.

**Theorem 10.** ***Every finite group of composite order possesses proper subgroups.***

**Proof.** Let $\mathbf{G}$ be a finite group of composite order $mn$ where $m (\neq 1)$ and $n (\neq 1)$ are positive integers.

(i) Let $\mathbf{G} = <a>$. Then $\mathbf{O}(a) = \mathbf{O}(\mathbf{G}) = mn$.

$\therefore$ $a^{mn} = e \Rightarrow (a^n)^m = e \Rightarrow \mathrm{O}(a^n)$ is finite and $\leq m$.

Let $\mathrm{O}(a^n) = p$ where $p < m$. Then $(a^n)^p = e \Rightarrow a^{np} = e$

But $p < m \Rightarrow np < mn$ Thus $a^{np} = e$ where $np < mn$.

Since $\mathbf{O}(a) = mn, a^{np} = e$ is not possible, so $p = m$

$\therefore$ **O** $(a^n) = m$ .

$\therefore$ **H** $= <a^n>$ is a cyclic subgroup of **G** and **O** (**H**) = **O** $(a^n)$ .

Thus **O** (**H**) = $m$ .

Since $2 \le m < n$, **H** is a proper cyclic subgroup of **G**.

(ii) Let **G** be not a cyclic group.

Then the order of each element of **G** must be less than $mn$. So there exists an element, say $b$ in **G** such that $2 \le$ **O** $(b) < mn$. Then **H** $= <b>$ is a proper subgroup of **G**.

**Theorem. 10 (*a*).** ***If G is a group of order pq where p,q are prime numbers, then every proper subgroup of G is cyclic.*** **(*K. U. 07*)**

**Proof.** Let **H** be a proper sub group of **G** where $|\mathbf{G}| = pq$ ($p$,$q$ are prime numbers).

By Lagrange's Theorem, $|\mathbf{H}|$ divides $|\mathbf{G}|$.

$\therefore$ Either $|\mathbf{H}| = 1$ or $p$ or $q$. $\therefore$ $|\mathbf{H}| = 1 \Rightarrow \mathbf{H} = \{e\}$ which is cyclic;

$|\mathbf{H}| = p$ ($p$ is prime) $\Rightarrow$ **H** is cyclic and $|\mathbf{H}| = q$ ($q$ is prime) $\Rightarrow$ **H** is cyclic.

$\therefore$ **H** is a proper subgroup of **G** which is cyclic. Hence every proper subgroup of **G** is cyclic.

**Theorem 11.** ***If a cyclic group G is generated by an element $a$ of order $n$, then $a^m$ is a generator of G iff the greatest common divisor of $m$ and $n$ is 1 i.e. iff $m, n$ are relatively prime i.e. (m,n) = 1.***

***(K. U. 08, A.N.U. M11, M97, S.V.U. M11, A.98, M 09, O.U. O 98)***

**Proof.** Let **G** $= <a>$ such that **O** $(a) = n$ i.e. $a^n = e$ .

The group **G** contains exactly $n$ elements.

(i) Let $m$ be relatively prime to $n$. Consider the cyclic subgroup

**H** $= <a^m>$ of **G**. Clearly **H** $\subseteq$ **G** ... (1)

since each integral power of $a^m$ will be some integral power of $a$.

Since $m, n$ are relatively prime, there exist two integers $x$ and $y$ such that $mx + ny = 1$ .

$\therefore$ $a = a^1 = a^{mx+ny} = a^{mx}.a^{ny} = a^{mx}.(a^n)^y = a^{mx}e^y = a^{mx}e = (a^m)^x$

$\therefore$ Each integral exponent of $a$ will also be some integral exponent of $a^m$ .

$\therefore$ **G** $\subseteq$ **H**

$\therefore$ From (1) and (2), **H** = **G** and $a^m$ is a generator of **G**.

(ii) Let **G** $= <a^m>$ . Let the greatest common divisor of $m$ and $n$ be $d$ ($\neq 1$) i.e. $d > 1$ . Then $m/d$, $n/d$ just be integers.

Now $(a^m)^{n/d} = a^{mn/d} = (a^n)^{m/d} = e^{m/d} = e$ $\therefore$ **O** $(a^m) < n$ $\left(\because \frac{n}{d} < n\right)$

$\therefore$ $a^m$ cannot be a generator of **G** because the order of $a^m$ is not equal to the order of **G**. So $d$ must be equal to 1. Thus $m$ and $n$ are relatively prime.

**Note 1.** If **G** $= <a>$ is a cyclic group of order $n$, then the total number of generators of **G** will be equal to the number of integers less than and prime to $n$.

**2.** $\mathbf{Z}_8$ is a cyclic group with 1, 3, 5, 7 as generators.

Note that $<3> = \{3, (3+3) \bmod 8, (3+3+3) \bmod 8, .....\} = \{3,6,1,4,7,2,5,0\} = \mathbf{Z_8}$

$<2> = \{0,2,4,6\} \neq \mathbf{Z_8}$ implies 3 is a generator and 2 is not a generator of $\mathbf{Z_8}$.

**Theorem 12.** ***If*** $\mathbf{G}$ ***is a finite cyclic group of order*** $n$ ***generated by*** $a$***, then the subgroups of*** $\mathbf{G}$ ***are precisely the subgroups generated by*** $a^m$ ***where*** $m$ ***divides*** $n$**.**

**Proof.** Since $\mathbf{G}$ is a finite cyclic group of order $n$ generated by $a$, then $a^m$ generates a cyclic subgroup, say $\mathbf{H}$ of $\mathbf{G}$.

Since $\mathbf{O}(\mathbf{G}) = n, a^n = e$ where $e$ is the identity in $\mathbf{G}$.

Since $\mathbf{H}$ is a subgroup of $\mathbf{G}, e \in \mathbf{H}$ i.e. $a^n \in \mathbf{H}$.

If $m$ is the least positive integer such that $a^m \in \mathbf{H}$ then by division algorithm, there exist positive integers $q$ and $r$ such that $n = mq + r$, $0 \le r < m$.

$\therefore \quad a^n = a^{mq+r} = a^{mq}.a^r = (a^m)^q.a^r$

But $a^m \in \mathbf{H}$. $\qquad \therefore \quad (a^m)^q \in \mathbf{H} \Rightarrow a^{mq} \in \mathbf{H} \Rightarrow a^{-mq} \in \mathbf{H}$.

Now $a^n \in \mathbf{H} \Rightarrow a^{-mq} \in \mathbf{H} \Rightarrow a^{n-mq} \in \mathbf{H} \Rightarrow a^r \in \mathbf{H}$.

But $0 < r < m$ and $a^r \in \mathbf{H}$ is a contradiction to our assumption that $m$ is the smallest positive integer such that $a^m \in \mathbf{H}$. $\qquad \therefore \quad r = 0$

$\therefore \quad n = mq$ i.e. $m$ divides $n$ and $a^n = a^{mq} = (a^m)^q \in \mathbf{H}$ which means that $a^m$ generates the cyclic subgroup $\mathbf{H}$ of $\mathbf{G}$.

**Ex. 10.** ***Find all orders of subgroups of*** $\mathbf{Z}_6, \mathbf{Z}_8, \mathbf{Z}_{12}, \mathbf{Z}_{60}$**.**

**Sol.** $(\mathbf{Z}_6, +_6)$ is a cyclic group and its subgroups have orders 1, 2, 3, 6(Theorem. 12)

(Proper subgroup of order 2 is $(\{0,3\}, +_6)$, Proper subgroup of order 3 is $(\{0,2,4\}, +_6)$)

$(\mathbf{Z}_8, +_8)$ is a cyclic group and its subgroups have orders 1, 2, 4, 8.

$(\mathbf{Z}_{12}, +_{12})$ is a cyclic group and its subgroups have orders 1, 2, 3, 4, 6,12.

$(\mathbf{Z}_{60}, +_{60})$ is a cyclic group and its subgroups have orders 1,2,3,4,5,6,10,12,15,20,30,60.

**Ex. 11.** *Write down all the subgroups of a finite cyclic group G of order 18, the cyclic group being generated by* $a$.

**Sol.** Let $e$ be the identity in $\mathbf{G} = < a >$.

Now $\mathbf{G}, \{e\}$ are the trivial subgroups of $\mathbf{G}$ and generated by $a$ and $a^{18} = e$ respectively.

The other proper subgroups are precisely the subgroups generated by $a^m$ where $m$ divides 18. Such $m$'s are 2, 3, 6, 9. These subgroups are

$$< a^2 > = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18} = e\}, < a^3 > = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18} = e\},$$

$$< a^6 > = \{a^6, a^{12}, a^{18} = e\}, < a^9 > = \{a^9, a^{18} = e\}.$$

**Theorem 13.** ***The order of a cyclic group is equal to the order of its generator.***
***(A.N.U.M 02, S 01, S.K.U.M 01, S.V.U.M 05, O97)***

**Proof.** Let $\mathbf{G}$ be a cyclic group generated by $a$ i.e. $\mathbf{G} = < a >$

(i) Let $\mathbf{O}(a) = n$, $a$ a finite integer.

Then $e = a^0, a^1, a^2, \ldots\ldots, a^{n-1} \in \mathbf{G}$

Now we prove that these elements are distinct and these are the only elements of $\mathbf{G}$ such that $\mathbf{O}(\mathbf{G}) = n$.

Let $i, j$ $(\le n-1)$ be two non-negative integers such that $a^i = a^j$ for $i \ne j$.

Now either $i > j$ or $i < j$.

Suppose $i > j$. Then $a^{i-j} = a^{j-j} \Rightarrow a^{i-j} = a^0 = e$ and $0 < i - j < n$.

But this contradicts the fact that $\mathbf{O}(a) = n$. Hence $i = j$.

$\therefore$ $a^0, a^1, a^2, \ldots\ldots, a^{n-1}$ are all distinct.

Consider any $a^p \in \mathbf{G}$ where $p$ is any integer. By Euclid's Algorithm we can write $p = nq + r$ for some integers $q$ and $r$ such that $0 \le r < n$.

Then $a^p = a^{nq+r} = (a^n)^q . a^r = e^q . a^r = e . a^r = a^r$

But $a^r$ is one of $a^0, a^1, \ldots\ldots, a^{n-1}$

Hence each $a^p \in \mathbf{G}$ is equal to one of the elements $a^0, a^1, \ldots\ldots, a^{n-1}$

i.e. $\mathbf{O}(\mathbf{G}) = n = o(a)$.

(ii) Let $\mathbf{O}(a)$ be infinite. Let $m, n$ be two positive integers such that $a^m = a^n$ for $n \ne m$.

Suppose $m > n$. Then $a^{m-n} = a^0 = e \Rightarrow \mathbf{O}(a)$ is finite.

It is a contradiction to the fact that $\mathbf{O}(a)$ is infinite.

$\therefore$ $n = m$ i.e. for every pair of unequal integers $m$ and $n$, $a^m \ne a^n$

Hence $\mathbf{G}$ is of infinite order.

Thus from (i) and (ii), the order of a cyclic group is equal to the order of its generator.

**Note.** Thus : Let $(\mathbf{G}, \cdot)$ be a group and $a \in \mathbf{G}$.

If $a$ has finite order, say, $n$, then $< a > = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if $n$ divides $i - j$.

If $a$ has infinite order, then all distinct powers of $a$ are distinct group elements.

**Theorem. 14.** ***If $\mathbf{G}$ is a cyclic group of order $n$, then there is a one - one correspondence between the subgroups of $\mathbf{G}$ and positive divisors of $n$.***

**Proof.** Let $\mathbf{G} = < a >$ be a finite cyclic group of order $n$.

$\therefore$ $\mathbf{O}(a) = n$, $a$ +ve integer. If $d$ ($a$ +ve integer) is a divisor of $n$, $\exists$ $a$ +ve integer $m$ such that $n = dm$.

Now $\mathbf{O}(a) = n \Rightarrow a^n = e \Rightarrow a^{dm} = e \Rightarrow (a^m)^d = e \Rightarrow \mathbf{O}(a^m) \le d$

Let $\mathbf{O}(a^m) = s$ where $s < d$.

Then $(a^m)^s = e \Rightarrow a^{ms} = e$ where $ms < md$ i.e. $ms < n$.

Since $\mathbf{O}(a) = n$, when $ms < n$, $a^{ms} = e$ is absurd.

$\therefore s \not< d$ i.e. $s = d$.

$\therefore a^m \in \mathbf{G}$ where $\mathbf{O}(a^m) = d$. Thus $< a^m >$ is a cyclic subgroup of order $d$.

Now we show that $< a^m >$ is a unique cyclic subgroup of $\mathbf{G}$ of order $d$.

We know that every subgroup of a cyclic group is cyclic. If possible suppose that there is another subgroup $< a^k >$ of $\mathbf{G}$ of order $d$ where $n = dm$.

We shall have to show that $< a^k > = < a^m >$.

By division algorithm $\exists$ integers $q$ and $r$ such that

$$k = mq + r \text{ where } 0 \le r < m \qquad \ldots(1)$$

$\therefore$ $$kd = mqd + rd \text{ where } 0 \le rd < md$$

Now $a^{kd} = a^{mqd+rd} = a^{mqd}.a^{rd} = (a^{md})^q.a^{rd} = (a^n)^q.a^{rd} = e^q.a^{rd} = e.a^{rd}$

$\Rightarrow \quad a^{kd} = a^{rd}$ …(2)

Since $<a^k>$ is of order $d$, $\mathbf{O}(a^k) = d \Rightarrow (a^k)^d = e \Rightarrow a^{kd} = e$.

$\Rightarrow a^{rd} = e$ from (2) which is impossible $(\because \quad rd < md \Rightarrow rd < m)$ unless $r = 0$.

$\therefore$ From (1), $k = mq \Rightarrow a^k = a^{mq} = (a^m)^q \Rightarrow a^k \in <a^m> \Rightarrow <a> \subseteq <a^m>$

But number of elements in $<a^k>$ = number of elements in $<a^m>$.

$\therefore <a^k> = <a^m>$

$\therefore$ If $\mathbf{G}$ is a finite cyclic group of order $n$, there corresponds a unique subgroup of $\mathbf{G}$ of order $d$ for every divisor $d$ of $n$ i.e. there is a $1-1$ correspondence between the subgroups of $\mathbf{G}$ and positive divisors of $n$.

[$\because$ a one-one onto mapping is always possible to be defined between the set of subgroups of order $d$ (any +ve divisor of $n$) and the set of +ve divisors of $n$]

**Theorem 15.** ***Every isomorphic image of a cyclic group is again cyclic.*** ***(S.V.U. A 93)***

**Proof.** Let $\mathbf{G}$ be a cyclic group generated by $a$ so that $a^n \in \mathbf{G}$ from $n \in \mathbf{Z}$.

Let $\mathbf{G}'$ be its isomorphic image under an isomorphism $f$.

Now $a^n \in \mathbf{G} \Rightarrow f(a^n) \in \mathbf{G}'$

$\therefore \quad f(a^n) = f(a.a.a.\ldots\ldots, n \text{ times})$ when $n$ is a +ve integer

$= f(a).f(a)\ldots\ldots, n \text{ times} = [f(a)]^n$

We can prove that $f(a^n) = [f(a)]^n$ when $n = 0$ or $a$ – ve integer

Hence every element $f(a^n) \in \mathbf{G}'$ can be expressed as $[f(a)]^n$

$\therefore$ $f(a)$ is a generator of $\mathbf{G}'$ implying that $\mathbf{G}'$ is cyclic.

**Theorem. 16.** ***Let a be a generator of a cyclic group*** $(\mathbf{G},\cdot)$ ***of order n. Then*** $a^m$ ***generates of a cyclic sub-group of*** $(\mathbf{H},\cdot)$ ***of*** $(\mathbf{G},\cdot)$ ***and*** $\mathbf{O}(\mathbf{H}) = n/d$ ***where d is the H.C.F. of n and m.***

**Proof.** $a^m$ generates a cyclic subgroup $(\mathbf{H},\cdot)$ of $(\mathbf{G},\cdot)$ (vide Theorem of Art. 8.1)

Let $p$ be the smallest positive integer such that $(a^m)^p = e$ where $e$ is the identity in $\mathbf{H}$.

Let $a^m = b$. Let $b^k \in \mathbf{H}; k > p$.

Now there exist integers $q$ and $r$ such that $k = pq + r, 0 \le r < p$.

$\therefore \quad b^k = b^{pq+r} = b^{pq}.b^r = (b^p)^q.b^r = e^q.b^r = b^r$ for $0 \le r < p$.

$\therefore$ Any exponent $k$ of $b$, greater than or equal to $p$, is reducible to $r$ for $0 \le r < p$.

$\therefore$ $\mathbf{H}$ contains $p$ elements given by

$\mathbf{H} = \{b, b^2, \ldots, b^{p-1}, b^p = e\}$ i.e. $\mathbf{H} = \{(a^m)^1, (a^m)^2, \ldots, (a^m)^p = e\}$

$\therefore$ $\mathbf{H}$ has $p$ elements, as many elements as the smallest power of $a^m$ which gives the identity $e$. Now $a^{pm} = e$ if and only if $n$ divides $pm$ since $a^n = e$, $(\mathbf{G},\cdot)$ be a cyclic group of order $n$.

$\therefore$ $pm/n$ must be an integer.

Let $d$ be the H. C. F of $n$ and $m$. Now $\frac{pm}{n} = p \cdot \frac{m/d}{n/d}$.

But $n/d$ does not divide $m/d$.

$\therefore$ $n/d$ divides $p$. $\therefore$ Least value of $p$ is $n/d$. $\therefore$ $\mathbf{O}(\mathbf{H}) = n/d$.

**e.g.** Let $|\mathbf{G}| = 24$ and $\mathbf{G}$ be cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\mathbf{G} = <a>$

Divisors of 24 are 1,2,3,4,6,8,12, 24. If $|a| = 2$, then $a^2 = e$ and $a^4 = (a^2)^2 = e^2 = e = a^8$.

Also if $|a| = 3$, then $a^3 = e$ and $a^{12} = (a^3)^4 = e^4 = e = a^6$.

$\therefore |a| = 24$ is only acceptable and hence $\mathbf{G} = <a>$.

**Theorem 17.** ***A cyclic group of order $n$ has $\phi(n)$ generators.***
***(S.V.U. A 01,O.U.O 03, A 02, O 02, N.U. O 85, O 83, A 93, M 01)***

**Proof.** First we prove Theorem 11.

$\therefore$ $\mathbf{G} = <a^m> \Leftrightarrow (m, n) = 1$

$\therefore$ $a^m$ is a generator of $\mathbf{G} \Leftrightarrow m$ is a positive integer less than $n$ and relatively prime to $n$.

$\Rightarrow$ The number of generators of $\mathbf{G}$ = the number of positive integers that are less than $n$ and relatively prime to $n = \phi(n)$.

**Note.** For $n = 1, \phi(1) = 1$ and for $n > 1$ the number of generators $\phi(n)$ is the number of positive integers less than $n$ and relatively prime to $n$.

**e.g.** $a$ is a generator of a cyclic group $\mathbf{G}$ of order 8. Then $\mathbf{G} = <a>$ and $\mathbf{O}(a) = 8$.

Here $\mathbf{G} = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$

Since 3, 5, 7 are relatively prime to 8 and each is less than 8, $a^3, a^5, a^7$ are the only other generators of $\mathbf{G}$. Also $a^2, a^4, a^6, a^8$ cannot be the generators of $\mathbf{G}$. Hence $\mathbf{G}$ has only 4 generators and they are $a^1, a^3, a^5, a^7$.

Now $<a^3> = \{a^3, a^6, a^1, a^4, a^7, a^2, a^5, a^8\}$, etc.

**Ex. 12.** *Show that the group $(\mathbf{G} = \{1, 2, 3, 4, 5, 6\}, \times_7)$ is cyclic. Also write down all its generators.* ***(A.N.U. M99, A.U.M 05, K.U.S 01, O99, O.U.O. 02, S.K.U. M11, O 03, S.V.U.M 03, O. U. 91)***

**Sol.** Clearly $\mathbf{O}(\mathbf{G}) = 6$. If there exists an element $a \in \mathbf{G}$ such that $\mathbf{O}(a) = 6$, then $\mathbf{G}$ will be a cyclic group with generator $a$.

Since $3^1 = 3$, $3^2 = 3 \times_7 3 = 2$, $3^3 = 3^2 \times_7 3 = 6$, $3^4 = 3^3 \times_7 3 = 4$,

$3^5 = 3^4 \times_7 3 = 5$, $3^6 = 3^5 \times_7 3 = 1$, the identity element.

$\therefore$ $\mathbf{G} = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ and is cyclic with 3 as a generator.

Since 5 is relatively prime to 6, $3^5$ i.e. 5 is also a generator of $\mathbf{G}$.

$\therefore$ Generators of $\mathbf{G}$ are 3, 5.

**Note.** If $(\mathbf{G}, .)$ is a cyclic group of order $n$, then the number of generators of $\mathbf{G} = \phi(n)$ = the number of numbers less than $n$ and prime to $n$.

From theory of numbers, if $n = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$ where $p_1 \ldots\ldots p_k$ are all prime factors of $n$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_k}\right)$

In Ex. 12, $\phi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2$ *i.e.* G has 2 generators.

Further if $n = p^{\alpha}$ where $p$ is less than and prime to $n$, then $\phi(n) = p^{\alpha}\left(1-\frac{1}{p}\right)$

**Ex. 13.** *Find all the subgroups of* $(\mathbf{Z}_{18}, +_{18})$.

**Sol.** $(\mathbf{Z}_{18}, +_{18})$ is a cyclic group with 1 as its generator.

$\mathbf{Z}_{18} = \{0,1,2,3,.....,17\}$ and all subgroups are cyclic.

Now all the generators of the group $\mathbf{Z}_{18}$ are less than 18 and are prime to 18.

Thus 1, 3, 5, 7, 11, 13 and 17 are all generators of $\mathbf{Z}_{18}$.

All the subgroups of $\mathbf{Z}_{18}$ are the subgroups generated by 1,2,3,6,9,18 (Divisors of 18).

The number that corresponds 18 is 0.

The subgroups are :

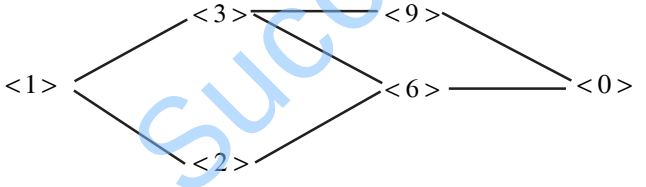
Trivial (improper) subgroups - $(\mathbf{Z}_{18}, +_{18}) = <1>, (\{0\}, +_{18}) = <0>$.

Proper subgroups $(\{0,2,4,6,8,10,12,14,16\}, +_{18}) = <2>$,

$(\{0,3,6,9,12,15\}, +_{18}) = <3>$, $(\{0,6,12\}, +_{18}) = <6>$, $(\{0,9\}, +_{18}) = <9>$.

**Note. 1.** $\mathbf{O}(<1>) = 18, \mathbf{O}(<0>) = 1, \mathbf{O}(<2>) = 9, \mathbf{O}(<3>) = 6, \mathbf{O}(<6>) = 3, \mathbf{O}(<9>) = 2$.

**2.** *Lattice diagram* for $(\mathbf{Z}_{18}, +_{18})$.




**Ex. 14.** *Find the number of elements in the cyclic subgroup of* $(\mathbf{Z}_{30}, +_{30})$ *generated by 25 and hence write the subgroup* ***(O. U. 2008)***

**Sol.** $(\mathbf{Z}_{30}, +_{30})$ is a cyclic group. Clearly 1 is a generator of $(\mathbf{Z}_{30}, +_{30})$.

Now $25 \in \mathbf{Z}_{30}$ and $25 = 1^{25} = (25)(1)$. Clearly $(1^{25}, +_{30})$ is a subgroup of $(\mathbf{Z}_{30}, +_{30})$.

The g.c.d. of 30 and 25 is 5.

$\therefore$ $25 = 1^{25}$ generates a cyclic subgroup of order $(30/5) = 6$

*i.e.* $(\{0,5,10,15,20,25\}, +_{30})$ is the cyclic subgroup generated by 25.

**Ex. 15.** *Find the no. of elements in the cyclic subgroup of* $(\mathbf{Z}_{42}, +_{42})$ *generated by 30 and hence write the subgroup.*

**Sol.** $(\mathbf{Z}_{42}, +_{42})$ is a cyclic group. Clearly 1 is a generator of $(\mathbf{Z}_{42}, +_{42})$.

Now $30 \in \mathbf{Z}_{42}$ and $30 = 1^{30} = (30)(1)$. Clearly $(1^{30}, +_{42})$ is a subgroup of $(\mathbf{Z}_{42}, +_{42})$.

The g.c.d. of 30 and 42 is 6.

$\therefore$ $30 = 1^{30}$ generates a cyclic subgroup of order $(42/6) = 7$

*i.e.* $(\{0,6,12,18,24,30,36\}, +_{42})$ is the cyclic subgroup generated by 30.

**Ex. 16.** *Find the order of the cyclic subgroup of* $(\mathbf{Z}_{60}, +_{60})$ *generated by 30.*

**Sol.** $(\mathbf{Z}_{60}, +_{60})$ is a cyclic group and 1 is a generator of it.

Now $30 \in \mathbf{Z}_{60}$ and $30 = 1^{30} = 30\,(1)$ .

Clearly $(1^{30}, +_{60})$ *i.e.* $(30, +_{60})$ is a subgroup of $(\mathbf{Z}_{60}, +_{60})$ .
The g.c.d. of 60 and 30 is 30.

$\therefore$ $30 = 1^{30}$ generates a cyclic subgroup of order $(60/30) = 2$ .

**Ex. 17.** *Find the number of generators of cyclic groups of orders* 5,6,8,12,15,60.

**Sol.** $\mathbf{O}(\mathbf{G}) = 5$, the number of generators of $\mathbf{G} = \phi(5) = 5\left(1 - \frac{1}{5}\right) = 4$

$\mathbf{O}(\mathbf{G}) = 6$, the number of generators of $G = \phi(6)$
$= 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 2$ ($\because$ 2, 3 are prime factors of 6)

$\mathbf{O}(\mathbf{G}) = 8$, the number of generators of $\mathbf{G}$
$= \phi(8) = 8\left(1 - \frac{1}{2}\right) = 4$ ($\because$ 2 is the only prime factor of 8)

$\mathbf{O}(\mathbf{G}) = 12$, the number of generators of $\mathbf{G}$
$= \phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$ ($\because$ 2, 3 are the only prime factors of 12)

$\mathbf{O}(\mathbf{G}) = 15$, the number of generators of $\mathbf{G} = \phi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$.
($\because$ 3, 5 are the only prime factors of 15.)

$\mathbf{O}(\mathbf{G}) = 60$, the number of generators of $\mathbf{G} = \phi(60) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16$.

($\because$ $60 = 2^2.3.5$; 2, 3, 5 are the only prime factors of 60)

**Ex. 18.** Show that $(\mathbf{Z}_p, +_p)$ has no proper subgroups if $p$ is prime.

**Sol.** $(\mathbf{Z}_p, +_p)$ is a cyclic group and $\mathbf{O}(\mathbf{Z}_p) = p$ where $p$ is prime.

$\therefore$ Number of generators of $(\mathbf{Z}_p, +_p) = p\left(1 - \frac{1}{p}\right)$

$\therefore$ All the $p - 1$ elements of $\mathbf{Z}_p$ except the identity element, generate the group $(\mathbf{Z}_p, +_p)$. But this is a trivial subgroup. So $(\mathbf{Z}_p, +_p)$ has no proper subgroups.

**Ex. 19.** *Find all orders of subgroups of the group* $\mathbf{Z}_{17}$. ***(K. U. 07)***

**Sol.** $(\mathbf{Z}_{17}, +_{17})$ is a cyclic group and $\mathbf{O}(\mathbf{Z}_{17}) = 17$ (17 is prime)

$\therefore$ The no. of generators of $(\mathbf{Z}_{17}, +_{17}) = 17\left(1-\frac{1}{17}\right) = 16$

The 16 elements of $\mathbf{Z}_{17}$ except identity element 0 (which corresponds to 17), generate the group $(\mathbf{Z}_{17}, +_{17})$ which is of course a trivial subgroup.

Hence $(\mathbf{Z}_{17}, +_{17})$ has no proper subgroups.

Also $\{0\}$ is a trivial subgroup. Now $\mathbf{O}(\mathbf{Z}_{17}) = 17, \mathbf{O}(\{0\}) = 1$.

**Ex. 20.** *(i) If p, q be prime numbers, find the number of generators of the cyclic group* $(\mathbf{Z}_{pq}, +_{pq})$.

**Sol.** The number of generatros of $(\mathbf{Z}_{pq}, +_{pq})$

$$= \phi(pq) = pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) \qquad (\because p, q \text{ are prime})$$

*(ii) If p be a prime number, find the number of generators of the cyclic group* $(\mathbf{Z}_{p^r}, +_{p^r})$ *where r is an integer* $\geq 1$.

**Sol.** The number of generators $= \phi(p^r) = p^r\left(1-\frac{1}{p}\right) = p^{r-1}(p-1)$.

**Ex. 21.** *G is a group. If a is the only element in G such that* $|<a>| = 2$, *then show that for every* $x \in \mathbf{G}, a\,x = x\,a$.

**Sol.** $a$ is the only element in group $\mathbf{G}$ such that $|<a>| = 2$.

Let $e$ be the identity in $\mathbf{G}$. $\therefore\ a^2 = e$.

Also whenever $b \in \mathbf{G} \Rightarrow b^2 = e$, we have $b = a$.

Now for $x \in \mathbf{G}, x\,a\,x^{-1} \in \mathbf{G}$.

$\therefore$ In G, $(x\,a\,x^{-1})^2 = (x\,a\,x^{-1})(x\,a\,x^{-1}) = x\,a\,(x^{-1}x)\,a\,x^{-1} = x\,a\,e\,a\,x^{-1}$

$$= x\,a\,a\,x^{-1} = x\,a^2\,x^{-1} = x\,e\,x^{-1} = x\,x^{-1} = e.$$

$\therefore\ x\,a\,x^{-1} = a \Rightarrow x\,a\,x^{-1}x = a\,x \Rightarrow x\,a\,e = a\,x \Rightarrow x\,a = a\,x$.

**Ex. 22.** *Find all cosets of the subgroup* $<4>$ *of* $\mathbf{Z}_{12}$. ***(K. U. M 08)***

**Sol.** $(\mathbf{Z}_{12} = \{0,1,2,.....,11\}, +_{12})$ is a cyclic group.

Let the subgroup $<4>$ of $\mathbf{Z}_{12}$ be $\mathbf{H}$.

Since $<4> = \{.....,-12,-8,-4,0,4,8,12,....\}$, $(\mathbf{H} = \{0,4,8\}, +_{12})$ is the subgroup of $(\mathbf{Z}_{12}, +_{12})$ for which all left cosets have to be found out.

Composition Table :

| $+_{12}$ | 0 | 4 | 8 |
|---|---|---|---|
| 0 | 0 | 4 | 8 |
| 4 | 4 | 8 | 0 |
| 8 | 8 | 0 | 4 |

$0 +_{12} \mathbf{H} = \{0,4,8\}, 1 +_{12} \mathbf{H} = \{1,5,9\}$

$2 +_{12} \mathbf{H} = \{2,6,10\}, 3 +_{12} \mathbf{H} = \{3,7,11\}$

$4 +_{12} \mathbf{H} = \{4,8,0\}, 5 +_{12} \mathbf{H} = \{5,9,1\}$

$6 +_{12} \mathbf{H} = \{6,10,2\}, 7 +_{12} \mathbf{H} = \{7,11,3\}$

.....

$11 +_{12} \mathbf{H} = \{11,3,7\}$

$\therefore \quad 0 +_{12} \mathbf{H} = 4 +_{12} \mathbf{H} = ..... = \{0,4,8\};$

$1 +_{12} \mathbf{H} = 5 +_{12} \mathbf{H} = ..... = \{1,5,9\};$

$2 +_{12} \mathbf{H} = 6 +_{12} \mathbf{H} = ..... = \{2,6,10\};$

$3 +_{12} \mathbf{H} = 7 +_{12} \mathbf{H} = ..... = \{3,7,11\}.$

Since $(\mathbf{Z}_{12}, +_{12})$ is abelian, left cosets of H are also right cosets of H.

In $\mathbf{Z}_{12}$ cosets of $\mathbf{H}$ are $0 +_{12} \mathbf{H}, 1 +_{12} \mathbf{H}, ....., 11 +_{12} \mathbf{H}$ or $\mathbf{H} +_{12} 0, \mathbf{H} +_{12} 1, ...., \mathbf{H} +_{12} 11$.

Also $0 +_{12} \mathbf{H} = \mathbf{H}, 1 +_{12} \mathbf{H}, 2 +_{12} \mathbf{H}, 3 +_{12} \mathbf{H}$ are disjoint.

**Ex. 23.** *Find all cosets of the subgroup <18> of* $\mathbf{Z}_{36}$ ***(K. U. 07)***

**Sol.** $(\mathbf{Z}_{36} = \{0,1,2,3,.....,35\}, +_{36})$ is a finite cyclic abelian group.

The subgroup $<18>$ of $\mathbf{Z}_{36}$ is cyclic and let it be denoted by **H.** $\therefore \mathbf{H} = \{0,18\}$.

Here + means $+_{36}$.

$\therefore$ Left cosets of **H** in $\mathbf{Z}_{36}$ are

| | |
|---|---|
| $0 + \mathbf{H} = \{0,18\}$ | $18 + \mathbf{H} = \{18,0\}$ |
| $1 + \mathbf{H} = \{1,19\}$ | $19 + \mathbf{H} = \{19,1\}$ |
| $2 + \mathbf{H} = \{2,20\}$ | $20 + \mathbf{H} = \{20,2\}$ |
| ..... | .... |
| ..... | .... |
| $17 + \mathbf{H} = \{17,35\}$ | $35 + \mathbf{H} = \{35,17\}$ |

$\therefore$ Distinct left cosets of H in $\mathbf{Z}_{36}$ are $0 + \mathbf{H}, 1 + \mathbf{H}, ...., 17 + \mathbf{H}$ and their number is 18.

Since $\mathbf{G} = (\mathbf{Z}_{36}, +_{36})$ is abelian,

left coset of **H** in **G** = right coset of **H** in **G**.

Cosets of <18> of $\mathbf{Z}_{36}$ are $0 + \mathbf{H}, 1 + \mathbf{H}, ...., 17 + \mathbf{H}$ or $\mathbf{H} + 0, \mathbf{H} + 1, ...., \mathbf{H} + 17$.

**Ex. 24.** *$S_5$ is the set of all permutations on 5 symbols is a group. Find the index of the cyclic subgroup generated by the permutation (1 2 4) in $S_5$*

**Sol.** Let $f = (1\ 2\ 4)$. $\therefore f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

$\therefore f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$ and

$$f^3 = f^2 f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathbf{I}$$

$\therefore |< f >| = 3$ and $|S_5| = 5! = 120$.

$\therefore$ Index of the cyclic subgroup $f$ in $S_5 = \dfrac{|S_5|}{|< f >|} = \dfrac{120}{3} = 40$

**Ex. 25.** *If* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ *are two permutations defined on* $\mathbf{A} = \{1,2,3,4\}$, *find the cyclic groups generated by* $\sigma, \tau$.

**Sol.** If $n$ is a least positive integer such that $f^n = e$ where $f$ is a permutation on A, then $< f > = \{ \mathrm{I}, f, f^2, ....., f^{n-1} \}$

Now $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{I} \Rightarrow < \sigma > = \{ \mathrm{I}, \sigma \}$.

Also $\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$,

$\tau^3 = \tau^2 \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$,

$\tau^4 = \tau^3 \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{I}$

$\Rightarrow < \tau > = \{ \mathrm{I}, \tau, \tau^2, \tau^3 \}$.

**Ex. 26.** *If* $f : \mathbf{G} \to \mathbf{G}'$ *is isomorphic then the order of an element in G is equal to the order of its image in* $\mathbf{G}'$.

**Sol.** Since $f$ is one - one onto mapping, corresponding to any element $a' \in \mathbf{G}'$ there exists an element $a \in \mathbf{G}$ such that $f(a) = a'$. If $e$ is the identity in $\mathbf{G}$ and $e'$ is the identity in $\mathbf{G}'$ we have $f(e) = e'$.

Let $n$ be the order of $a \in$ G so that $a^n = e$ where $n$ is the least positive integer.

We have to show that the order of the image $f(a)$ of $a$ is also $n$.

Now $a^n = e \Rightarrow f(a^n) = f(e) = e'$

$\Rightarrow f(a \,.\, a \,.\, a ..... n \text{ times}) = e' \Rightarrow f(a) \,.\, f(a) \,.\, f(a) ..... \text{ to } n \text{ times} = e'$

$\Rightarrow [f(a)]^n = e' \Rightarrow$ the order of $f(a) \le n$.

Let us suppose that $m$ is the order of $f(a)$ where $m < n$

so that $[f(a)]^m = e' = f(e)$

*i.e.* $f(a) \,.\, f(a) \,.\, f(a) .... m \text{ times} = f(e)$

*i.e.* $f(a.a.a....m \text{ times}) = f(e)$ *i.e.* $f(a^m) = f(e) \Rightarrow a^m = e$

Since $m$ is less than $n$, $a^m = e$ is a contradiction.

Hence there cannot be any other integer $m$ less than $n$ such that $a^m = e$.

$\therefore$ $m = n \Rightarrow$ Order of $f(a) =$ Order of $a$

$\Rightarrow$ Order of the image of an element = order of that element.

**Theorem 18.** ***If G is an infinite cyclic group, then G has exactly two generators which are inverses of each other.*** ***(A.N.U. M12, S 02, S 91, S 00, A91, O.U.O 03, S.K.U. M 09, M 07, M 03, O 01, S.V.U.A.99)***

**Proof.** Let **G** be an infinite cyclic group generated by $a$.

$\therefore$ $\mathbf{G} = \{a^n / n \in \mathbf{Z}\}$. Let $a^m$ be a generator of **G**.

Since $a \in \mathbf{G}, \exists$ an integer $p$ such that $a = (a^m)^p$.

i.e. $a^{mp} = a$ i.e. $a^{mp}a^{-1} = a.a^{-1}$ i.e. $a^{mp-1} = e$

If $mp - 1 > 0$ then $\exists q = mp - 1$ such that $a^q = e$ implying that **G** is finite.

But **G** is infinite. $\therefore$ $mp - 1 = 0$

i.e. $mp = 1$ i.e. $m = \pm 1, p = \pm 1$ $\therefore$ $a^1, a^{-1}$ are generators of **G**.

i.e. **G** has exactly two generators and one is the inverse of the other in **G**.

**Note.** $(\mathbf{Z}, +)$ is an infinite cyclic group and it has only two generators 1 and $-1$.

**Theorem 19.** ***Any infinite cyclic group is isomorphic to the additive group of integers (Z, +).*** ***(S. K. U. M11, A.U.M.74, N.U.O.90, A92, S.V.U.O.99)***

**Proof :** Let **G** be an infinite cyclic group generated by an elemnt **a**$(\in \mathbf{G})$

Thus $0(a) = 0$ or $\infty$ and $a^0 = e$ (identity in **G**)

$\therefore$ $\mathbf{G} = \{a^n / n \in \mathbf{Z}\}$ and all the elements of **G** are distinct.

Define a mapping $f : \mathbf{G} \to \mathbf{Z}$ such that $f(a^n) = n, \forall a^n \in \mathbf{G}$

Let $a^i, a^j \in \mathbf{G}$. Let $(\mathbf{Z}, +)$ be the additive group of integers.

Now $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j$

$\therefore$ $f$ is $1 - 1$.

Let $k \in \mathbf{Z}$. $\therefore$ $a^k \in \mathbf{G}$ and $f(a^k) = k$ $\therefore$ $f$ is onto.

Further $a^i, a^j \in \mathbf{G}$ and $f(a^i a^j) = f(a^{i+j)} = i + j = f(a^i) + f(a^j)$

$\therefore$ $f$ is a homomorphism and hence $f$ is an isomorphism from **G** to **Z**.

$\therefore$ $\mathbf{G} \cong \mathbf{Z}$.

**Theorem 20 :** ***Every finite cyclic group G of order n is isomorphic to the group of integers addition modulo n. i.e.*** $(\mathbf{Z}_n, +_n)$. ***(A.N.U.A.92)***

***Proof :*** Let **G** be a finite cyclic group of order $n$ generated by an elemnt $a(\in \mathbf{G})$. Let $e$ be the identitiy in G.

$\therefore$ $\mathbf{G} = \{a^0 = e, a, a^2, a^3, ....., a^{n-1}\} = \{a^m / m$ is an integer and $0 \le m < n\}$

$\mathbf{Z}_n = \{0, 1, 2, .....(n - 1)\}$ is the group of integers w.r.t. $+_n$.

Define a mapping $f : \mathbf{G} \to \mathbf{Z}_n$ such that $f(a^m) = m \forall a^m \in \mathbf{G}$.

Since $a^0 = e, f(e) = f(a^0) = 0$ where 0 s the identity in $(\mathbf{Z}_n, +_n)$.

Let $a^i, a^j \in \mathbf{G}$. Now $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j$

$\therefore$ $f$ is $1-1$. Let $k \in \mathbf{Z}_n$. $\cdot\ a^k \in \mathbf{G}$ and $f(a^k) = k$

$\therefore$ $f$ is onto.

Let $a^i, a^j \in \mathbf{G}$. Then $a^i . a^j \in \mathbf{G}$ and $f(a^i a^j) = f(a^{i+j})$. By division algorithm, there exist integers $q$ and $r$.

Such that $i + j = qn + r,\ 0 \le r < n$.

$\therefore\ a^{i+j} = a^{qn+r} = (a^n)^q . a^r = e^q a^r = a^r\ (\because a^n = a^0 = e)$

$\therefore\ f(a^i a^j) = f(a^{i+j}) = f(a^r) = r$

$\therefore\ f(a^i) +_n f(a^j) = r$ by the definition of $f$.

$\therefore$ $f$ is a homomorphism and hence $f$ is an isomorphism from $\mathbf{G}$ to $\mathbf{Z}_n$.

$\therefore\ \mathbf{G} \cong \mathbf{Z}_n$.

**Theorem 21 :** ***Every cyclic group is isomorphic to either Z or $\mathbf{Z}_n$ for some n.***

**Proof :** The proof follows from Theorem 19 and Theorem 20.

## EXERCISE 8

**1.** (*a*) Find the generators of the group $\{a, a^2, a^3, a^4 = e\}$.
(*b*) Find all the generators of a cyclic group of order 10.

**2.** (*a*) For each of the following cyclic groups, find all the subgroups and give Lattice diagram for each of the subgroups.
(i) $\mathbf{Z_8}$ (ii) $\mathbf{Z_{12}}$ (iii) $\mathbf{Z_{36}}$
(*b*) Howmany subgroups does $\mathbf{Z_{20}}$ have ? List a generator for each of the subgroups.
Let $\mathbf{G} = < a >$ and $|a| = 20$. How many subgroups does G have ? Write a generator for each of these subgroups.

**3.** Prove that every homomorphic image of a cyclic group is cyclic.

**4.** Let $(\mathbf{Z}, +)$ be a cyclic group and $(\mathbf{G} = \{1, -1, i, -i\}, .)$ be a group where $i^2 = -1$. Show that under the mapping $f$ from $\mathbf{Z}$ to $\mathbf{G}$ defined by $f(n) = i^n\ \forall n \in \mathbf{Z}$ is the homomorphic image of $(\mathbf{Z}, +)$.

**5.** Prove that order of a finite cyclic group is the same as that of any generator of the group.

**6.** Show that the group of automorphisms of a cyclic group of order (degree) 4 is of order 2.

**7.** $\mathbf{Z}$ is the centre of a group $\mathbf{G}$. If $a \in \mathbf{Z}$, prove that the cyclic subgroup $< a >$ of $\mathbf{G}$ generated by $a$ is a normal subgroup of $\mathbf{G}$.

**8.** Let **G** be a group having no proper subgroups. Show that **G** must be a finite group of order $n$ where $n$ is either 1 or a prime number.

**9.** Prove that all cyclic groups of the same order are isomorphic to each other.

**10.** List all subgroups of a cyclic group $(i)$ $(\mathbf{G},\cdot)$ of order 24 and whose generator is $a$ $(ii)$ $(\mathbf{Z}_{30},+_{30})$.

**11.** Prove that the subgroups of the additive group of integers $(\mathbf{Z},+)$ are precisely the groups $(n\mathbf{Z},+)$ for any integer $n$.

**12.** $\mathbf{G}=\{a,a^2,a^3,.....,a^{15}=e\}$ is a cyclic group of order 15 and **H** is its subgroup generated by $a^3$. Then find in $\mathbf{G}/\mathbf{H}$ $(i)$ the inverse of $\mathbf{H}a$ and $(ii)$ solutions of $(\mathbf{H}a^5)x=\mathbf{H}a^7$.

**13.** $(i)$ Find all left cosets of the subgroup $<9>$ of $\mathbf{Z}_{36}$.

$(ii)$ Find all right cosets of the subgroup $<3>$ of $\mathbf{Z}_{12}$

**14.** $\mathbf{S}_5$ is the set of all permutations on 5 symbols is a group. Find the index of the cyclic subgroup generated by the permutation (2,3,5) in $\mathbf{S}_5$.

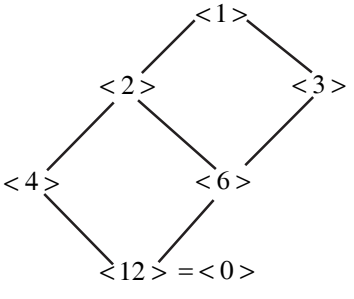
## ANSWERS

**1.** $(a)$ $a,a^3$ $(b)$ $a,a^3,a^7,a^9$

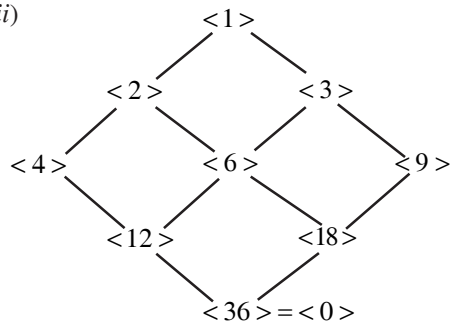
**2.** $(a)$ $(i)$ $<1>=\{0,1,2,3,4,5,6,7\},<2>=\{0,2,4,6\},<4>=\{0,4\},<8>=\{0\}$


$(ii)$ $<1>=\mathbf{Z}_{12},<2>=\{0,2,4,6,8,10\},<3>=\{0,3,6,9\},$

$<4>=\{0,4,8\},<6>=\{0,6\},<12>=<0>=\{0\}$



(*iii*)




**2.** (*b*) $<1>,<2>,<4>,<5>,<10>,<20>$; six subgroups; subgroups are those subgroups generated by $a^m$ where $m = 1,2,4,5,10,20$ and they are six in number.

**10.** (*i*) $(\{a^2, a^4, a^6, ....., a^{22}, a^{24} = e\}, \cdot), (\{a^3, a^6, a^9, ....., a^{21}, a^{24} = e\}, \cdot),$

$(\{a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24} = e\}, \cdot), (\{a^6, a^{12}, a^{18}, a^{24} = e\}, \cdot),$

$(\{a^8, a^{16}, a^{24} = e\}, \cdot), (\{a^{12}, a^{24} = e\}, \cdot)$

(*ii*) $<1> = \{0,1,2,.....,29\}, <2> = \{0,2,4,.....,28\}, <3> = \{0,3,6,....,27\},$

$<5> = \{0,5,10,15,20,25\}, <6> = \{0,6,12,18,24\}, <10> = \{0,10,20\},$

$<15> = \{0,15\}, <30> = \{0\}$

**13.** (*i*) $r + <9>, r = 0,1,2,.....,8$ (*ii*) $<3>, <3>+1, <3>+2$

**14.** 40

# Problems For Practicals

**1.** Define a permutation on $n$ symbols. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ is $fg$ equal to $gf$.

**2.** Define cyclic permutation. If $S$ consists of elements 1,2,3,...,9 then find (1 2 3 ) (5 6 4 1 8 ).

**3.** Define transposition. Give an example of transposition on $S = \{1, 2, 3, 4, 5\}$ and obtain its inverse $f = (2\,3)$ and $f^{-1} = f$.

**4.** Find the orbit and cycle of $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$

**5.** Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$ as product of disjoint cycles.

**6.** Express (1,2,3) (4,5) (1,6,7,8) (1,5) as product of disjoint cycles.

**7.** Express (2 5 4) (1 4 3) (2 1) as product of disjoint cycles and find its inverse.

**8.** Express $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ as product of transpositions. If f an odd or even permutation.

**9.** If $f = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 9), g = (4\ 1\ 5\ 6\ 7\ 3\ 2\ 8)$ are cyclic permutations prove that $(fg)^{-1} = g^{-1}f^{-1}$

**10.** Compute $a^{-1}ba$ where $a = (5\ 7\ 9), b = (1\ 2\ 3)$

**11.** Write the inverse cycle of $(1\ 2\ 4)(3\ 2\ 6) \in S_6$

**12.** Define orbit of a permutation. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} \in S_6$ find the orbit of 5.

**13.** Write the elements of the permutation group $S_3$ where $S = \{1,2,3\}$ Which of them are even?

**14.** Define order of a cyclic permutation. Find the order of $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$

**15.** By means of an example prove that a cycle of even length can be expressed as product of odd number of transpositions.

**16.** Supporting that a cycle of length $(n-1)$ can be expressed as product of $f \in S_n$ transpositions; prove that $f \in S_n$ is either even permutation or odd permutation.

**17.** By means of an example justify the statement

(i) "Product of two odd permutations is even"

(ii) "Product of two even permutations is even"

**18.** By means of an example justify the statement "Inverse of odd permutation is odd permutation"

**19.** Prove that $(1,2,3,4,.....,n)^{-1} = (n, n-1,.....4,3,2,1)$

**20.** Given $x = (1\ \ 2)(3\ \ 4)$ and $y = (5\ \ 6)(1\ \ 3)$ find permutation '$a$' so that $a^{-1}x\ a = y$.

**21.** How do you find the order of a given permuatation. Find the order of

$f = (1\ \ 2\ \ 3\ \ 4\ \ 5) \in S_5$

**22.** Examine whether the following permutations are even or odd.

$(i)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$ $(ii)\ (1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ \ 5)$

**23.** Define alternating group of degree $n$. Write the alternating group $A_3$ where $S = \{1,2,3\}$.

**24.** Write the regular permutation group isomorphic to the multiplicative group $G = \{1, w, w^2\}$.

**25.** Find the order of $n-$cycle in the permutation group $S_n$.

**26.** If $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} \in S_5$ write $AB, BA$ and $A^{-1}$.

**27.** State Cayley's theorem. Define regular permutation group.

**28.** Define a cyclic group and its generator. Write the generators of multiplicative group $G = \{1,-1,i,-i\}$

**29.** Prove that $G = \{A, B, C, D\}$ where $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,

$D = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$ is a cyclic group w.r.t matrix multiplication.

**30.** Prove that $(\overline{z}_5, +)$ where $\overline{z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ the set of congruence classes modulo 5 is a cyclic group.

**31.** Is every cyclic group abelian ? Prove that the converse is not true by an example.

**32.** What is the number of generators of cyclic group of order $n$ ? Find the number of generators of multiplicative group $G = \{1, \omega, \omega^2\}$. Write the generators.

**33.** Show that $G = \{1,2,3,4,5,6\}$ under multiplication modulo 7 is a cyclic group. Find the number of generators.

**34.** What is the number of generators of an infinite cyclic group ? If '$a$' is one generator then write other generators.

**35.** If $a^m$ is also generator of an $nth$ order cyclic group $G = < a >$ prove that $(m, n) = 1$.

**36.** Find the generators of cyclic group $G = \{0,1,2,3,4\}$ w.r.t addition modulo 5 Prove order of a generator is equal to the order of the group.

**37.** Is a subgroup of cyclic group cyclic ? If '$a$' is a generator of cyclic group G then what is the generator of its subgroup H.

**38.** If G is a finite cyclic group of order $n$ with generator '$a$' then prove that order of subgroup is $(n/m)$ when $a^m$ is its generator.

**39.** If $G\{w, w^2, w^3, w^4, w^5, w^6 = e\}$ is a cyclic group under multiplication, write the subgroups of G. Verify that order of subgroup divides order of the group.

**40.** When do you say that a cyclic group is finite and infinite ?

**41.** Prove that a group of prime order is cyclic. Give an example.

**42.** Verify the statement "every group of composite order possesses proper subgroups" by giving examples.

**43.** Give an example of infinite cyclic group. Establish it by means of its generators.

**44.** Write the isomorphic images of (i) infinite cyclic group and (ii) finite cyclic group.

**45.** If $G = \{0, \pm 1, \pm 2, .....\}$ is an infinite cyclic group w.r.t. addition find its generators. Write a cyclic subgroup H of G. Find index of H in G.

**46.** $G = \{0,1,2,3,4,5,6,7,8,9\}$ is a cyclic group w.r.t. addition modulo 10. Prove $H = \{0,5\}$ is a cyclic subgroup of G. Find $i(H)$.

## ANSWERS

**1.** $fg \neq gf$

**2.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$

**3.** $f = (2,3), f^{-1} = f$

**4.** Orbit of $1 = \{1,2,3,4,5\}$, Orbit of $2 = \{2,3,4,5,1\}$

Orbit of $3 = \{3,4,5,1,2\}$, Orbit of $4 = \{4,5,1,2,3\}$

Orbit of $5 = \{5,1,2,3,4\}$, Orbit of $6 = \{6\}$,

Orbit of $7 = \{7\}$ Orbit of $8 = \{8,9\}$ Orbit of $9 = \{9,8\}$

Cycle of the permutation = $(1\ 2\ 3\ 4\ 5)(8\ 9)$

**5.** $(1\ 6\ 2\ 5)(3\ 4)$ **6.** $(2\ 3\ 4\ 5\ 6\ 7\ 8\ 9)$ **7.** $(1\ 5\ 4\ 3)(2); (3\ 4\ 5\ 1)(2)$

**8.** $(1\ 2)(1\ 3)(5\ 6)$ **10.** $(1\ 2\ 3)$ **11.** $(6\ 2\ 3)(4\ 2\ 1)$

**12.** $\{5,6,4\}$ **14.** 3 **21.** 5 **22.** $(i)$ odd $(ii)$ odd

**23.** $A_3 = \left[\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right]$

**24.** $G = \left\{e, \begin{pmatrix}1&w&w^2\\w&w^2&1\end{pmatrix}, \begin{pmatrix}1&w&w^2\\w^2&1&w\end{pmatrix}\right\}$ **25.** $n$

**26.** $\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}, \begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$

**28.** $i, -i$ **31.** Yes, Klein's group of 4 **32.** $\phi(n)$; $\omega, \omega^2$

**33.** 2 **34.** 2, $a^{-1}$ **36.** 1,2,3,4

**37.** Yes, $a^{\alpha} \in H$ where d is the least positive integer **43.** $(Z,+) = \langle 1 \rangle = \langle -1 \rangle$

**44.** $\langle Z,+ \rangle, \left(z = e^{\frac{i2\pi}{n}}, \times\right)$ **45.** 3 **46.** 5

# Rings, Integral Domains & Fields

**9.1. Ring** is the second algebraic system of the subject of Modern Algebra. The abstract concept of rings has its origin from the set of integers. Eventhough integers, real numbers, integers modulo - $n$ and Matrices are endowed with two binary operations, when dealt them in Groups we have considered only one binary operation ignoring the other. The concept of Ring will take into account both addition and multiplication. The algebra of rings will follow the pattern already laid out for groups.

**Definition. (Ring.)** *Let R be a non-empty set and* $+, \bullet$ *be two binary operations in R.* $(R, +, \bullet)$ *is said to be a ring if, for* $a, b, c \in R$*;* **(*O. U. 03, 07, S. V. U. 98*)**

$R_1$. $a + b = b + a$ $\qquad$ $R_2$. $(a + b) + c = a + (b + c)$

$R_3$. *there exists* $0 \in R$ *such that* $a + 0 = a$ *for* $a \in R$.

$R_4$. *there exists* $-a \in R$ *such that* $a + (-a) = 0$ *for* $a \in R$.

$R_5$. $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ and

$R_6$. $a \,.\, (b + c) = a \,.\, b + a \,.\, c$ and $(b + c) \,.\, a = b \,.\, a + c \,.\, a$.

**Note 1.** The operation '+' is called the addition and the operation '$\bullet$' is called the multiplication in the ring $(R, +, \bullet)$.

**2.** The ring $(R, +, \bullet)$ is also called the ring $R$. **3.** We write $a \,.\, b$ as $ab$.

**4.** The properties $R_1, R_2, R_3, R_4$ merely state that $(R, +)$ is a commutative group.

Thus $(R, +)$ is called the additive group of the ring $R$.

**5.** The identity element '0' in $(R, +)$ is called the zero of the ring $R$. The zero of a ring should not be confused with the zero of the numbers.

**6.** By $R_3, 0 + 0 = 0$ for $0 \in R$.

**7.** The properties $R_5, R_6$ may be respectively called the Associative and Distributive laws.

In view of Note (4) and Note (7) a ring may also be defined as follows:

**Definition. (Ring.)** *Let.R be a non-empty set and* $+, \bullet$ *be two binary operations in R.* $(R, +, \bullet)$ *is said to be a ring, if* (*i*) $(R, +)$ *is a commutative group,* (*ii*) $(R, \bullet)$ *is a semigroup and* (*iii*) *Distributive laws hold.* **(*O. U. 07*)**

**Definition. (Unity Element.)** *In a ring* $(R,+,\bullet)$ *if there exists* $1\in R$ *such that* $a.1=1.a=a$ *for every* $a\in R$ *then we say that R is a ring with unity element or identity element.*

**Note 1.** If *R* is a ring with identity element, by $R_4$, we have $-1\in R$ so that $1+(-1)=0$.

**2.** A ring with unity element contains at least two elements 0 and 1 if $R\neq\{0\}$.

**Definition.** *In a ring* $(R,+,\bullet)$ *if* $a.b=b.a$ *for* $a,b\in R$ *then we say that R is a commutative ring.* **(*S. V. U. 04, A. U. 04*)**

**Imp.** A ring R (*i*) need not be commutative under multiplication and (*ii*) need not have an identity (unity) element under multiplication, unless or otherwise stated.

**e.g. 1.** Let $R=\{0\}$ and $+,\bullet$ be the operations defined by $0+0=0$ and $0\bullet 0=0$. Then $(R,+,\bullet)$ is clearly a ring called the *Null ring* or *Zero ring.*

**e.g. 2.** The set *Z* of integers w.r.t. usual addition and multiplication is a commutative ring with unity element. **(*S. V. U. 99, N. U. 00*)**

For (*i*) $(Z,+)$ is a commutative group (*ii*) Multiplication is associative in *Z* and (*iii*) Multiplication is distributive over addition.

**e.g. 3.** The set *N* of natural numbers is not a ring w.r.t. usual addition and multiplication, because, $(N,+)$ is not a group.

**e.g. 4.** The sets $Q,R,C$ are rings under the usual addition and multiplication of numbers.

**e.g. 5.** The set of integers $\bmod m$ under the addition and multiplication $\bmod m$ is a ring.

**e.g. 6.** The set of irrational numbers under addition and multiplication is not a ring as there is no zero element.

**9.2.** Let $(R,+,\bullet)$ be a commutative ring with unity element. Then $(R,+)$ is a commutative group and $(R,\bullet)$ is a semi - group with identity element 1. So we have the following results which are obvious from the theory of groups.

**1.** The zero element of *R* is unique and $a+0=a$ for every element '*a*' in *R*.

**2.** For $a\in R$ the additive inverse $-a\in R$ is unique and $a+(-a)=0$.

**3.** The identity element $1\in R$ is unique and $a.1=1.a=a$ for every $a\in R$.

**4.** For $a\in R,-(-a)=a$. **5.** For $0\in R,-0=0$. **6.** For $a,b\in R,-(a+b)=-a-b$.

**7.** For $a,b,c\in R, a+b=a+c\Rightarrow b=c$ and $b+a=c+a\Rightarrow b=c$

**8.** For $a,b,x\in R$, the equations $a+x=b$ and $x+a=b$ have unique solutions.

**9.** For $1\in R$, the identity element, $-(-1)=1$.

**10.** For $a,b_1,b_2,.....b_n\in R$, from $R_6$, we have $a(b_1+b_2+.....+b_n)=ab_1+ab_2+...+ab_n$ and $(b_1+b_2+.....+b_n)a=b_1a+b_2a+....+b_na$.

**Notation. 1.** If $R$ is a ring and $a,b\in R$ then $a+(-b)\in R$. $a+(-b)$ is written as $a-b$.

**2.** If $R$ is a ring and $a\in R$ then $a+a\in R$ and $a+a$ is written as $2a$.

**3.** If $R$ is a ring and $a\in R$ then $a.a\in R$ and $a.a$ is written as $a^2$.

## 9.3. SOME BASIC PROPERTIES OF RINGS

**Theorem 1.** ***If R is a ring and*** $0,a,b\in R$, ***then*** **(*i*)** $0a=a0=0$, ***(A. U. 12)***

**(*ii*)** $a(-b)=(-a)b=-(ab)$ ***(O. U. 07)*** **(*iii*)** $(-a)(-b)=ab$ ***(A. U. 12)***

**(*iv*)** $a(b-c)=ab-ac$. ***(O. U. 07, A.U. 03, 08; N.U. 03)***

**Proof.** (*i*) $0a=(0+0)a\Rightarrow 0+0a=0a+0a$ (By $R_3,R_6$)

$\therefore 0=0a$ (By right cancellation law of $(R,+)$)

Similarly we can prove that $a0=0$. Hence $0a=a0=0$

(*ii*) To prove that $a(-b)=-(ab)$ we have to show that $a(-b)+(ab)=0$.

$a(-b)+ab=a\{(-b)+b\}=a0=0$ (By $R_6,R_4$) $\Rightarrow a(-b)=-(ab)$

Similarly we can prove that $(-a)b=-(ab)$. Hence $a(-b)=(-a)b=-(ab)$.

(*iii*) $(-a)(-b)=-\{(-a)b\}=-\{-(ab)\}=ab$ (by (*ii*)) [$\because (R,+)$ is a group]

(*iv*) $a(b-c)=a[b+(-c)]=ab+a(-c)=ab-ac$ (By $R_6$) [By theorem (*i*), (*ii*)]

Similarly we can prove that $(b-c)a=ba-ca$.

**Theorem. 2.** ***If*** $(R,+,\bullet)$ ***is a ring with unity then this unity 1 is the only multiplicative identity.***

**Proof.** Suppose that there exist $1,1'\in R$ such that $1.x=x.1=x$ and

$1'.x=x.1'=x\ \forall\ x\in R$

Regarding 1 as identity, $1.1'=1'$. Regarding $1'$ as identity, $1.1'=1$

Thus $1'=1.1'=1$. $\therefore$ 1 is the only multiplicative identity.

**Theorem. 3.** ***If R is a ring with unity element 1 and*** $a\in R$ ***then*** **(*i*)** $(-1)a=-a$ **(*ii*)** $(-1)(-1)=1$

**Proof.** (*i*) $(-1)a+a=(-1)a+1a=\{(-1)+1\}a=0a=0$ ($\because a=1a$, $R_6$, $R_4$)

$\therefore (-1)a=-a$

(*ii*) For $a\in R$ we have $(-1)a=-a$. Taking $a=-1,(-1)(-1)=-(-1)=1$

## 9.4. BOOLEAN RING

***(N. U. 07, S. V. U. M 07)***

**Definition.** *In a ring R if* $a^2=a\ \forall\ a\in R$ *then R is called a Boolean ring.*

**Theorem 1.** ***If R is a Boolean ring then*** **(*i*)** $a+a=0\ \forall\ a\in R$ **(*ii*)** $a+b=0\Rightarrow a=b$ ***and (iii) R is commutative under multiplication. Or, Every Boolean ring is abelian.***

***(S. V. U. 07, S. K.D. 04, N. U.07)***

**Proof.** $(i)$ $a \in R \Rightarrow a + a \in R$.

Since $a^2 = a \; \forall \; a \in R$, we have $(a+a)^2 = a + a \Rightarrow (a+a)(a+a) = a + a$

$\Rightarrow a(a+a) + a(a+a) = a + a \Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$ (By $R_6$)

$\Rightarrow (a+a) + (a+a) = a + a$ ($\because$ $R$ is Boolean)

$\Rightarrow (a+a) + (a+a) = (a+a) + 0$ (By $R_3$)

$\Rightarrow a + a = 0$ [By left cancellation law of group $(R, +)$]

$(ii)$ For $a, b \in R, a + b = 0 \Rightarrow a + b = a + a \Rightarrow b = a$ [By $(i)$]

$(iii)$ $a, b \in R \Rightarrow a + b \in R \Rightarrow (a+b)^2 = a + b$ ($\because$ $R$ is Boolean)

$\Rightarrow (a+b)(a+b) = a + b \Rightarrow a(a+b) + b(a+b) = a + b$ (By $R_6$)

$\Rightarrow (a^2 + ab) + (ba + b^2) = a + b$ (By $R_6$)

$\Rightarrow (a + ab) + (ba + b) = a + b$ ($\because$ $R$ is Boolean)

$\Rightarrow (a+b) + (ab + ba) = a + b$ [$\because$ $(R, +)$ is a group]

$\Rightarrow (a+b) + (ab + ba) = (a+b) + 0 \Rightarrow ab + ba = 0 \Rightarrow ab = ba$ (By $(ii)$)

## SOLVED PROBLEMS

**Ex. 1.** *If $R$ is a ring with identity element 1 and $1 = 0$ then $R = \{0\}$.*

**Sol.** $x \in R \Rightarrow x = 1x \Rightarrow x = 0x \Rightarrow x = 0$ [By Theorem $1(i)$]

$\therefore$ $R = \{0\}$

Thus a ring $R$ with unity has atleast two elements if $R \neq \{0\}$.

**Ex. 2.** *Prove that the set of even integers is a ring, commutative without unity under usual addition and multiplication of integers.*

**Sol.** Let $R$ = the set of even integers. Then $R = \{2x \mid x \in Z\}$.

$a, b, c \in R \Rightarrow a = 2m, b = 2n, c = 2p$ where $m, n, p \in Z$.

$(R, +)$ is a commutative group. (see ex. in groups)

$a \,.\, b = (2m)(2n) = 2l$ where $l = 2mn \in Z$

$\therefore$ Multiplication $(\bullet)$ of integers is a binary operation in $R$.

$(a \,.\, b) \,.\, c = (2m \,.\, 2n) \,.\, 2p = 8mnp$ and $a \,.\, (b \,.\, c) = 2m \,.\, (2n \,.\, 2p) = 8mnp$

$\therefore$ $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ $\Rightarrow$ Multiplication $(\bullet)$ is associative in $R$.

$a \,.\, (b + c) = 2m \,(2n + 2p) = 2m \,.\, 2n + 2m \,.\, 2p = a \,.\, b + a \,.\, c$

Similarly, $(b + c) \,.\, a = b \,.\, a + c \,.\, a$

$\therefore$ Distributive laws hold in $R$. Hence $(R, +, \bullet)$ is a ring.

Since '1' is not an even integer; $1 \notin R$ and hence $R$ has no unity element.

**Ex. 3.** $(R,+)$ *is an abelian group.*

*Show that* $(R,+,\bullet)$ *is a ring if multiplication* $(\bullet)$ *is defined as* $a\,.\,b=0\ \forall\ a,b\in R$.

**Sol.** To prove that $(R,+,\bullet)$ is a ring we have to show that $(R,\bullet)$ is semigroup and distributive laws hold.

$\forall\ a,b\in R, a\,.\,b=0$ where $0\in R$ is the zero element in the group.

$\therefore$ multiplication '$\bullet$' is a binary operation in $R$.

Let $a,b,c\in R$. Then $(a\,.\,b)\,.\,c=0\,.\,c=0\,;a\,.\,(b\,.\,c)=a\,.\,0=0$ (By Def.)

$\therefore\ (a\,.\,b)\,.\,c=a\,.\,(b\,.\,c)\ \forall\ a,b,c\in R$ $\therefore\ (R,\bullet)$ is a semi group.

Let $a,b,c\in R$. $a\in R, b+c\in R\Rightarrow a\,.\,(b+c)=0$

$a\in R, b\in R\Rightarrow ab=0; a\in R, c\in R\Rightarrow ac=0$ $\Rightarrow ab+ac=0+0=0$.

Hence $a\,.\,(b+c)=a\,.\,b+a\,.\,c$

Similarly we can prove that $(b+c)\,.\,a=b\,.\,a+c\,.\,a$ $\therefore$ Distributive laws hold.

**Ex. 4.** *Prove that* $Z_m=\{0,1,2,.....,m-1\}$ *is a ring with respect to addition and multiplication modulo m.* **(*N. U. 01, O. U. 03*)**

**Sol.** We denote addition modulo $m$ by $+_m$ and multiplication modulo $m$ by $\times_m$. We also know that $a+_m b=a+b\ (\text{mod}\,m)=r$ where $r$ is the remainder when $a+b$ is divided by $m$. $a\times_m b=ab\ (\text{mod}\,m)=s$ where $s$ is the remainder when $ab$ is divided by $m$.

Let $a,b,c\in Z_m$. $a+_m b=a+b\ (\text{mod}\,m)\in Z_m\Rightarrow +_m$ is a binary operation in $Z_m$.

$a+_m b=a+b\ (\text{mod}\,m)=b+a\ (\text{mod}\,m)=b+_m a$ $\Rightarrow +_m$ is commutative in $Z_m$.

$(a+_m b)+_m c=(a+b)+c\ (\text{mod}\,m)=a+(b+c)\ (\text{mod}\,m)=a+_m(b+_m c)$

$\therefore +_m$ is associative in $Z_m$.

There exists $0\in Z_m$ such that $0+_m a=0+a\ (\text{mod}\,m)=a\ (\text{mod}\,m)=a$.

$\Rightarrow 0$ is the zero element.

For $0\in Z_m$, we have $0+_m 0=0\ (\text{mod}\,m)\Rightarrow$ additive inverse of $0=0$.

For $a\neq 0\in Z_m$ we have $0<a<m$ $\Rightarrow 0<m-a<m\Rightarrow m-a\in Z_m$

$a+_m(m-a)=a+(m-a)\ (\text{mod}\,m)=m\ (\text{mod}\,m)=0\ (\text{mod}\,m)$

$\therefore$ inverse of $a\neq 0\in Z_m$ is $m-a\in Z_m$. Hence $(Z_m,+)$ is an abelian group.

Let $a,b,c\in Z_m$. $a\times_m b=ab\ (\text{mod}\,m)\in Z_m\Rightarrow\times_m$ is a binary operation in $Z_m$

$(a\times_m b)\times_m c=(ab)\,c\ (\text{mod}\,m)=a\,(bc)\ (\text{mod}\,m)=a\times_m(b\times_m c)$

$\therefore\ \times_m$ is associative in $Z_m$.

$a\times_m(b+_m c)=a\,(b+c)\ (\text{mod}\,m)=ab+ac\ (\text{mod}\,m)=(a\times_m b)+_m(a\times_m c)$

and $(b+_m c)\times_m a=(b\times_m a)+_m(c\times_m a)$ so that distributive laws hold.

$\therefore\ (Z_m,+_m,\times_m)$ is a ring.

**Note.** Put $m=6$ in the above proof to prove that $Z_6$ is a ring.

**Ex. 5.** *Prove that the set* $R=\{a,b\}$ *with addition* $(+)$ *and multiplication* $(\bullet)$ *defined as follows is a ring.*

| $+$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $b$ | $a$ |

and

| $\bullet$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ |

**Sol.** From the above tables, clearly $+,\bullet$ are binary operation in $R$.

1. $(a+a)+b=a+b=b;\ a+(a+b)=a+b=b\Rightarrow(a+a)+b=a+(a+b)$

   $(a+b)+a=b+a=b;a+(b+a)=a+b=b\Rightarrow(a+b)+a=a+(b+a)$, etc,

   $\therefore$ Associativity is true.
2. $a\in R$ is the zero element because $a+a=a,b+a=b$
3. $a+b=b=b+a\Rightarrow$ commutativity is true.
4. $a+a=a\Rightarrow$ additive inverse of $a=a$ and $b+b=a\Rightarrow$ additive inverse of $b=b$.
5. $a\,.\,(a\,.\,b)=a\,.\,a=a;\ (a\,.\,a)\,.\,b=a\,.\,b=a\Rightarrow a\,.\,(a\,.\,b)=(a\,.\,a)\,.\,b$, etc

   $\therefore$ Associativity is true.
6. $a\,.\,(b+a)=a\,.\,b=a;a\,.\,b+a\,.\,a=a+a=a\Rightarrow a\,.\,(b+a)=a\,.\,b+a\,.\,a$

   $(b+a)\,.\,a=b\,.\,a=a;\ b\,.\,a+a\,.\,a=a+a=a\Rightarrow(b+a)\,.\,a=b\,.\,a+a\,.\,a$, etc.

   $\therefore$ Distributive laws are true. Hence $(R,+,\bullet)$ is a ring.

**Ex. 6.** *If* $R$ *is a ring and* $a,b,c,d\in R$ *then prove that*

$(i)$ $(a+b)(c+d)=ac+ad+bc+bd$, *and* **(S. V. U. 99)** $(ii)$ $a+b=c+d\Leftrightarrow a-c=d-b$

**Sol.** $(i)$ $(a+b)(c+d)=a(c+d)+b(c+d)=ac+ad+bc+bd$ (By $R_6$)

$(ii)$ $a+b=c+d\Leftrightarrow(a+b)+(-b)=(c+d)+(-b)$

$\Leftrightarrow a+(b+(-b))=(c+d)+(-b)$

$\Leftrightarrow a+0=(c+d)+(-b)$ (By $R_4$)

$\Leftrightarrow a+(-c)=(-c)+\{(c+d)+(-b)\}$

$\Leftrightarrow a-c=((-c)+c)+\{d+(-b)\}$ (By $R_4$)

$\Leftrightarrow a-c=0+(d-b)\Leftrightarrow a-c=d-b$

## EXERCISE 9 ( *a* )

**1.** If $R$ is a ring and $a,b,c\in R$ prove that $(a-b)-c=(a-c)-b$

**2.** If $R$ is a ring and $a,b\in R$ then prove that the equation $a+x=b$ has unique solution in $R$.

**3.** In a ring $R$ if '$a$' commutes with '$b$' prove that '$a$' commutes with '$-b$' where $a,b\in R$.

**4.** If $R$ is a ring with unity element '1' and $R\neq\{0\}$ prove that $1\neq0$ where $0\in R$ is the zero element.

**5.** $R$ is a Boolean ring and for $a\in R,\ 2a=0\Rightarrow a=0$ then prove that $R=\{0\}$.

**6.** If $R$ is a commutative ring prove that $(a+b)^2 = a^2 + 2ab + b^2 \quad \forall\, a,b \in R$.

**7.** If $R$ is a ring and $a,b,c,d \in R$ evaluate $(a-b)(c-d)$.

**8.** If $R = \{a\sqrt{2} \mid a \in Q\}$ is $(R,+,\bullet)$ under ordinary addition and multiplication, a ring ?

**9.** Is the set of all pure imaginary numbers $= \{iy \mid y \in R\}$ a ring with respect to addition and multiplication of complex numbers ?

**10.** If $Z =$ the set of all integers and '$n$' is a fixed integer prove that the set $nZ = \{nx \mid x \in Z\}$ is a ring under ordinary addition and multiplication of integers.

**ANSWERS**

**2.** $b-a$ **7.** $ac+bd-ad-bc$ **8.** Not a ring **9.** Not a ring

## 9.5. ZERO DIVISORS OF A RING

Though rings are generalisation of number system some algebraic properties of number system need not hold in general rings.

The product of two numbers can only be zero if atleast one of them is zero, whereas in any ring it may not be true. For example, in the ring $(Z_6,+,\bullet)$ of modulo - 6, we have $2.3 = 0$ with neither $2 = 0$ nor $3 = 0$.

**Definition. (Zero Divisors).** *Two non zero elements $a,b$ of a ring $R$ are said to be zero divesors (divisors of zero) if $ab = 0$, where $0 \in R$ is the zero element.*

**(*O. U. 12, S.K.D. 04*)**

In particular '$a$' is left zero divisor and '$b$' is right zero divisor.

**Definition. (Zero Divisor).** $a \neq 0 \in R$ is a zero divisor if there exists $b \neq 0 \in R$ such that $ab = 0$.

**Note. 1.** In a commutative ring there is no distinction between left and right zero divisors.

**2.** A ring $R$ has no zero divisors $\Leftrightarrow a,b \in R$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$

**e.g.1.** The ring of integers $Z$ has no zero divisors.

**e.g. 2.** In the ring $(Z_{12},+,\bullet)$, the elements $2,3,4,6,8,9,10$ are zero divisors.

For $2.6 = 0, 3.4 = 0, 3.8 = 0, 4.6 = 0, 4.9 = 0, 6.10 = 0$

Observe that the G. C. D of any of $\{2,3,4,6,8,9,10\}$ and $12 \neq 1$.

**e.g.3.** The ring $(M_2,+,\bullet)$ of $2\times 2$ matrices whose elements are in $Z$, has zero divisors.

For, we have $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq O,\ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq O$, where $O$ is zero matrix, are such that $AB = O$.

**e.g. 4.** The ring $(Z_3,+,\bullet)$ of modulo - 3 has no zero divisors.

**e.g. 5.** The ring $Z\times Z = \{(a,b) \mid a,b \in Z\}$ has zero divisors.

For, $(0,1),(1,0) \in Z\times Z \Rightarrow (0,1)\cdot(1,0) = (0,0) =$ zero element in $Z\times Z$.

**Imp.** In the ring of integers Z, all the solutions of $x^2-4x+3=0$ are obtained by factoring as $x^2-4x+3=(x-1)(x-3)$ and equating each factor to zero. While doing so, we are using the fact that Z is an Integral Domain, so that it has no zero divisors.

But if we want to find all solutions of an equation in a ring R which has zero divisors, we can do so, by trying every element in the Ring by substitution in the product $(x-1)(x-3)$ for zero.

**e.g. 6.** In the ring Z of integers, the equation $x^2+2x+4=0$ *i.e.* $(x+1)^2+3=0$ has no solution as $(x+1)^2+3\geq 3\ \forall\ x\in Z$. **(*O. U. 12*)**

But, in the ring $Z_6=\{0,1,2,3,4,5\}, (x+1)^2+3$ takes respectively the values $4,1,0,1,4,3$ for $x=0,1,2,3,4,5\in Z_6$.

$\therefore\ x^2+2x+4=0$ has $2\in Z_6$ as solution.

## 9. 6. CANCELLATION LAWS IN A RING

If $(R,+,\bullet)$ is a ring, then $(R,+)$ is an abelian group. So, cancellation laws with respect to addition are true in $R$. Now, we are concerned about the cancellation laws in $R$, namely $ab=ac\Rightarrow b=c, ba=ca\Rightarrow b=c$ for $a,b,c\in R$ with respect to multiplication.

**Definition. (Cancellation laws).** *In a ring R, for* $a,b,c\in R$ *if* $a\neq 0, ab=ac\Rightarrow b=c$ *and* $a\neq 0, ba=ca\ \Rightarrow b=c$ *then we say that cancellation laws hold in* $R$.

**Theorem.** ***A ring R has no zero divisors if and only if the cancellation laws hold in R.*** **(*S. K. D. 04, K. U. 03, 08, S. V. U. 08*)**

**Proof.** Let the ring have no zero divisors. We prove that cancellation laws hold in $R$.

$a,b,c\in R$ and $a\neq 0, ab=ac\Rightarrow ab-ac=0$

$\Rightarrow a(b-c)=0\Rightarrow b-c=0\quad (\because a\neq 0)\Rightarrow b=c$

Similarly we can prove $a\neq 0, ba=ca\Rightarrow b=c$

**Conversely**, let the cancellation laws hold in $R$. We prove that R has no zero divisors. If possible, suppose that there exist $a,b\in R$ such that $a\neq 0, b\neq 0$ and $ab=0$.

$ab=0\Rightarrow ab=a0\Rightarrow b=0$ (By cancellation law)

This is a contradiction. $\therefore\ a\neq 0, b\neq 0$ and $ab=0$ is not true in $R$.

$\therefore\ R$ has no zero divisors.

**Note.** The importance of having no zero divisors in a ring $R$, is, that an equation $ax=b$ where $a\neq 0, b\in R$ can have atmost one solution in $R$.

For $x_1,x_2\in R$ if $ax_1=b$ and $ax_2=b$ then $ax_1=ax_2\Rightarrow x_1=x_2$ (By cancellation law)

If $a\neq 0\in R$ has multiplicative inverse, say, $a^{-1}\in R$ then the solution is $a^{-1}b\in R$.

## SOLVED PROBLEMS

**Ex. 1.** *Find the zero divisors of* $Z_{12}$, *the ring of residue classes modulo - 12.*

**Sol.** $Z_{12} = \{\bar{0}, \bar{1}, ....., 11\}$. **(*O. U. 04*)**

For $\bar{a} \neq \bar{0} \in Z_{12}$ there should exist $\bar{b} \in Z_{12}$ such that $\bar{a} \times \bar{b} \equiv 0 \pmod{12}$

We have $\bar{2} \times \bar{6} = \bar{0}, \bar{3} \times \bar{4} = \bar{0}, \bar{4} \times \bar{3} = \bar{0}, \bar{6} \times \bar{2} = \bar{0}, \bar{8} \times \bar{3} = \bar{0}, \bar{8} \times \bar{6} = \bar{0}, \bar{8} \times \bar{9} = \bar{0}, \overline{10} \times \bar{6} = \bar{0}$

$\therefore$ $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \overline{10}$ are zero divisors.

**Ex. 2.** *Solve the equation* $x^2 - 5x + 6 = 0$ *in the ring* $Z_{12}$. **(*O. U. 12*)**

**Sol.** In the ring of integers Z, which has no zero divisors,

$x^2 - 5x + 6 = 0 \equiv (x-2)(x-3) = 0$ has two solutions $2, 3 \in Z$.

But in $Z_{12}$; for $x = 6, (x-2)(x-3) = (4)(3) = 12 = 0$

and for $x = 11, (x-2)(x-3) = (9)(8) = 72 = 0$.

$\therefore$ the given equation has 4 solutions, namely, 2, 3, 6 and 11 in the ring $Z_{12}$.

**Ex. 3.** *In the ring* $Z_n$, *show that the zero divisors are precisely those elements that are not relatively prime to n.* (or) show that every non-zero element of $Z_n$ is a unit or zero divisor.

**Sol.** Let $m \in Z_n = \{0, 1, 2, ...., n-1\}$ and $m \neq 0$. Let $m$ be not relatively prime to $n$.

Then G. C.D of $m, n = (m, n) \neq 1$. Let $(m, n) = d$.

We have $(m, n) = d \Rightarrow \left(\frac{m}{d}, \frac{n}{d}\right) = 1 \Rightarrow \frac{m}{d}, \frac{n}{d} \in Z_n$ and $\frac{m}{d} \neq 0, \ \frac{n}{d} \neq 0$

$\therefore$ $m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right) n = 0 \pmod{n}$. Thus $m \neq 0, \frac{n}{d} \neq 0 \Rightarrow m\left(\frac{n}{d}\right) = 0$

$\Rightarrow m$ is a zero divisor.

$\therefore$ Every $m \in Z_n$ which is not relatively prime to $n$ is a zero divisor.

Let $m \in Z_n$ be relatively prime to $n$.

Then $(m, n) = 1$. Let $mr = 0$ for some $r \in Z_n$.

We have $mr = 0 \pmod{n} \Rightarrow n \mid mr \quad \Rightarrow n \mid r \quad (\because (m, n) = 1) \quad \Rightarrow r = 0 \quad (0 \leq r < n-1)$

$\therefore$ If $m \in Z_n$ is relatively prime to $n$ then $m$ is not a zero divisor.

**Note.** If $p$ is a prime, then $Z_p$ ring has no zero divisors.

## 9. 7. SOME SPECIAL TYPES OF RINGS

**Definition. (Integral Domain)** *A commutative ring D with unity containing no zero divisors is an Integral Domain.* **(*O. U. 07, S. V. U. 03*)**

**Note. 1.** Some authors define integral domain without unity element.

**2.** For "Integral Domain" we simply use the word "Domain" and denote by the symbol D.

**Imp.** D is an integral domain $\Leftrightarrow$ (1) D is a ring, (2) D is commutative, (3) D has unity element and (4) D has no zero divisors.

**e.g. 1.** The ring of integers $Z$ is naturally an integral domain. ***(N. U. 00, S. V. U. 99)***

$1 \in Z$ is the unity element and $\forall\, a, b \in Z$ we have $ab = ba$ (commutativity)

and $ab = 0 \Rightarrow a = 0$ or $b = 0$ (no zero divisors).

**e.g.2.** $(Z_6, +, \bullet)$ where $Z_6 = \{0,1,2,3,4,5\}$, the set of integers under modulo - 6 system, is a ring. $1 \in Z_6$ is the unity element and $\forall\, a, b \in Z_6$ we have

$$ab \pmod 6 = ba \pmod 6 \text{ (commutative)}$$

But, for $2 \neq 0, 3 \neq 0 \pmod 6$, $2.3 = 6 \pmod 6 = 0$ and hence $Z_6$ has zero divisors.

Therefore, $Z_6$ is not an integral domain.

**e.g. 3.** If $Q =$ the set of all rational numbers and $R =$ the set of all real numbers then $(Q, +, \bullet)$ and $(R, +, \bullet)$ are integral domains.

**e.g. 4.** $Z_7 = \{0,1,2,3,4,5,6\}$, the set of all integers under modulo - 7 is an integral domain with respect to addition and multiplication modulo - 7.

**e.g. 5.** The ring $(M_2, +, \bullet)$ of $2 \times 2$ matrices is not an integral domain because it is not commutative and has zero divisors.

**e.g. 6.** $Z \times Z = \{(a,b) \mid a, b \in Z\}$ is not Integral Domain under addition and multiplication of components.

**Theorem. 1.** ***In an integral domain, cancellation laws hold.*** **(*A. U. 07, O. U. 07*)**

(Write the proof of (1) part of theorem in Art. 9.6)

**Theorem. 2.** ***A commutative ring with unity is an integral domain if and only if the cancellation laws hold.***

(Write the proof of theorem in Art. 9.6)

**Definition. (Multiplicative Inverse).** *Let R be a ring with unity element '1'. A non-zero element $a \in R$ is said to be invertible under multiplication, if there exists $b \in R$ such that $ab = ba = 1$. $b \in R$ is called* ***multiplicative inverse*** *of $a \in R$.*

From the theory of groups, multiplicative inverse of $a \neq 0 \in R$, if exists, is unique. It is denoted by $a^{-1}$. Also $aa^{-1} = a^{-1}a = 1$.

**Definition. (Unit of a Ring).** *Let R be a ring with unity. An element $u \in R$ is said to be a* ***unit of R*** *if it has multiplicative inverse in R.*

**Note. 1.** Zero element of a ring is not an unit.

**2.** Unity element of a ring and unit of a ring $R$ are different. Unity element is the multiplicative identity while unit of a ring is an element of the ring having multiplicative inverse in the ring. Ofcourse unity element is a unit.

**Theorem. 3.** ***In a ring R with unity, if*** $a(\neq 0)\in R$ ***has multiplicative inverse, then it is unique.***

**Proof.** Suppose that there exist $b,b'\in$ R such that $ab=ba=1$ and $ab'=b'a=1$.

Then $ab=ab'=1$.

By definition of cancellation law, $b=b'$.

**e.g. 1.** $Z$ is a ring with unity element = 1. We have $1.1=1$ and $(-1)(-1)=1$ for $-1,1\in Z$.

If $a\neq\pm1\in Z$ then there exists no $b\in Z$ such that $ab=ba=1$. Therefore, $-1,1$ are the only units in the ring $Z$. Observe that unity element is also unit.

**e.g.2.** Consider the ring $Z_7=\{0,1,2,3,4,5,6\}$ under addition and multiplication modulo - 7. It has unity element = 1 which is also a unit.

Further $2.4=4.2=1\,(\text{mod}\,7), 3.5=5.3=1\,(\text{mod}\,7)$ and $6.6=1\,(\text{mod}\,7)$.

Thus every non-zero element is a unit.

**e.g.3.** Consider the ring $Z\times Z=\{(m,n);m,n\in Z\}$.

The unity element $=(1,1)$ which is also unit.

Also, $(1,-1)(1,-1)=(1.1,(-1)(-1))=(1,1)$; $(-1,1)(-1,1)=(1,1)$ and $(-1,-1)(-1,-1)=(1,1)$

Thus $(1,1),(1,-1),(-1,1)$ and $(-1,-1)$ are units in $Z\times Z$.

**Definition. (Division Ring or Skew Field)** *Let R be a ring with unity element. If every non-zero element of R is a unit then R is a Division Ring.* **(*S. V. U. 00, 03, 05*)**

$(R,+,\bullet)$ is a Division ring $\Leftrightarrow$ (1) $R$ is a ring, (2) R has unity element and (3) every non - zero element in $R$ is invertible under multiplication.

**e.g.1.** $(Z,+,\bullet)$ is not a division ring, for, $2\neq 0\in Z$ has no multiplicative inverse in $Z$.

**e.g. 2.** $(Q,+,\bullet)$ and $(R,+,\bullet)$ are division rings.

**e.g. 3.** The ring $(M_2,+,\bullet)$ of non-singular $2\times2$ matrices is a division ring.

**Definition. (Field)** *Let R be a commutative ring with unity element. If every non-zero element of R is invertible under multiplication then R is a field.*

**(*S. V. U. 03, O. U. M12, 03, 08, S. K. U. 01*)**

**Another Definition.** *A commutative ring with unity is called a field if every non-zero element is a unit.*

$(R,+,\bullet)$ is a field $\Leftrightarrow$ (1) $R$ is a ring, (2) $R$ is commutative (3) $R$ has unity element and (4) every non - zero element of $R$ is a unit.

Usually a field is denoted by the symbol $F$.

**Note. 1.** A division ring which is also commutative is a field.

**2.** In a field, the zero element and the unity element are different. Therefore, a field has atleast two elements.

**e.g. 1.** We know that $(Q,+)$ where $Q=$ the set of all rational numbers is an additive group and $(Q-\{0\},\bullet)$ is a multiplicative group. Further distributive laws hold.

Therefore $(Q,+,\bullet)$ is a field.

**e.g. 2.** $(Z,+,\bullet)$ where $Z=$ the set of all integers is not a field, because all non-zero elements of $Z$ are not units.

**e.g. 3.** $(Z_7,+,\bullet)$ where $Z_7=$ the set of integers under modulo - 7 is a field.

**Theorem. 4.** ***A field has no zero - divisors.*** **(A. U. 07,12, O. U. 03, S. V. U. 00, K. U. 12)**

**Proof.** Let $(F,+,\bullet)$ be a field. Let $a,b\in F$ and $a\neq 0$.

$a\neq 0\in F, F$ is a field $\Rightarrow$ there exists $a^{-1}\in F$ such that $aa^{-1}=a^{-1}a=1$.

$ab=0\Rightarrow a^{-1}(ab)=a^{-1}0\Rightarrow (a^{-1}a)\,b=0\Rightarrow 1b=0\Rightarrow b=0$

Thus $a,b\in R, a\neq 0$ and $ab=0\Rightarrow b=0$.

Similarly, we can prove that, $a,b\in R, b\neq 0$ and $ab=0\Rightarrow a=0$.

$\therefore$ $F$ has no zero divisors.

**Note.** A division ring has no zero divisors. (Write the proof of the theorem (3))

**Theorem. 5.** ***Every field is an integral domain.***

**(N. U. 12, 01, O. U. 03, S. K. U. 07, S. V. U. 08)**

**Proof.** Let $(F,+,\bullet)$ be a field. Then the ring F is a commutative ring with unity and having every non - zero element as unit.

But an integral domain is a commutative ring with unity and having no zero divisors.

So, we have to prove that F has no zero divisors.

(Write the proof of the above Theorem (3))

**Note.** The converse of the above theorem need not be true. But an integral domain with finite number of elements can become a field.

**Theorem 6.** ***Every finite integral domain is a field.***

**(N. U. 08, O. U. 12, 07, 08, A. U. 07, 08, S. K. D. 08, K. U. 03, S. V. U. 99)**

**Proof.** Let $0,1,a_1,a_2,.....,a_n$ be all the elements of the integral domain $D$.

Then $D$ has $n+2$ elements which is finite.

Integral domain $D$ is a commutative ring with unity and having no zero divisors.

So, we have to prove that every non-zero element of $D$ has multiplicative inverse in $D$.

Let $a\in D$ and $a\neq 0$

Now consider the $n+1$ products $a1, aa_1, aa_2, ...., aa_n$.

If possible, suppose that $aa_i=aa_j$ for $i\neq j$.

Since $a\neq 0$, by cancellation law we have $a_i=a_j$.

This is a contradiction since $i\neq j$.

Therefore $a1, aa_1, aa_2, ....., aa_n$ are $(n+1)$ distinct elements in $D$.

Since $D$ has no zero divisors, none of these $(n+1)$ elements is zero element.

Hence, by counting ;

$a1, aa_1, aa_2, ....., aa_n$ are the $(n+1)$ elements $1,a_1,a_2,.....,a_n$ in some order.

$\therefore$ $a1 = 1$ or $a = 1$ or $aa_i = 1$ for some $i$.

For $a \neq 0 \in D$ there exists $b = a_i \in D$ such that $ab = 1$

$\Rightarrow a \neq 0 \in D$ has multiplicative inverse in $D$. $\therefore$ D is a field.

**Theorem 7.** ***If p is a prime then $Z_p$, the ring of integers modulo p, is a field.***

***(N. U. 07, S. K. U. 05)***

**Proof.** In Ex. 4 on page 5, we proved that $(Z_p, +, \bullet)$ is a ring.

Since $Z_p = \{0, 1, 2, ....., p-1\}$ has $p$ distinct elements, $Z_p$ is a finite ring.

We prove now that $Z_p$ is an integral domain.

Clearly, $1 \in Z_p$ is the unity element.

For $a, b \in Z_p, ab \pmod p \equiv ba \pmod p \Rightarrow ab = ba$ and hence $Z_p$ is commutative.

For $a, b \in Z_p$ and $ab = 0 \Rightarrow ab \equiv 0 \pmod p \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$ ($\because p$ is prime)

$\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$ $\Rightarrow a = 0$ or $b = 0$.

$\therefore$ $Z_p$ has no zero divisors. Thus $(Z_p, +, \bullet)$ is a finite integral domain.

$\therefore$ $Z_p$ is a field.

**Theorem. 8.** ***If $(Z_n, +, \bullet)$ is a field then n is a prime number.*** ***(N. U. 07)***

**Proof.** If possible let $m$ be a divisor of $n$.

$\therefore$ there exists $q \in Z$ such that $n = mq$. Clearly $1 \leq m, q \leq n$.

$mq = n \Rightarrow mq \equiv 0 \pmod n$. Since $Z_n$ is a field, $Z_n$ has no zero divisors.

$\therefore$ $mq \equiv 0 \pmod n \Rightarrow m = 0 \pmod n$ or $q = 0 \pmod n$

$\Rightarrow m = n$ or $q = n \Rightarrow m = n$ or $m = 1 (\because mq = n)$. $\therefore$ $n$ is a prime number.

**Theorem. 9.** ***$Z_p = \{0, 1, 2, ....., p-1\}$ is a field if and only if p is a prime number.***

**Proof.** Write the proofs of Theorem 6 and Theorem 7.

**Note.** In the field $Z_p = \{0, 1, 2, ....., p-1\}$ where $p$ is a prime, 1 and $p-1$ are the only elements that are their own multiplicative inverses.

## SOLVED PROBLEMS

**Ex. 4.** *Find all solutions of $x^2 - x + 2 = 0$ over $Z_3[i]$.*

**Sol.** We have $Z_3 = \{0, 1, 2\}$ under modulo - 3 system. $Z_3[i] = \{a + ib \mid a, b \in Z_3 \text{ and } i^2 = -1\}$

$= \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$, containing 9 elements.

Let $P(x) = x^2 - x + 2$. Then $P(0) \neq 0, P(1) \neq 0, P(2) \neq 0, P(i) = -1 - i + 2 \neq 0,$

$P(1+i) = (1 - 1 + 2i) - 1 - i + 2 \neq 0$, $P(2+i) = (4 - 1 + 4i) - (2 + i) + 2 \neq 0$, $P(2i) = -4 \neq 0$

$P(1+2i) = (1 - 4 + 4i) - (1 + 2i) + 2 \neq 0, P(2+2i) = (4 - 4 + 8i) - (2 + 2i) + 2 \neq 0$

$\therefore$ $x^2 - x + 2 = 0$ has no solution over $Z_3[i]$.

**Ex. 5.** *Show that* $1, p-1$ *are the only elements of the field* $Z_p$, $p$ *is prime, that are their own multiplicative inverses.*

**Sol.** Observe that, in $Z_p$ field, $x^2-1=0$ has only two solutions.

$x^2-1=0 \Rightarrow x^2=1 \Rightarrow x.x=1 \Rightarrow$ Multiplicate inverse of $x=x$.

So, we have to prove that $1, p-1$ are solutions of $x^2-1=0$ in $Z_p$.

$1 \in Z_p \Rightarrow 1^2-1=1-1=0$

$p-1 \in Z_p \Rightarrow (p-1)^2-1=p^2-2p+1-1=p^2-2p$

$= p(p-2)=0.(p-2)=0 \quad (\because\ p=0 \pmod p)$

**Ex. 6.** *In a ring* $R$ *with unity if* $a \in R$ *has multiplicative inverse then* $a \in R$ *is not a zero divisor.*

**Sol.** $a \in R$ has multiplicative inverse

$\Rightarrow$ There exists $a^{-1} \in R$, such that $aa^{-1}=a^{-1}a=1$, where $1 \in R$ is the unity element.

To prove that $a \in R$ is not a zero divisor we have to prove that

for $b \in R$ so that $ab=0$ or $ba=0 \Rightarrow b=0$ only.

$ab=0 \Rightarrow a^{-1}(ab)=a^{-1}0 \Rightarrow 1b=0 \Rightarrow b=0$; $ba=0 \Rightarrow (ba)\,a^{-1}=0a^{-1} \Rightarrow b1=0 \Rightarrow b=0$

$\therefore$ $a \in R$ is not a zero divisor.

**Ex. 7.** *Construct a field of two elements.*

**Sol.** Let $F=\{0,1\}$ and addition $(+)$, multiplication $(\bullet)$ in $F$ be defined as follows :

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

,

| $\bullet$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Clearly, $+$ and $\bullet$ are binary operations in $F$.

We have $0+1=1+0$ and $0.1=1.0$ and hence $+, \bullet$ are commutative.

The two operations are associative.

$0 \in F$ is the zero element and $1 \in F$ is the unity element.

Clearly, distributivity is also true.

Additive inverse of $0=0$, additive inverse of $1=1$.

Multiplicative inverse of $1 \neq 0 \in F$ is 1. Hence $(\{0,1\}, +, \bullet)$ is a field.

**Ex. 8.** *Show that the set* $R$ *of all real - valued continuous functions defined on* $[0,1]$ *is a commutative ring with unity, with respect to addition* $(+)$ *and multiplication* $(\bullet)$ *of functions defined as*

$(f+g)(x)=f(x)+g(x)$ *and* $(f.g)(x)=f(x).g(x)\ \forall\ x \in [0,1]$ *and* $f, g \in R$.

**Sol.** $f, g$ are real - valued continuous functions on $[0,1] \Rightarrow (i)$ $f+g$ and $f.g$ are real - valued continuous functions on $[0,1]$ and $(ii)$ $f(x), g(x)$ are real numbers for $x \in [0,1]$.

$\therefore$ Addition and multiplication of functions are binary operations in $R$.

Let $f, g, h \in R \quad \forall\, x \in [0,1], ((f+g)+h)(x) = (f+g)(x) + h(x) = (f(x) + g(x)) + h(x)$

$= f(x) + (g(x) + h(x)) = f(x) + (g+h)(x) = (f + (g+h))(x)$

$\therefore\ (f+g)+h = f+(g+h)\ \forall\ f, g, h \in R$

If $O(x) = 0\ \forall\ x \in [0,1]$ then $O$ is a real valued continuous function. Therefore there exists $O \in R$ so that $(f+O)(x) = f(x) + O(x) = f(x)\ \forall\ x \in [0,1]$ and $f \in R$.

If $f$ is a real - valued continuous function on $[0,1]$ then '$-f$' is also a real - valued continuous function so that $(-f)(x) = -f(x)\ \forall\ x \in [0,1]$.

Therefore for $f \in R$ there exists $-f \in R$

so that $(f + (-f))(x) = f(x) - f(x) = 0 = O(x)\ \forall\ x \in [0,1]$

That is, additive inverse exists $\forall\ f \in R$. $\quad\therefore\ (R, +)$ is a commutative group.

$\forall\ x \in [0,1]; ((fg)h)(x) = (fg)(x)\, h(x) = (f(x)\, g(x))\, h(x)$

$= f(x)(g(x)\, h(x)) = f(x)(gh)(x) = (f(gh))(x)$

$\therefore (fg)h = f(gh)\ \forall\ f, g, h \in R$

$\forall x \in [0,1]; (f(g+h))(x) = f(x)(g+h)(x) = f(x)(g(x) + h(x))$

$= f(x)\, g(x) + f(x)\, h(x) = (fg)(x) + (fh)(x) = (fg + fh)(x)$

$\therefore\ f(g+h) = fg + fh\ \forall\ f, g, h \in R$

Similarly $(g+h)f = gf + hf \quad \forall\ f, g, h \in R$. Hence $(R, +, \bullet)$ is a ring.

$\forall\ x \in [0,1], (fg)(x) = f(x)\, g(x) = g(x) f(x) = (gf)(x)$

$\therefore fg = gf\ \forall\ f, g \in R$. $\quad\therefore\ R$ is a commutative ring.

The constant function $e(x) = 1\ \forall\ x \in [0,1]$ is real valued and continuous.

Also $e \in R$ is such that $(ef)(x) = e(x) f(x) = f(x)\ \forall\ x \in [0,1]$

$\therefore\ e \in R$ defined as above is the unity element.

**Ex. 9.** *Prove that the set* $Z[i] = \{a + bi \mid a, b \in Z, i^2 = -1\}$ *of Gaussian integers is an integral domain with respect to addition and multiplication of numbers. Is it a field ?*

**(*S. V. U. 01, O.U. 01, N.U. 04*)**

**Sol.** Let $Z(i) = \{a + bi \mid a, b \in Z\}$.

Let $x, y \in Z(i)$ so that $x = a + bi, y = c + di$ where $a, b, c, d \in Z$

$x+y=(a+c)+(b+d)\,i=a_1+b_1 i$ where $a_1=a+c, b_1=b+d\in Z$

$x\,.\,y=(ac-bd)+(ad+bc)\,i=a_2+b_2 i$ where $a_2=ac-bd$, $b_2=ad+bc\in Z$

$\therefore$ $+, \bullet$ are binary operations in $Z\,(i)$.

Since the elements of $Z\,(i)$ are complex numbers we have that

$(i)$ addition and multiplication are commutative in $Z\,(i)$,

$(ii)$ addition and multiplication are associative in $Z\,(i)$ and

$(iii)$ multiplication is distributive over addition in $Z\,(i)$.

Clearly zero element $=0+0i=0$ and unity element $=1+0i=1$.

Further, for every $x=a+ib\in Z\,(i)$ we have $-x=(-a)+i\,(-b)\in Z\,(i)$

so that $x+(-x)=\{a+(-a)\}+i\,\{b+(-b)\}=0+i0=0$

$\Rightarrow$ Additive inverse exists. $\therefore$ $Z\,(i)$ is a commutative ring with unity element.

For $x, y\in Z\,(i), x\,.\,y=0\Rightarrow x=0$ or $y=0$ since $x, y$ are complex numbers.

Hence $Z\,(i)$ is an integral domain with unity element.

For $\alpha=3+4i\neq 0\in Z\,(i)$ we have $\beta=\frac{3}{25}-i\frac{4}{25}$ so that

$\alpha\,.\,\beta=\left(\frac{9}{25}+\frac{16}{25}\right)+i\left(\frac{-12}{25}+\frac{12}{25}\right)=1+i0=1$. But $\beta\notin Z\,(i)$ as $\frac{3}{25}, -\frac{4}{25}\notin Z$.

So, every non - zero element of $Z\,(i)$ is not invertible. $\therefore$ $Z\,(i)$ is not a field.

**Ex. 10.** *Prove that* $Q[\sqrt{2}]=\{a+b\sqrt{2}\,|\,a,b\in Q\}$ *is a field with respect to ordinary addition and multiplication of numbers.* **(*A. N. U. 12, S. V. U. 00, K. U. 05*)**

**Sol.** Let $x, y, z\in Q[\sqrt{2}]$ so that

$x=a_1+b_1\sqrt{2},\ y=a_2+b_2\sqrt{2},\ z=a_3+b_3\sqrt{2}$ where $a_1, b_1, a_2, b_2, a_3, b_3\in Q$

$x+y=(a_1+a_2)+(b_1+b_2)\sqrt{2}=a+b\sqrt{2}$ where $a_1+a_2=a, b_1+b_2=b\in Q$

$x\,.\,y=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}=c+d\sqrt{2}$ where $c=a_1a_2+2b_1b_2\in Q$

and $d=a_1b_2+a_2b_1\in Q$

$\therefore$ Addition $(+)$ and multiplication $(\bullet)$ of numbers are binary operations in $Q[\sqrt{2}]$.

$x+y=(a_1+a_2)+(b_1+b_2)\sqrt{2}=(a_2+a_1)+(b_2+b_1)\sqrt{2}$

$=(a_2+b_2\sqrt{2})+(a_1+b_1\sqrt{2})=y+x\Rightarrow$ Addition is commutative.

$(x+y)+z=(a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{2}$

and $x+(y+z)=(a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{2}$

$\Rightarrow (x+y)+z=x+(y+z)\Rightarrow$ Addition is associative.

For $0\in Q$ we have $0+0\sqrt{2}=0\in Q[\sqrt{2}]$ so that

$x+0=x$ for $x\in Q[\sqrt{2}]\Rightarrow 0\in Q[\sqrt{2}]$ is the zero element.

For $x=a_1+b_1\sqrt{2}\in Q[\sqrt{2}]$ we have

$-x=(-a_1)+(-b_1)\sqrt{2}\in Q[\sqrt{2}]$ so that $x+(-x)=0\Rightarrow$ Additive inverse exists.

$\therefore$ $(Q[\sqrt{2}],+)$ is a commutative group.

$x\,.\,y=(a_1+b_1\sqrt{2})\,.\,(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$

$=(a_2a_1+2b_2b_1)+(a_2b_1+b_2a_1)\sqrt{2}=y\,.\,x\Rightarrow$ Multiplication is commutative.

$(x\,.\,y)\,.\,z=(\overline{a_1a_2+2b_1b_2}+\overline{a_1b_2+a_2b_1}\sqrt{2})\,.\,(a_3+b_3\sqrt{2})$

$=(a_1a_2a_3+2b_1b_2a_3+2a_1b_2b_3+2a_3b_1b_3)+(a_1a_2b_3+2b_1b_2b_3+a_1a_3b_2+a_2a_3b_1)\sqrt{2}$

and $x\,.\,(y\,.\,z)=(a_1+b_1\sqrt{2})\,(\overline{a_2a_3+2b_2b_3}+\overline{a_2b_3+a_3b_2}\sqrt{2})$

$=(a_1a_2a_3+2a_1b_2b_3+2a_2b_1b_3+2a_3b_1b_2)+(a_1a_2b_3+a_1a_3b_2+a_2a_3b_1+2b_1b_2b_3)\sqrt{2}$

$\therefore$ $(x\,.\,y)\,.\,z=x\,.\,(y\,.\,z)\Rightarrow$ Multiplication is associative.

$x\,.\,(y+z)=(a_1+b_2\sqrt{2})\,(\overline{a_2+a_3}+\overline{b_2+b_3}\sqrt{2})$

$=(a_1a_2+a_1a_3+2b_1b_2+2b_1b_3)+(a_1b_2+a_1b_3+a_2b_1+a_3b_1)\sqrt{2}$

and $x\,.\,y+x\,.\,z=(\overline{a_1a_2+2b_1b_2}+\overline{a_1b_2+a_2b_1}\sqrt{2})+(\overline{a_1a_3+2b_1b_3}+\overline{a_1b_3+a_3b_1}\sqrt{2})$

$=(a_1a_2+2b_1b_2+a_1a_3+2b_1b_3)+(a_1b_2+a_2b_1+a_1b_3+a_3b_1)\sqrt{2}$

$\therefore$ $x\,.\,(y+z)=x\,.\,y+x\,.\,z\Rightarrow$ Distributivity is true. Hence $(Q[\sqrt{2}],+,\bullet)$ is a ring.

$1=1+0\sqrt{2}\in Q[\sqrt{2}]$ so that $x\,.\,1=(a_1+b_1\sqrt{2})\,(1+0\sqrt{2})=x\;\forall\;x\in Q[\sqrt{2}]$.

$\therefore$ $Q[\sqrt{2}]$ is a commutative ring with unity element.

To show that $Q[\sqrt{2}]$ is a field we have to prove further every non-zero element in $Q[\sqrt{2}]$ has multiplicative inverse.

Let $a+b\sqrt{2}\in Q[\sqrt{2}]$ and $a\neq 0$ or $b\neq 0$

Then $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}=\left(\dfrac{a}{a^2-2b^2}\right)+\left(\dfrac{-b}{a^2-2b^2}\right)\sqrt{2}$

since $a^2-2b^2\neq 0$ for $a\neq 0$ or $b\neq 0$. $\quad a,b\in Q\Rightarrow \dfrac{a}{a^2-2b^2},\dfrac{-b}{a^2-2b^2}\in Q$

For $a+b\sqrt{2}\neq 0\in Q[\sqrt{2}]$ there exists $\left(\dfrac{a}{a^2-2b^2}\right)+\left(\dfrac{-b}{a^2-2b^2}\right)\sqrt{2}\in Q[\sqrt{2}]$ such that

$(a+b\sqrt{2})\left[\left(\dfrac{a}{a^2-2b^2}\right)+\left(\dfrac{-b}{a^2-2b^2}\right)\sqrt{2}\right]=1=1+0\sqrt{2}$

$\therefore$ Every non-zero element of $Q[\sqrt{2}]$ is invertible. Hence $Q[\sqrt{2}]$ is a field.

**Ex. 11.** *If $Z$ = the set of integers then prove that the set $z\times z=\{(m,n)\,|\,m,n\in z\}$ with respect to addition $(+)$ and multiplication $(\bullet)$ defined as*

$(m_1,n_1)+(m_2,n_2)=(m_1+m_2,n_1+n_2)$ *and* $(m_1,n_1).(m_2,n_2)=(m_1m_2,n_1n_2)$

$\forall\ (m_1,n_1),(m_2,n_2)\in z\times z$ is a ring and not an integral domain.

**Sol.** Let $x=(m_1,n_1), y=(m_2,n_2), z=(m_3,n_3)\in z\times z$ so that $m_1,n_1,m_2,n_2,m_3,n_3\in Z$

(1) $x+y=(m_1,n_1)+(m_2+n_2)=(m_1+m_2,n_1+n_2)\in z\times z$

$x\,.\,y=(m_1,n_1)\,.\,(m_2,n_2)=(m_1m_2,n_1n_2)\in z\times z$ as $m_1+m_2,n_1+n_2,m_1m_2,n_1n_2\in z$

$\therefore$ $+$ and $\bullet$ are binary operations in $z\times z$

(2) $x+y=(m_1+m_2,n_1+n_2)=(m_2+m_1,n_2+n_1)=y+x$

and $x\,.\,y=(m_1m_2,n_1n_2)=(m_2m_1,n_2n_1)=yx$ $\Rightarrow$ $+$ and $\bullet$ are commutative.

(3) $(x+y)+z=(m_1+m_2,n_1+n_2)+(m_3,n_3)$

$=(\overline{m_1+m_2}+m_3,\overline{n_1+n_2}+n_3)=(m_1+\overline{m_2+m_3},n_1+\overline{n_2+n_3})=x+(y+z)$

$(x\,.\,y)\,.\,z=(m_1m_2,n_1n_2)\,.\,(m_3,n_3)=((m_1m_2)\,m_3,(n_1,n_2)\,n_3)$

$=(m_1(m_2m_2),n_1(n_2n_3))=x\,.\,(y\,.\,z)$ $\Rightarrow$ $+$ and $\bullet$ are associative.

(4) $x\,.\,(y+z)=(m_1,n_1)\,.\,(m_2+m_3,n_2+n_3)$

$=(m_1(m_2+m_3),n_1(n_2+n_3))=(m_1m_2+m_1m_3,n_1n_2+n_1n_3)$

$=(m_1m_2,n_1n_2)+(m_1m_3,n_1n_3)=x\,.\,y+x\,.\,z$

Since multiplication is commutative, $(y+z)\,.\,x=y\,.\,x+z\,.\,x$

$\therefore$ Distributivity is true.

(5) For $0\in z$ we have $(0,0)\in z\times z$ and $(m,n)+(0,0)=(m+0,n+0)=(m,n)$

$\therefore$ $(0,0)\in z\times z$ is the zero element.

(6) For $1\in z$ we have $(1,1)\in z\times z$ and $(m,n)\,.\,(1,1)=(m\,.\,1,n\,.\,1)=(m,n)$

$\therefore$ $(1,1)\in z\times z$ is the unity element. Hence $z\times z$ is a commutative ring with unity.

But we have, $(0,1),(1,0)\in z\times z$ and $(0,1)\neq(0,0)$, $(1,0)\neq(0,0)$

such that $(0,1)\,.\,(1,0)=(0\,.1,1\,.\,0)=(0,0)$

$\therefore$ $(0,1),(1,0)$ are zero divisors in $z\times z$. Hence $z\times z$ is not an integral domain.

## EXERCISE 9 ( *b* )

**1.** List all zero divisors in the ring $Z_{20}$. Also find the units in $Z_{20}$. Is there any relationship between zero divisors and units.

**2.** Solve the equation $3x=2$ in (*a*) $Z_7$ (*b*) $Z_{23}$

**3.** (*a*) Find all solutions of $x^3-2x^2-3x=0$ in $Z_{12}$. ***(O. U. 08, 12)***

(*b*) Find all solutions of $x^2+x-6=0$ in $Z_{14}$. ***(K. U. 11)***

**4.** Describe all units in (*a*) $Z_4$ (*b*) $Z_5$

**5.** Prove that $Z_2 \times Z_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ under componentwise addition and multiplication is a Boolean ring.

**6.** Find all solutions of $a^2 + b^2 = 0$ in $Z_7$.

**7.** Write the multiplication table for $Z_3[i] = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$.

**8.** R is a set of real numbers. Show that $R \times R$ forms a field under addition and multiplication defined by $(a,b)+(c,d) = (a+c, b+d)$ and $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$ is a field.

(**Hint.** $R \times R = C = \{a+ib \mid a,b \in R, i^2 = -1\}$) ***(S. V. U. 07)***

**9.** If Z is the set of all integers and addition $\oplus$, multiplication $(\times)$ are defined in Z as $a \oplus b = a+b-1$ and $a \times b = a+b-ab \ \forall\ a, b \in Z$ then prove that $(Z, \oplus, \times)$ is a commutative ring.

**10.** Let $(R,+)$ be an abelian group. If multiplication $(\bullet)$ in R is defined as $a \,.\, b = 0$, '0' is the zero element in R, $\forall\ a, b \in R$ then prove that $(R, +, \bullet)$ is a ring.

**11.** If $R = \{0, 1, 2, 3, 4\}$ prove that $(R, +_5, \times_5)$ under addition and multiplication modulo - 5 is a field. ***(S. V. U. 99)***

**12.** Give examples of (1) a commutative ring with unity (2) an integral domain and (3) Division ring. ***(N. U. 97)***

**13.** If R = the set of all even integers and (+) is ordinary addition and multiplication $(*)$ is defined as $a * b = \frac{ab}{2} \ \forall\ a, b \in R$ then prove that $(R, +, *)$ is a commutative ring.

**14.** S is a non-empty set containing n elements. Prove that P(S) forms finite Boolean ring w.r.t '+' and '•' defined as $A + B = (A \cap B) - (A \cup B)$ and $A \cdot B = A \cap B \ \forall\ A, B \in P(S)$. Find addition and multiplication tables when $S = \{a, b\}$.

**15.** If $R_1, R_2, ....., R_n$ are rings, then prove that $R_1 \times R_2 \times ..... \times R_n = \{(r_1, r_2, ....., r_n) \mid r_i \in R_i\}$ forms a ring under componentwise addition and multiplication, that is, $(a_1, a_2, ....., a_n) + (b_1, b_2, ....., b_n) = (a_1 + b_1, a_2 + b_2, ...., a_n + b_n)$ and $(a_1, a_2, ....., a_n) \cdot (b_1, b_2, ....., b_n) = (a_1 b_1, a_2 b_2, ...., a_n b_n)$

## 9. 8. INTEGRAL MULTIPLES AND INTEGRAL POWERS OF AN ELEMENT

**Integral multiples :** Let $(R, +, \cdot)$ be a ring and $a \in R$.

We define $0\,a = O$ where '0' is the integer and O is the zero element of the ring.

If $n \in N$ we define $n\,a = a + a + ... + a$, ( $n$ terms ).

If $n$ is negative integer, $n\,a = (-a) + (-a) + ... + (-a)$, ( $-n$ terms ).

$(-n)\,a = (-a) + (-a) + ... + (-a)$, $n$ terms $= n\,(-a) = -(na)$ where $n \in N$.

The set $\{n\,a \mid n \in Z, a \in R\}$ is called the set of integral multiples of an element '$a$'.

It may be noted that for $n \in Z, a \in R$ we have $na \in R$.

**Theorem.** If $m, n \in Z$ and $a, b \in R$, a ring, then $(i)$ $(m+n)a = ma + na$, $(ii)$ $m(na) = (mn)a$, $(iii)$ $m(a+b) = ma + mb$ and $(iv)$ $m(ab) = (ma)b$.

( Proof is left as an exercise )

**Note 1.** If the ring R has unity element then for $n \in Z$ and $a \in R$ we have $na = n(1a) = (n1)a$.

**2.** If $m, n \in Z$ and $a, b \in R$, a ring then we have

$(ma)(nb) = m\{a(nb)\} = m\{(na)b\} = m\{n(ab)\} = (mn)(ab)$.

**Integral powers :** Let $(R, +, \cdot)$ be a ring and $a \in R$.

For $n \in N$ we write $a^n = a.a \ldots a$ ( $n$ times ).

It may be noted that $a^n = a^{n-1}.a$.

**Theorem.** If $m, n \in N$ and $a, b \in R$, a ring then $(i)$ $a^m.a^n = a^{m+n}$ and $(ii)$ $(a^m)^n = a^{mn}$.

( Proof is left as an exercise )

## 9. 9. IDEMPOTENT ELEMENT AND NILPOTENT ELEMENT OF A RING

**Definition.** *In a ring R, if $a^2 = a$ for $a \in R$ then 'a' is called* ***idempotent element of R*** *with respect to multiplication.* ***(S. V. U. 01)***

**Theorem. 1.** ***If $a \neq 0$ is an idempotent element of an integral domain with unity then a = 1.***

**Proof.** Let $(R, +, \cdot)$ be an integral domain.

$a \neq 0 \in R$ is an idempotent element $\Rightarrow a^2 = a \quad \Rightarrow a^2 = a1 \quad (\because a1 = a)$

$\Rightarrow a^2 - a1 = 0 \Rightarrow a(a-1) = 0$ ('0' is the zero element)

$\Rightarrow a - 1 = 0$ since R has no zero divisors $\Rightarrow a = 1$.

**Note. 1.** An integral domain with unity contains only two idempotent elements '0' and '1'.

**2.** A division ring contains exactly two idempotent elements.

**3.** Product of two idempotent elements in a commutative ring R is idempotent.

For, $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb)$

$= a^2b^2 = ab$ for $a, b \in R$ which are idempotent.

**Definition.** *Let R be a ring and $a \neq 0 \in R$. If there exists $n \in N$ such that $a^n = 0$ then 'a' is called* ***nilpotent element of R.***

**Theorem. 2.** ***An integral domain has no nilpotent element other than zero.*** ***(A. U. 08)***

**Proof.** Let R be an integral domain and $a \neq 0 \in R$.

we have $a^1 = a \neq 0$, $a^2 = a.a \neq 0$ since R has no zero divisors.

Let $a^n \neq 0$ for $n \in N$.

Then $a^{n+1} = a^n . a \neq 0$, since R has no zero divisors.

$\therefore$ By induction, $a^n \neq 0$ for every $n \in N$.

Hence $a \neq 0 \in R$ is not a nilpotent element.

**e.g. 1.** In the ring $(Z_6, +, \cdot)$, $\bar{3}$ and $\bar{4}$ and idempotent elements, for $\bar{3}^2 = \bar{3}$ and $\bar{4}^2 = \bar{4}$.

**e.g. 2.** In the ring $(Z_8, +, \cdot)$, there are no idempotent elements.

**e.g. 3.** In the ring $(Z_8, +, \cdot)$, $\bar{2}$ and $\bar{4}$ are nilpotent elements, for $\bar{2}^3 = \bar{0}$ and $\bar{4}^2 = \bar{0}$.

**e.g. 4.** In the ring $(Z_6, +, \cdot)$ there are no nilpotent elements.

**Ex. 1.** If *a, b* are nilpotent elements in a commutative ring R then prove that $a+b, a.b$ are also nilpotent elements.

**Sol.** $a, b \in R$ are nilpotent elements

$\Rightarrow$ there exists $m, n \in N$ such that $a^m = 0, b^n = 0$. We have

$$(a+b)^{m+n} = a^{m+n} + (m+n) C_1 . a^{m+n-1} . b + \ldots + (m+n) C_n . a^m . b^n + \ldots + \ldots + b^{m+n}$$

$$= a^m \{a^n + (m+n) C_1 a^{n-1} . b + (m+n) C_2 . a^{n-2} . b^2 + \ldots + (m+n) C_n . b^n\}$$

$$+ \{(m+n) C_{n+1} . a^{m-1} . b + (m+n) C_{n+2} . a^{m-2} . b^2 + \ldots + b^m\} b^n = 0 \quad (\because a^m = 0 = b^n)$$

Also, $(ab)^{mn} = a^{mn} . b^{mn} = (a^m)^n (b^n)^m = 0$ ($\because$ R is commutative)

$\therefore$ $a+b$ and $a.b$ are nilpotent elements.

## 9.10. CHARACTERISTIC OF A RING

**Definition.** *The characteristic of a ring R is defined as the least positive integer p such that $pa = 0$ for all $a \in R$. In case such a positive integer p does not exist then we say that the characteristic of R is zero or infinite.* **(S. V. U. 00)**

**Note 1.** If R is a ring and $Z = \{ n \in N \mid na = 0 \; \forall \; a \in R \} \neq \phi$ then the least element in Z is the characteristic of R.

**2.** If the ring R has characteristic zero then $ma = 0$ where $a \neq 0$ can hold only if $m = 0$.

**3.** If the characteristic of a ring R is not zero then we say that the characteristic of R is finite.

**4.** As the integral domain, division ring and field are also rings characteristic has meaning for these structures.

**Imp.** If for some $a \in R$, $pa \neq 0$ then characteristic of $R \neq p$.

Characteristic of a ring $R = p \Rightarrow pa = 0 \; \forall \; a \in R$.

**e.g. 1**. R = { 0, 1, 2, 3, 4, 5, 6 } $= Z_7$ is a ring under addition and multiplication modulo 7. Zero element of R = 0.

$\forall \; a \in R$ we have $7a \equiv 0 \pmod 7 \Rightarrow 7a = 0 \; \forall \; a \in R$.

Further for $1 \in R$, $p(1) = p \neq 0$ where $p \neq 0$ and $0 < p < 7$

$\therefore$ 7 is the least positive integer so that $7a = 0 \; \forall \; a \in R \Rightarrow$ Characteristic of R = 7.

**e.g. 2.** The characteristic of the ring $(Z, +, \cdot)$ is zero. For, there is no positive integer $n$ so that $na = 0$ for all $a \in Z$.

**e.g. 3.** If $R \neq \{0\}$ and characteristic of R is not zero then characteristic of R > 1.

Characteristic of $R = 1 \Rightarrow 1a = 0 \; \forall \; a \in R \Rightarrow a = 0 \; \forall \; a \in R \Rightarrow R = \{0\}$.

**e.g. 4.** For any element $x \in Z_3[i]$ ring, we have $3x = 0 \; \forall \; x \in Z_3[i] \Rightarrow$ characteristic of $Z_3[i] = 3$.

**e.g. 5.** In the ring $R = \{0,3,6,9\} \subset Z_{12}, 4x = 0 \; \forall \; x \in R$ and '4' is the least positive integer.

$\therefore$ Characteristic of $R = \{0,3,6,9\} = 0$

**Theorem 1.** ***If R is a ring with unity element, then R has characteristic $p > 0$ if and only if p is the least positive integer such that $p1 = 0$.***

**Proof.** Let characteristic of $R = p \; (> 0)$

By definition, $pa = 0 \; \forall \; a \in R$. In particular $p1 = 0$.

**Conversely,** let $p$ be the least positive integer such that $p1 = 0$.

$\therefore \; q < p$ and $q \in N \Rightarrow q1 \neq 0$. Then for any $a \in R$ we have

$p \,.\, a = a + a + ... + a$ ( $p$ terms ) $= a(1 + 1 + ... + 1) = a(p1) = a\,0 = 0$.

$\therefore \; p$ is the least positive integer so that $p \,.\, a = 0 \; \forall \; a \in R$. $\therefore$ Characteristic of $R = p$.

**Theorem 2.** ***The characteristic of a ring with unity element is the order of the unity element regarded as a member of the additive group.*** ***(K. U. 12)***

**Proof.** Let $(R, +, \cdot)$ be a ring so that $(R, +)$ is its additive group.

**Case 1.** Let $O(1) = 0$ when the unity element 1 is regarded as an element of $(R, +)$. By the definition of order of an element in a group, there exists no positive integer $n$ so that $n\,1 = 0$.

$\therefore$ Characteristic of R = 0.

**Case 2.** Let $O(1) = p \; (\neq 0)$.

By the definition of order of element in a group, $p$ is the least positive integer, so that $p1 = 0$. For any $a \in R$, $pa = p(1a) = (p1)\,a = 0a = 0$

$\therefore$ Characteristic of $R = p$.

**e.g.** For the commutative ring $Z \times Z$, the zero element $= (0,0)$ and the unity element $= (1,1)$. By the definition of order of an element in the additive group $Z \times Z$, there exists no positiveinteger $m$ such that $m(1,1) = (m,m) = (0,0)$.

Therefore characterestic of $Z \times Z$ is zero.

**Theorem 3.** ***The characteristic of an integral domain is either a prime or zero.*** ***(A.U. 12, A. N. U. 12, O. U. 04, S. V. U. 00, 01)***

**Proof.** Let $(R, +, \cdot)$ be an integral domain. Let the characteristic of $R = p\ (\neq 0)$.

If possible, suppose that $p$ is not a prime. Then $p = mn$ where $1 < m, n < p$.

$a \neq 0 \in R \Rightarrow a \,.\, a = a^2 \in R$ and $a^2 \neq 0$ ($\because$ R is integral domain )

$pa^2 = 0 \Rightarrow (mn)\, a^2 = 0 \Rightarrow (ma)\,(na) = 0$

$\Rightarrow ma = 0$ or $na = 0$ ($\because$ R is integral domain )

Let $ma = 0$. For any $x \in R$, $(ma)\, x = 0 \Rightarrow a\,(mx) = 0 \Rightarrow mx = 0$ ($\because a \neq 0$)

This is absurd, as $1 < m < p$ and characteristic of R = $p$.

$\therefore$ $ma \neq 0$. Similarly, we can prove that $na \neq 0$.

This is a contradiction and hence $p$ is a prime.

**Theorem 4.** ***The characteristic of a field is either a prime or zero.*** **(*S. V. U. 00*)**

**Proof.** Since every field is an integral domain, by the above theorem the characteristic of a field is either a prime or zero.

**Note. 1.** The characteristic of a division ring is either a prime or zero.

**2.** The characteristic of $Z_p$, where $p$ is a prime, is $p$.

## SOLVED PROBLEMS

**Ex. 2.** The characteristic of an integral domain **$(R, +, \cdot)$** is zero or a positive integer according as the order of any non-zero element of R regarded as a member of the group **$(R, +)$**. **(*O. U. 97*)**

**Sol.** Let $a \in R$ and $a \neq 0$.

**Case (1).**Let $O(a) = 0$ when '$a$' is regarded as a member of (R, + ).

By the definition of order, there exists no positive integer $n$ so that $na = 0$.

$\therefore$ Characteristic of R = 0.

**Case (2).** Let $O(a) = p$.

By the definition of order, $p$ is the least positive integer, so that $pa = 0$.

For any $x \in R$, $pa = 0 \Rightarrow (pa)\, x = 0x \Rightarrow a\,(px) = 0 \Rightarrow px = 0$ since $a \neq 0$.

$\therefore$ $p$ is the least positive integer so that $px = 0\ \forall\ x \in R$.

Hence characteristic of R = $p$.

**Ex. 3.** *If R is a non-zero ring so that* **$a^2 = a\ \forall\ a \in R$** *prove that characteristic of R = 2 or prove that the characteristic of a Boolean ring is 2.* **(*S. K. U. 01, S. V. U 00*)**

**Sol.** Since $a^2 = a\ \forall\ a \in R$, we have $(a+a)^2 = a + a$

$\Rightarrow (a+a)\,(a+a) = a + a \Rightarrow a\,(a+a) + a\,(a+a) = a + a$

$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a \Rightarrow (a+a) + (a+a) = (a+a) + 0 \Rightarrow a + a = 0 \Rightarrow 2a = 0$.

$\therefore$ for every $a \in R$, we have $2a = 0$. Further for $a \neq 0$, $1a = a \neq 0$.

$\therefore$ 2 is the least positive integer so that $2a = 0\ \forall\ a \in R$.

Hence characteristic of R = 2.

**Ex. 4.** *Find the characteristic of the ring* $Z_3 \times Z_4$.

**Sol.** We have $Z_3 = \{0,1,2\}, Z_4 = \{0,1,2,3\}$

$Z_3 \times Z_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),(2,0),(2,1),(2,2),(2,3)\}$

contains 12 ordered pairs as elements. Zero element $(0,0)$ and unity element $= (1,1)$

We have, $1\,(1,1) = (1,1) \neq (0,0)$; $2\,(1,1) = (2,2) \neq (0,0)$;

$3\,(1,1) = (3,3) = (0,3) \neq (0,0)$; $4\,(1,1) = (4,4) = (1,0) \neq (0,0)$;

$5\,(1,1) = (5,5) = (2,1) \neq (0,0)$; $6\,(1,1) = (6,6) = (0,2) \neq (0,0)$;

$7\,(1,1) = (7,7) = (1,3) \neq (0,0)$; $8\,(1,1) = (8,8) = (2,0) \neq (0,0)$;

$9\,(1,1) = (9,9) = (0,1) \neq (0,0)$; $10\,(1,1) = (10,10) = (1,2) \neq (0,0)$;

$11\,(1,1) = (11,11) = (2,3) \neq (0,0)$; $12\,(1,1) = (12,12) = (0,0)$;

$\therefore$ Least positive integer = 12. Hence characteristic of $Z_3 \times Z_4 = 12$.

Also, G. C. D of $3,4 = (3,4) = 1 \Rightarrow$ the additive group $Z_3 \times Z_4$ is isomorphic with $Z_{12}$

$\therefore$ Characteristic of $Z_3 \times Z_4$ = Characteristic of $Z_{12} = 12$.

**Ex. 5.** *If the characteristic of a ring is 2 and the elements a, b of the ring commute prove that* $(a+b)^2 = a^2 + b^2 = (a-b)^2$.

**Sol.** Since characteristic of the ring R = 2 $\Rightarrow 2x = 0 \ \forall \ x \in R$.

$a, b \in R$ commute $\Rightarrow ab = ba$.

$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2 = a^2 + 2ab + b^2$

$a, b \in R \Rightarrow ab \in R$ and $2(ab) = 0$. ($\because$ characteristic of $R = 2$)

$\therefore (a+b)^2 = a^2 + 0 + b^2 = a^2 + b^2$.

Similarly we can prove that $(a-b)^2 = a^2 + b^2$.

**Ex. 6.** *If R is a commutative ring with unity of characteristic = 3 then prove that* $(a+b)^3 = a^3 + b^3 \ \forall \ a, b \in R$

**Sol.** R is a ring with characteristic = 3 $\Rightarrow 3x = 0$, zero element of R $\forall \ x \in R$.

Since R is a commutative ring, by Binomial Theorem, $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$a, b \in R \Rightarrow a^2b, ab^2 \in R \Rightarrow 3a^2b = 0, 3ab^2 = 0$. $\therefore (a+b)^3 = a^3 + b^3$.

## EXERCISE 9 ( *c* )

1. Prove that the characteristic of the ring $Z_n = \{0,1,2,...,n-1\}$ under addition and multiplication modulo *n,* is *n*.
2. Prove that the characteristic of a field is either prime or zero.
3. Prove that the characteristic of a finite integral domain is finite.
4. Prove that any two non-zero elements of an integral domain regarded as the members of its additive group are of the same order.
5. Give examples of a field with zero characteristic and a field with characteristic 5.
6. Find the characteristics of the rings (*i*) 2 Z (*ii*) Z × Z **(*O. U. 08*)**
7. If R is a commutative ring with unity of characteristic = 4 then simplify $(a+b)^4$ for all $a, b \in R$. **(*K. U. 07*)**

**8.** If R is a commutative ring with unity of characteristic = 3
compute and simplify $(i)\ (x+y)^6$ $(ii)\ (x+y)^9\ \forall\ x, y \in R$

**ANSWERS**

**5.** $n\,Z$ ring, $Z_5$ ring **6.** $(i)\ 0$ $(ii)\ 0$. **7.** $a^4+a^3b+ab^3+b^4$

**8.** $(i)\ x^6+2x^3y^3+y^6$ $(ii)\ x^9+y^9$

## 9.11.DIVISIBILITY, UNITS, ASSOCIATES AND PRIMES IN A RING.

**Definition. (Divisor or Factor)** *Let R be a commutative ring and* $a \neq 0, b \in R$. *If there exists* $q \in R$ *such that* $b = aq$ *then 'a' is said to divide 'b'.*

**Notation.** '$a$' divides '$b$' is denoted by $a \mid b$ and '$a$' does not divide '$b$' is denoted by $a \nmid b$.

**Note. 1.** If '$a$' divides '$b$' then we say that **'$a$' is a divisor or factor of '$b$'.**

**2.** For $a \neq 0, 0 \in R$ we have $a \,.\, 0 = 0$ and hence every non-zero element of a ring R is a divisor of '0' = Zero element of R.

**3.** $a \neq 0, b \in R$ and $a \mid b \Leftrightarrow b = aq$ for some $q \in R$.

***e.g.* 1.** In the ring Z of integers ; $3 \mid 15$ and $3 \nmid 7$.

***e.g.* 2.** In the ring Q of rational numbers ; $3 \mid 7$ because there exists $(7/3) \in Q$ such that $7 = 3 \,.\, (7/3)$.

***e.g.* 3.** In a field F, two non-zero elements are divisors to each other.

***e.g.* 4.** In the ring $Z_6, 4 \mid 2$ ; In the ring $Z_8, 3 \mid 7$ and in the ring $Z_{15}, 9 \mid 12$.

***e.g.* 5.** Unit of a ring R divides every element of the ring. If $a \in R$ is a unit then $aa^{-1} = a^{-1}a = 1$ where $a^{-1} \in R$.

For any $b \in R$ we have $b = 1\,b = (a\,a^{-1})\,b = a\,(a^{-1}b) \Rightarrow a \mid b$.

**Theorem. 1.** ***If R is a commutative ring with unity and*** $a, b, c \in R$ ***then***
***(i)*** $a \mid a$ ***(ii)*** $a \mid b$ ***and*** $b \mid c \Rightarrow a \mid c$ ***(iii)*** $a \mid b \Rightarrow a \mid b\,x\ \forall\ x \in R$
***(iv)*** $a \mid b$ ***and*** $a \mid c \Rightarrow a \mid b\,x + c\,y\ \forall\ x, y \in R$.

**Proof.** $(i)$ If $1 \in R$ is the unity element in R then $a = a \,.\, 1$ which implies that $a \mid a$.

$(ii)$ $a \mid b \Rightarrow b = aq_1$ for some $q_1 \in R$ ; $b \mid c \Rightarrow c = b\,q_2$ for some $q_2 \in R$.

Now $c = b\,q_2 = (a\,q_1)\,q_2 = a\,(q_1 . q_2) = a\,q$ where $q = q_1\,q_2 \in R \Rightarrow a \mid c$.

$(iii)$ $a \mid b \Rightarrow b = aq$ for some $q \in R$.

Now $bx = (aq)\,x = a\,(qx) = aq^1$ where $q^1 = qx \in R \Rightarrow a \mid bx$.

$(iv)$ $a \mid b \Rightarrow a \mid bx\ \forall\ x \in R$ ; $a \mid c \Rightarrow a \mid cy\ \forall\ y \in R$

$a \mid bx \Rightarrow bx = aq_1$ for some $q_1 \in R$ ; $a \mid cy \Rightarrow cy = a\,q_2$ for some $q_2 \in R$.

$\therefore\ bx + cy = aq_1 + aq_2 = a\,(q_1 + q_2) = aq$ where $q = q_1 + q_2 \in R \Rightarrow a \mid (bx + cy)$.

**Note.** $a \mid b$ and $a \mid c \Rightarrow a \mid b \pm c$.

**Definition. (Greatest Common Divisor G.C.D)** *Let R be a commutative ring and* $a, b \in R$. $d \in R$ *is said to be greatest common divisor of 'a' and 'b' if*

*(i)* $d \mid a$ *and* $d \mid b$ *and (ii) whenever* $c \mid a$ *and* $c \mid b$ *where* $c \in R$ *then* $c \mid d$.

**Notation.** If '*d*' is a greatest common divisor (G. C. D) of '*a*' and '*b*' then we write $d = (a, b)$.

**Definition. (Unit)** *Let R be a commutative ring with unity. An element* $a \in R$ *is said to be a unit in R if there exists an element* $b \in R$ *such that* $ab = 1$ *in R. However, the unity element '1' is also a unit because 1 . 1 =1.*

**2.** In a ring, unity element is unique, while, units may be more than one.

**3.** If $ab = 1$ then $a^{-1} = b$. So, a unit in a ring R is an element of the ring so that its multiplicative inverse is also in the ring. That is $a \in R$ is a unit of R means that the element '*a*' is invertible.

**4.** Units of a ring are infact the two divisors of unity element in the ring..

**5.** '*a*' is a unit in $R \Rightarrow ab = 1$ for some $b \in R \Rightarrow$ '*b*' is also a unit of R.

***e.g.*** In a field F, every non-zero element has multiplicative inverse. So, every non-zero element in a field is a unit.

**Theorem 2.** ***Let D be an integral domain. For*** $a, b \in D$, ***if both*** $a \mid b$ ***and*** $b \mid a$ ***are true then*** $a = ub$ ***where u is a unit in D.***

**Proof.** $a \mid b \Rightarrow b = aq_1$ for some $q_1 \in D$; $b \mid a \Rightarrow a = bq_2$ for some $q_2 \in D$.

$b = aq_1 = (bq_2)\, q_1 = b\,(q_2\, q_1) \Rightarrow 1 = q_2\, q_1$, by using cancellation property in integral domain.

$\therefore\ q_2\, q_1 = 1 \Rightarrow q_2$ is a unit in D. Hence $a = bq_2$ where $q_2$ is a unit in D.

**Definition. (Associates)** *Let R be a commutative ring with unity. Two elements 'a' and 'b' in R are said to be associates if* $b = ua$ *for some unit u in R.*

**Note.** The relation of being associates in a ring R is an equivalence relation in R.

***e.g.*** **1.** If '1' is the unity element in the ring R then '1' is a unit in R. For $a\ (\neq 0) \in R$ we have $a = 1 . a$ and *a, a* are associates in R.

***e.g.*** **2.** In the ring Z of integers, the units are 1 and $-1$ only. For $a \neq 0 \in Z$, we have $a = a . 1$ and $a = (-a)\,(-1)$ only. Therefore, $a \in Z$ has only two associates, namely, $a, -a$.

***e.g.*** **3.** In the ring $Z_6 = \{0,1,2,3,4,5\}$ of integers modulo - 6, the units are 1, 5 only.

For $2 \in Z_6$; $2 \equiv 2 . 1 \pmod 6$ and $2 \equiv 4 . 5 \pmod 6$

$\therefore$ 2 has two associates 2, 4.

**Theorem. 3.** ***In an integral domain D, two non-zero elements*** $a, b \in D$ ***are associates iff*** $a \mid b$ ***and*** $b \mid a$.

**Proof.** From Theorem (2) we see that $a \mid b$ and $b \mid a$

$\Rightarrow$ there exists unit $u \in D$ such that $a = ub \Rightarrow a, b$ are associates.

$a$, $b$ are associates in D $\Rightarrow$ there exists unit $u$ in D such that $a = ub \Rightarrow b \mid a$.

$u$ is unit in D $\Rightarrow$ there exists unit $v \in$ D such that $uv = 1$.

Now $a = ub \Rightarrow va = v(ub) \Rightarrow va = (vu)\, b \Rightarrow va = (1)\, b \Rightarrow b = va \Rightarrow a \mid b$.

Hence $a \mid b$ and $b \mid a$.

**Definition. (Trivial Divisors and Proper Divisors)**

*Let $a \neq 0$ be an element in the integral domain D. The units in D and the associates of 'a' are divisors of 'a'. These divisors of 'a' are called Trivial divisors of 'a'. The remaining divisors of 'a' are called the proper divisors of 'a'.*

***e.g.*** Consider the integral domain $(Z, +, \cdot)$. The units in Z are 1 and $-1$ only.

For $a \neq 0 \in Z$, the trivial divisors are $1, -1, a, -a$ only. The remaining divisors of '$a$' are proper divisors.

$3 \in Z$ has only trivial divisors $\pm 1, \pm 3$ and no proper divisors.

$6 \in Z$ has trivial divisors $\pm 1, \pm 6$ and also proper divisors $\pm 2, \pm 3$.

**Definition. (Prime and Composite elements)**

*Let 'a' be non-zero and non-unit element in an integral domain D. If 'a' has no proper divisors in D then 'a' is called a prime element in D. If 'a' has proper divisors in D then 'a' is called Composite element in D.*

**Note.** $a \in$ D is a prime element and $a = bc$ then one of $b$ or $c$ is a unit in D.

***e.g.*1.** In the integral domain $(Z, +, \cdot)$;

$5 \in Z$ is prime element and $6 \in Z$ is composite element.

***e.g.* 2.** In the integral domain $(Q, +, \cdot)$; $6 \in Q$ is prime element since all its divisors are units.

## SOLVED PROBLEMS

**Ex.1.** *Find all the units of $Z_{12}$ the ring of residue classes modulo 12.* **(*O. U. 04*)**

**Sol.** We have $Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$.

Clearly, the unity element $= \bar{1}$ is a unit.

$\bar{a} \in Z_{12}$ is a unit if there exists $\bar{b} \in Z_{12}$ such that $\bar{a}\,\bar{b} = \bar{1}$.

For $\bar{a}$ = even there is no $\bar{b}$ so that $\bar{a}\,\bar{b} \equiv 1 \pmod{12}$, as $\bar{a}\,\bar{b}$ is even. So we have to verify for $\bar{a}$ = odd.

For $\bar{5} \in Z_{12}$ we have $\bar{5} \times \bar{5} = \bar{1}$; $\bar{7} \in Z_{12}$ we have $\bar{7} \times \bar{7} = \bar{1}$ and $\overline{11} \in Z_{12}$ we have $\overline{11} \times \overline{11} = \bar{1}$.

$\therefore \bar{1}, \bar{5}, \bar{7}$ and $\overline{11}$ are the units in $Z_{12}$.

**Ex.2.** *Prove that $\pm 1, \pm i$ are the only four units in the domain of Gaussian integers.* **(*A. U. 12*)**

**Sol.** $Z[i] = \{a + ib \mid a, b \in Z, i^2 = -1\}$ is the integral domain of Gaussian integers.

$1 + 0i = 1$ is the unity element.

Let $x+iy \in Z[i]$ be a unit. By the definition, there exists $u+iv \in Z[i]$ such that

$(x+iy)(u+iv)=1 \Rightarrow |(x+iy)(u+iv)|=1 \Rightarrow (x^2+y^2)(u^2+v^2)=1$

$\Rightarrow x^2=1,\ y^2=0$ or $x^2=0$ or $y^2=1 \Rightarrow x=\pm 1,\ y=0$ or $x=0,\ y=\pm 1$.

$\therefore \pm 1+0i, 0\pm 1\,i$ *i.e.,* $\pm 1, \pm i$ are the possible units.

**Ex.3.** *Find all the associates of* $(2-i)$ *in the ring of Gaussian integers.* **(*N. U. 97*)**

**Sol.** We have $2-i=(2-i).1$; $2-i=(-2+i).(-1)$; $(2-i)=(-2i-1).i$

and $2-i=(2i+1).(-i)$.

$\therefore 2-i, -2+i, -2i-1$ and $2i+1$ are the associates.

**Ex. 4.** *In the domain of Gaussian integers, prove that the associates of* $a+ib$ *are* $a+ib, -a-ib$, $ia-b, -ia+b$.

**Sol.** Since $\pm 1$ and $\pm i$ are the four units of $Z[i]$, $a+ib=(a+ib).1$;

$a+ib=(-a-ib).(-1)$; $a+ib=(ia-b).(-i)$ and $a+ib=(-ia+b).i$

$\therefore a+ib, -a-ib, ia-b$ and $-ia+b$ are the associates of $a+ib$.

**Ex. 5.** *If D is an integral domain and U is a collection of units in D, Prove that* $(U,\cdot)$ *is a group.*

**Sol.** (Left to the reader)

**Ex. 6.** *Find all units of* $Z_{14}$. **(*O.U. 2011*)**

**Sol.** $Z_{14}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$

Unity element $=1$ is a unit. Since 14 is even, even number in $Z_{14}$ cannot be unit.

For $3 \in Z_{14}$ we have $3.5=15=1 \Rightarrow 3,5$ are units.

For $9 \in Z_{14}$ we have $9.11=99=1 \Rightarrow 9,11$ are units.

For $13 \in Z_{14}$ we have $13.13=169=1 \Rightarrow 13$ is a unit.

**Ex. 7.** *Find all the units in the matrix ring* $M_2(Z_2)$ **(*K.U. 2010*)**

**Sol.** We have $Z_2=\{0,1\}$ so that $0+0=0, 0+1=1+0=1$ and $1+1=0$.

$$M_2(Z_2)=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ where } a,b,c,d \in \{0,1\}$$

Number of elements in $M_2(Z_2)=2^4=16$

Clearly $I_2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unity element and hence an unit.

$A \in M_2(Z_2)$ is a unit in $M_2$ if there exists a $B \in M_2$ such that $AB=I_2$ the unity element. $AB=I_2$ happens when A is non-singular and $B=A^{-1}$.

Hence the units of $M_2(Z_2)$ are all the non-singular matrices.

Matrices having only one '0' and three '1's are :

$\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix}$ which are non-singular

Hence the above 4 matrices are units.

Matrices having two '0's and two '1's are

$\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&1\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}$

Among the above six matrices of $M_2$; $\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}$ are only non-singular.

Hence these two matrices are units.

Matrices having three '0's and one '1' are : $\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}$ which are all singular.

The zero matrix $= O = \begin{pmatrix}0&0\\0&0\end{pmatrix}$ and the matrix having all '1's $\begin{pmatrix}1&1\\1&1\end{pmatrix}$ are both singular.

Hence the units of $M_2(Z_2)$ are $\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix}$ and $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ which are six in number.

## 9.12. SOME NONCOMMUTATIVE EXAMPLES.

There are many rings which are not Commutative under multiplication. We study three non-commutative rings, namely, the ring of square matrices over a field, the ring of endomorphisms of an abelian group and the Quaternions.

## SOLVED PROBLEMS

**Ex. 1.** *Prove that the set of all $2\times2$ matrices over the field of Complex numbers is a ring with unity under addition and multiplication of matrices.*

***(O. U. 04, S. V. U. 00)***

**Sol.** Let $R = \left\{\begin{bmatrix}a&b\\c&d\end{bmatrix} : a,b,c,d \in C\right\}$ be the set of $2\times2$ matrices over C.

Let $A = \begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix} = [a_{ij}]_{2\times2}$, $B = \begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix} = [b_{ij}]_{2\times2}$ and $C = \begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix} = [c_{ij}]_{2\times2}$ be three elements in R.

(1) $A + B = [a_{ij}]_{2\times2} + [b_{ij}]_{2\times2} = [a_{ij} + b_{ij}]_{2\times2}$ and

$A + B = [b_{ij} + a_{ij}]_{2\times2} = B + A$ $\qquad (\because a_{ij}, b_{ij} \in C)$

$\therefore$ Addition is a binary operation and also Commutative.

(2) $(A+B)+C=\left[a_{ij}+b_{ij}\right]_{2\times2}+\left[c_{ij}\right]_{2\times2}=\left[(a_{ij}+b_{ij})+c_{ij}\right]_{2\times2}$

$=\left[a_{ij}+(b_{ij}+c_{ij})\right]_{2\times2}=A+(B+C)\quad(\because a_{ij},b_{ij},c_{ij}\in\mathrm{C})$

$\therefore$ Addition is associative.

(3) We have $\mathrm{O}=\begin{bmatrix}0&0\\0&0\end{bmatrix}=[0]_{2\times2}\in\mathrm{R}$ such that $A+\mathrm{O}=\left[a_{ij}+0\right]_{2\times2}=\left[a_{ij}\right]_{2\times2}=A$

$\therefore\ \mathrm{O}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$ is the Zero element.

(4) For $A=\left[a_{ij}\right]_{2\times2}, a_{ij}\in\mathrm{C}\Rightarrow-a_{ij}\in\mathrm{C}$ so that $a_{ij}+(-a_{ij})=o\in\mathrm{C}$.

$\therefore$ there exists $-A=\left[-a_{ij}\right]_{2\times2}\in\mathrm{R}$ such that $A+(-A)=\left[a_{ij}+(-a_{ij})\right]_{2\times2}=[0]_{2\times2}=\mathrm{O}$.

$\therefore$ ( R, + ) is an abelian group.

(5) Let $A=\left[a_{ij}\right]_{2\times2}, B=\left[b_{jk}\right]_{2\times2}, C=\left[c_{kl}\right]_{2\times2}\in\mathrm{R}$.

From the definition of multiplication ; $AB=\left[a_{ij}\right]\left[b_{jk}\right]=\left[u_{ik}\right]_{2\times2}$

where $u_{ik}=\sum_{j=1}^{2}a_{ij}\,b_{jk}=a_{i1}\,b_{1k}+a_{i2}\,b_{2k}\in\mathrm{C}$

$\therefore$ Multiplication is a binary operation.

(6) $(AB)\,C=\left[\sum_{j=1}^{2}a_{ij}\,b_{jk}\right]_{2\times2}\left[c_{kl}\right]_{2\times2}=\left[\sum_{k=1}^{2}\left(\sum_{j=1}^{2}a_{ij}\,b_{jk}\right)c_{kl}\right]$

$=\left[\sum_{j=1}^{2}a_{ij}\left(\sum_{k=1}^{2}b_{jk}c_{kl}\right)\right]=A\,(BC)$

$\therefore$ Multiplication is associative.

(7) $A\,(B+C)=\left[a_{ij}\right]_{2\times2}\left[b_{jk}+c_{jk}\right]_{2\times2}$

$=\left[\sum_{j=1}^{2}a_{ij}\,(b_{jk}+c_{jk})\right]=\left[\sum_{j=1}^{2}(a_{ij}\,b_{jk}+a_{ij}\,c_{jk})\right]=\left[\sum_{j=1}^{2}a_{ij}\,b_{jk}\right]+\left[\sum_{j=1}^{2}a_{ij}\,c_{jk}\right]=AB+AC$.

Similarly, we can prove that $(B+C)A=BA+CA$. $\therefore$ Distributive laws hold.

Hence $(\mathrm{R},+,\cdot)$ is a ring.

Since $1\in\mathrm{C}$, $I=\begin{bmatrix}1&0\\0&1\end{bmatrix}\in\mathrm{R}$. For $A=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}_{2\times2}$

$A\,I=\begin{bmatrix}a_{11}+0&0+a_{12}\\a_{21}+0&0+a_{22}\end{bmatrix}_{2\times2}=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}=A$. Also $IA=A$.

$\therefore I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the unity element in R.

Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. Then $AB = \begin{bmatrix} 2+0 & 0+2 \\ 2+0 & 0+2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 6 & 4 \end{bmatrix}$

and $BA = \begin{bmatrix} 2+0 & 4+0 \\ 0+4 & 0+4 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 4 & 4 \end{bmatrix}$ so that $AB \neq BA$.

Hence $(\mathrm{R}, +, \cdot)$ is not a commutative ring.

**Notation.** The ring of all $2\times 2$ matrices over the field of complex numbers C is denoted by $\mathrm{M}_2(\mathrm{C})$. If F is a field the ring of all $n\times n$ matrices over F is denoted by $\mathrm{M}_n(\mathrm{F})$. The zero element in $\mathrm{M}_n(\mathrm{F})$ is denoted by $\mathrm{O}_{n\times n}$ and the unity element by $\mathrm{I}_n$.

**Zero divisors in $\mathrm{M}_2(\mathrm{C})$:** $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \mathrm{O}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq \mathrm{O}$.

Then $AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \mathrm{O}$ and $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathrm{O}$.

We observe that $AB \neq BA$ and $A \neq \mathrm{O}, B \neq \mathrm{O} \Rightarrow BA = \mathrm{O}$.

Therefore there exist Zero divisors in $\mathrm{M}_2(\mathrm{F})$ where F is a field.

**Nilpotent element in $\mathrm{M}_2(\mathrm{C})$:**

For $A = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ we have $A^2 = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathrm{O}$.

Therefore A is a nilpotent matrix in $\mathrm{M}_2(\mathrm{C})$.

$B = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$ is also a nilpotent matrix element in $\mathrm{M}_2(\mathrm{C})$.

**Ex.2.** *The set of $2\times 2$ matrices of the form $\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}$ where x, y are complex numbers and $\bar{x}, \bar{y}$ denote the complex conjugates of x y; is a skew field for compositions of matrix addition and multiplication.* **(S. V. U. 00, 03, 05, N. U. 00)**

**Sol.** Let $\mathrm{M} = \left\{ \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} : x = a+ib,\ y = c+id;\ a, b, c, d \in \mathrm{R} \right\}$ be the set of $2\times 2$ matrices.

Let $A = \begin{bmatrix} x_1 & y_1 \\ -\bar{y}_1 & \bar{x}_1 \end{bmatrix}$, $B = \begin{bmatrix} x_2 & y_2 \\ -\bar{y}_2 & \bar{x}_2 \end{bmatrix}$, $C = \begin{bmatrix} x_3 & y_3 \\ -\bar{y}_3 & \bar{x}_3 \end{bmatrix} \in \mathrm{M}$

**(1)** $A+B = \begin{bmatrix} x_1+x_2 & y_1+y_2 \\ -\bar{y}_1-\bar{y}_2 & \bar{x}_1+\bar{x}_2 \end{bmatrix} = \begin{bmatrix} x_1+x_2 & y_1+y_2 \\ -\overline{y_1+y_2} & \overline{x_1+x_2} \end{bmatrix} \in \mathrm{M}$, since

$\overline{Z_1 \pm Z_2} = \bar{Z}_1 \pm \bar{Z}_2$ for $\bar{Z}_1, \bar{Z}_2 \in \mathrm{C}$.

$$A \,.\, B = \begin{bmatrix} x_1 & y_1 \\ -\bar{y}_1 & \bar{x}_1 \end{bmatrix} \begin{bmatrix} x_2 & y_2 \\ -\bar{y}_2 & \bar{x}_2 \end{bmatrix} = \begin{bmatrix} x_1x_2 - y_1\bar{y}_2 & x_1y_2 + y_1\bar{x}_2 \\ -\bar{y}_1x_2 - \bar{x}_1\bar{y}_2 & -\bar{y}_1y_2 + \bar{x}_1\bar{x}_2 \end{bmatrix}$$

If $u = x_1x_2 - y_1\bar{y}_2$ and $v = x_1y_2 + y_1\bar{x}_2$ then $\bar{u} = \bar{x}_1\bar{x}_2 - \bar{y}_1y_2$ and $\bar{v} = \bar{x}_1\bar{y}_2 + \bar{y}_1x_2$

$$\therefore\ A \,.\, B = \begin{bmatrix} u & v \\ -\bar{v} & \bar{u} \end{bmatrix} \in \mathrm{M}.$$

Hence addition (+) and multiplication $(\cdot)$ are binary operations.

**(2)** Clearly $A + B = B + A$ for any $A, B \in \mathrm{M}$.

**(3)** Clearly $(A+B)+C = A+(B+C)$ and $(A \,.\, B) \,.\, C = A \,.\, (B \,.\, C)$ for any $A, B, C \in \mathrm{M}$ because addition and multiplication of matrices are associative.

**(4)** There exists $\mathrm{O} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0+i0 & 0+i0 \\ \overline{-0+i0} & \overline{0+i0} \end{bmatrix} \in \mathrm{M}$ so that $A + \mathrm{O} = A$ for any $A \in \mathrm{M}$.

**(5)** For $A = \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}$ there exists $-A = \begin{bmatrix} -x & -y \\ \bar{y} & -\bar{x} \end{bmatrix}$ so that $A + (-A) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathrm{O}$

(Zero matrix)

**(6)** For any $A, B, C \in \mathrm{M}$, distributive laws, namely, $A \,.\, (B+C) = A \,.\, B + A \,.\, C$ and $(B+C) \,.\, A = B \,.\, A + C \,.\, A$ are clearly true. Hence $(\mathrm{M}, +, \cdot)$ is a ring.

**(7)** We have $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+i0 & 0+i0 \\ \overline{-0+i0} & \overline{1+i\,.\,0} \end{bmatrix} \in \mathrm{M}$ so that $A \,.\, I = I \,.\, A = A$ for any $A \in \mathrm{M}$.

$\therefore$ the ring M has unity element I.

**(8)** Let $A \neq \mathrm{O} \in \mathrm{M}$ so that $A = \begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix} = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$ where

$a, b, c, d$ are not all zero.

$$\text{Det } A = (a+ib)(a-ib) - (c+id)(-c+id) = a^2 + b^2 + c^2 + d^2 \neq 0.$$

Since $\det A \neq 0$, $A \neq \mathrm{O}$ is invertible. Hence $(\mathrm{M}, +, \cdot)$ is a skew field.

**Note.** The matrix $\begin{bmatrix} x & y \\ -\bar{y} & \bar{x} \end{bmatrix}$ is also given as $\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$ in the problem.

## RING OF QUATERNIONS

**Ex. 3.** *Prove that the set of Quaternions is a skew field.* **(*O. U. 05, 04*)**

**Sol.** Let $\mathrm{Q} = \mathrm{R} \times \mathrm{R} \times \mathrm{R} \times \mathrm{R} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathrm{R}\}$ where $i, j, k$ are quaternion units satisfying the relations :

$$i^2 = j^2 = k^2 = i\ j\ k = -1,\ ij = -ji = k,\ jk = -kj = i, ki = -ik = j.$$

Let X, Y, Z $\in$ Q so that $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, $Y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$
and $Z = \gamma_0 + \gamma_1 i + \gamma_2 j + \gamma_3 k$ where $\alpha_t, \beta_t, \gamma_t$ for $t = 0,1,2,3$ are real numbers.
We define $X = Y \Leftrightarrow \alpha_t = \beta_t$ for $t = 0,1,2,3$.
We define addition (+) as $X + Y = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) i + (\alpha_2 + \beta_2) j + (\alpha_3 + \beta_3) k$
and multiplication $(\cdot)$ as

$$X \cdot Y = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2) i$$
$$+ (\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3) j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1) k .$$

(1) $\forall$ X, Y $\in$ Q ; $X + Y = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) i + (\alpha_2 + \beta_2) j + (\alpha_3 + \beta_3) k$
As $\alpha_t + \beta_t$ for $t = 0,1,2,3 \in R$, $X + Y \in Q$. $\therefore$ addition (+) is a binary operation.

(2) $\forall$ X, Y $\in$ Q ; $X + Y = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) i + (\alpha_2 + \beta_2) j + (\alpha_3 + \beta_3) k$
$= (\beta_0 + \alpha_0) + (\beta_1 + \alpha_1) i + (\beta_2 + \alpha_2) j + (\beta_3 + \alpha_3) k = Y + X$
$\therefore$ addition is commutative. ($\because \alpha_t + \beta_t = \beta_t + \alpha_t$ for $t = 0,1,2,3$).

(3) $\forall$ X, Y, Z $\in$ Q ;

$$(X + Y) + Z = \{(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) i + (\alpha_2 + \beta_2) j + (\alpha_3 + \beta_3) k\} + (\gamma_0 + \gamma_1 i + \gamma_2 j + \gamma_3 k)$$
$$= [(\alpha_0 + \beta_0) + \gamma_0] + [(\alpha_1 + \beta_1) + \gamma_1] i + [(\alpha_2 + \beta_2) + \gamma_2] j + [(\alpha_3 + \beta_3) + \gamma_3] k$$
$$= [\alpha_0 + (\beta_0 + \gamma_0)] + [\alpha_1 + (\beta_1 + \gamma_1)] i + [\alpha_2 + (\beta_2 + \gamma_2)] j + [\alpha_3 + (\beta_3 + \gamma_3)] k$$
$$= X + (Y + Z) . \quad (\because (\alpha_t + \beta_t) + \gamma_t = \alpha_t + (\beta_t + \gamma_t) \text{ for } t = 0,1,2,3).$$

$\therefore$ addition is associative.

(4) For $O = 0 + 0i + 0j + 0k \in Q$ and $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ we have
$O + X = (0 + \alpha_0) + (0 + \alpha_1) i + (0 + \alpha_2) j + (0 + \alpha_3) k = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = X = X + O$
$\therefore$ $O = 0 + 0i + 0j + 0k$ is additive identity.

(5) For $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ there exists $-X = (-\alpha_0) + (-\alpha_1) i + (-\alpha_2) j + (-\alpha_3) k \in Q$
such that $X + (-X) = [\alpha_0 + (-\alpha_0)] + [\alpha_1 + (-\alpha_1)] i + [\alpha_2 + (-\alpha_2)] j + [\alpha_3 + (-\alpha_3)] k$
$= 0 + 0i + 0j + 0k = O$, the additive identity.
$\therefore$ every element has additive inverse.
Hence, from (1), (2), (3), (4) and (5) : (Q, + ) is abelian group.

(6) $X \cdot Y = b_0 + b_1 i + b_2 j + b_3 k$ where $b_0 = \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3$
$b_1 = \alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2$, $b_2 = \alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3$
and $b_3 = \alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1$ are real numbers.
$\therefore$ multiplication $(\cdot)$ is a binary operation.

(7) $(X \cdot Y) \cdot Z = (b_0 + b_1 i + b_2 j + b_3 k) \cdot (\gamma_0 + \gamma_1 i + \gamma_2 j + \gamma_3 k)$

$$= (b_0\gamma_0 - b_1\gamma_1 - b_2\gamma_2 - b_3\gamma_3) + (b_0\gamma_1 + b_1\gamma_0 + b_2\gamma_3 - b_3\gamma_2) i + (b_0\gamma_2 + b_2\gamma_0 + b_3\gamma_1 - b_1\gamma_3) j$$
$$+ (b_0\gamma_3 + b_3\gamma_0 + b_1\gamma_2 - b_2\gamma_1) k$$

$Y \cdot Z = c_0 + c_1 i + c_2 j + c_3 k$ where $c_0 = \beta_0\gamma_0 - \beta_1\gamma_1 - \beta_2\gamma_2 - \beta_3\gamma_3$,

$c_1 = \beta_0\gamma_1 + \beta_1\gamma_0 + \beta_2\gamma_3 - \beta_3\gamma_2$, $c_2 = \beta_0\gamma_2 + \beta_2\gamma_0 + \beta_3\gamma_1 - \beta_1\gamma_3$,

$c_3 = \beta_0\gamma_3 + \beta_3\gamma_0 + \beta_1\gamma_2 - \beta_2\gamma_1$.

$X \cdot (Y \cdot Z) = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (c_0 + c_1 i + c_2 j + c_3 k)$

$= (\alpha_0 c_0 - \alpha_1 c_1 - \alpha_2 c_2 - \alpha_3 c_3) + (\alpha_0 c_1 + \alpha_1 c_0 + \alpha_2 c_3 - \alpha_3 c_2)\, i$

$+ (\alpha_0 c_2 + \alpha_2 c_0 + \alpha_3 c_1 - \alpha_1 c_3)\, j + (\alpha_0 c_3 + \alpha_3 c_0 + \alpha_1 c_2 - \alpha_2 c_1)\, k$

Since the corresponding terms of $(X \cdot Y) \cdot Z$ and $X \cdot (Y \cdot Z)$ are equal we have

$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$ $\therefore$ multiplication is associative.

(8) Both the distributive laws, namely, $X \cdot (Y + Z) = X \cdot Y + X \cdot Z$ and

$(Y + Z) \cdot X = Y \cdot X + Z \cdot X$ can be proved to be true.

From the truth of the above 8 properties we establish that $(Q, +, \cdot)$ is a ring.

(9) There exists $1 = 1 + 0i + 0j + 0k \in Q$ such that

$\forall\ X \in Q$ we have $1 \cdot X = (1 + 0i + 0j + 0k) \cdot (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)$

$= (1 \cdot \alpha_0 - 0 \cdot \alpha_1 - 0 \cdot \alpha_2 - 0 \cdot \alpha_3) + (1 \cdot \alpha_1 + \alpha_0 \cdot 0 + 0 \cdot \alpha_3 - 0 \cdot \alpha_2) i$

$+ (1 \cdot \alpha_2 + 0 \cdot \alpha_0 + 0 \cdot \alpha_1 - \alpha_1 \cdot 0)\, j + (1 \cdot \alpha_3 + 0 \cdot \alpha_0 + 0 \cdot \alpha_2 - 0 \cdot \alpha_1) k$

$= \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = X$. Also $X \cdot 1 = X$.

$\therefore\ 1 = 1 + 0i + 0j + 0k \in Q$ is the unity element.

(10) Let $X \neq O$, the zero element. Then not all $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are zero $\in R$.

$\therefore\ \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = \Delta \neq 0 \in R$.

For the real numbers $\frac{\alpha_0}{\Delta}, \frac{-\alpha_1}{\Delta}, \frac{-\alpha_2}{\Delta}, \frac{-\alpha_3}{\Delta}$ there exists

$X^1 = \frac{\alpha_0}{\Delta} - \frac{\alpha_1}{\Delta} i - \frac{\alpha_2}{\Delta} j - \frac{\alpha_3}{\Delta} k \in Q$. Further $X \cdot X^1 = \left(\frac{\alpha_0^2}{\Delta} + \frac{\alpha_1^2}{\Delta} + \frac{\alpha_2^2}{\Delta} + \frac{\alpha_3^2}{\Delta}\right)$

$+ \left(\frac{-\alpha_0\alpha_1}{\Delta} + \frac{\alpha_0\alpha_1}{\Delta} - \frac{\alpha_2\alpha_3}{\Delta} + \frac{\alpha_3\alpha_2}{\Delta}\right) i + \left(\frac{-\alpha_0\alpha_2}{\Delta} + \frac{\alpha_2\alpha_0}{\Delta} - \frac{\alpha_3\alpha_1}{\Delta} + \frac{\alpha_1\alpha_3}{\Delta}\right) j$

$+ \left(\frac{-\alpha_0\alpha_3}{\Delta} + \frac{\alpha_3\alpha_0}{\Delta} - \frac{\alpha_1\alpha_2}{\Delta} + \frac{\alpha_2\alpha_1}{\Delta}\right) k = 1 + 0i + 0j + 0k = 1$, the unity element.

Similarly we can prove that $X^1 \cdot X = 1$.

$\therefore$ every non-zero element of Q has multiplicative inverse.

We have $X \cdot Y = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_0 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2) i$

$+ (\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)\, j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)\, k$

$= b_0 + b_1 i + b_2 j + b_3 k$ and

$$Y \cdot X = (\beta_0\alpha_0 - \beta_1\alpha_1 - \beta_2\alpha_2 - \beta_3\alpha_3) + (\beta_0\alpha_1 + \beta_1\alpha_0 + \beta_2\alpha_3 - \beta_3\alpha_2)i$$

$$+ (\beta_0\alpha_2 + \beta_2\alpha_0 + \beta_3\alpha_1 - \beta_1\alpha_3)j + (\beta_0\alpha_3 + \beta_3\alpha_0 + \beta_1\alpha_2 - \beta_2\alpha_1)k = a_0 + a_1 i + a_2 j + a_3 k .$$

we observe that $b_0 = a_0, b_1 \neq a_1, b_2 \neq a_2, b_3 \neq a_3$.

$\therefore$ multiplication is not commutative.

Hence $(Q, +, \bullet)$ is a Division ring or Skew field.

**Note.1.** We can take 1 = ( 1, 0, 0, 0 ), $i$ = ( 0, 1, 0, 0 ), $j$ = ( 0, 0, 1, 0 ) and $k$ = ( 0, 0, 0, 1 ).

**2.** The set $G = \{\pm 1, \pm i, \pm j, \pm k\}$ form a non abelian group of order 8 under multiplication $(\bullet)$ defined as follows :

$i^2 = j^2 = k^2 = i\,j\,k = -1$ ; $i\,j = -j\,i = k$ ; $j\,k = -k\,j = i$ and $k\,i = -i\,k = j$ .

## RING OF ENDOMORPHISMS OF AN ABELIAN

Let G be an abelian group. A homomorphism of G into itself is an endomorphism of G. The set of all endomorphisms of G is denoted by Hom (G,G) or Hom (G).

For $f, g \in$ Hom (G,G) if we define addition (+) and multiplication $(\bullet)$ of two endomorphisms as $(f + g)(x) = f(x) + g(x)$ and $(f . g)(x) = f(g(x)) \; \forall \; x \in G$ then Hom (G,G) is a ring. ***(A.U. 12, 11)***

(Proof of Hom (G, G) is a ring is left to the student as an exercise)

**Note.** Hom (G, G) is not commutative as the composition of functions is not commutative.

# Subrings, Ideals,Quotient Rings & Euclidean Rings

## 10.1. SUB RINGS

In analogy with the concept of a subgroup of a group we now introduce the concept of a subring. If $(R, +, \bullet)$ is a ring then a non-empty subset of $R$ with the induced operations $+, \bullet$ as in $R$ can be a ring. Such a ring is called a subring of the ring $R$.

**Definition. (Subring).** *Let $(R, +, \bullet)$ be a ring and S be a non-empty subset of R. If $(S, +, \bullet)$ is also a ring with respect to the two operations $+, \bullet$ in R then $(S, +, \bullet)$ is a* ***subring of R.*** ***(O. U. 03, N. U. 95)***

The binary operations in S thus defined are the induced operations in $S$ from $R$.

**Definition.** *Let $(F, +, \bullet)$ be a field and $(S, +, \bullet)$ be a subring of F. If $(S, +, \bullet)$ is a field then we say that S is a subfield of F. If $(S, +, \bullet)$ is an integral domain then we say that S is a subdomain of F.*

**Note. 1.** If $(S, +, \bullet)$ is a subring of the ring $(R, +, \bullet)$ then $(S, +)$ is a subgroup of $(R, +)$ group.**Hence zero element in *R* is also zero element in *S*.**

**2.** If $(S, +, \bullet)$ is a subfield of the field $(F, +, \bullet)$ then $(i)$ $(S, +)$ is a subgroup of $(F, +)$ group and $(ii)$ $(S - \{0\}, \bullet)$ is subgroup of $(F - \{0\}, \bullet)$ group.

**e.g. 1.** The set of even integers is a subring of $(Z, +, \bullet)$ ring or integral domain.

**e.g. 2.** $(Z, +, \bullet)$, $(Q, +, \bullet)$ are subrings of the field of real numbers $(R, +, \bullet)$.

**e.g. 3.** Let $(Q, +, \bullet)$ be the ring of rational numbers. Then $S = \{a/2 \mid a \in Z\}$ is a non-empty subset of $Q$ and $(S, +)$ is a subgroup of the group $(Q, +)$.

But for $1/2 \in S$ we have $(1/2).(1/2) = (1/4) \notin S$ and hence '$\bullet$' is not a binary operation in $S$. Thus $(S, +, \bullet)$ is not a subring of $(Q, +, \bullet)$

**e.g. 4.** Let $(R, +, \bullet)$ be a ring and $0 \in R$ be the zero element of $R$. Then $S = \{0\}$ is a non - empty subset of $R$ so that $(S, +, \bullet)$ is itself a ring. Therefore $(S, +, \bullet)$ is a subring of $R$.

$(\{0\}, +, \bullet)$ is called trivial subring and $(R, +, \bullet)$ is called improper subring of $R$.

**e.g. 5.** For each positive integer $n$, the set $nz = \{0, \pm n, \pm 2n, \pm 3n, .....\}$ is a subring of Z.

**e.g. 6.** The set of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z, i^2 = -1\}$ is a subring of complex number field C.

**Theorem 1. (Subring Test).** *Let $S$ be a non-empty subset of a ring $R$. Then $S$ is a subring of $R$ if and only if $a-b\in S$ and $ab\in S$ for all $a,b\in S$.* **(S.K.U. 01)**

**Proof.** Let $S$ be a subring of $R$.

We now prove that $a-b\in S$ and $ab\in S\ \forall\ a,b\in S$.

Since $S$ is a subring of $R$, $S$ is a ring with respect to the addition and multiplication operations in $R$.

$\therefore\ a,b\in S\Rightarrow a,-b\in S\Rightarrow a+(-b)=a-b\in S$ and $a,b\in S\Rightarrow ab\in S$

Let $a-b\in S$ and $ab\in S\ \forall\ a,b\in S$.

We now prove that $S$ is a ring.

Since $S$ is a non empty subset of the commutative group $(R,+)$ with the condition $a-b\in S\ \ \forall\ a,b\in S$; by group theory $(S,+)$ is a commutative subgroup of $(R,+)$.

Since $ab\in S\ \forall\ a,b\in S$, multiplication $(\bullet)$ is a binary operation in $S$.

Also, $a,b,c\in S\Rightarrow a,b,c\in R\Rightarrow a(bc)=(ab)c$

Further $a,b,c\in S\Rightarrow a,b,c\in R\Rightarrow a(b+c)=ab+ac$ and $(b+c)a=ba+ca$

$\therefore\ (S,+,\bullet)$ is a ring and hence $(S,+,\bullet)$ is a subring of $R$.

**Note.** Every subring contains atleast zero element of the ring.

**Theorem 2. (Subfield Test).** *Let $K$ be a non-empty subset of a field $F$. Then $K$ is a subfield of $F$ if and only if $a,b\in K\Rightarrow a-b\in K$ and $a\in K, b\neq 0\in K\Rightarrow ab^{-1}\in K$.*

(Proof is left as an exercise)

**e.g. 1.** $nZ$ is a subdomain of $Z$.

We know that $(Z,+,\bullet)$ where $Z$ = the set of all integers is an integral domain.

For a fixed $n\in Z$ we have $nZ=\{nx\mid x\in Z\}$

$0\in Z$ is zero element and $n0=0\Rightarrow 0\in nZ$. $\therefore\ nZ\neq\phi$ and $nZ\subset Z$

Let $x, y\in Z$. Then $nx, ny\in nZ$.

$nx-ny=n(x-y)\in nZ$ $(\because\ x-y\in Z)$

Also $(nx)(ny)=n(x\,n\,y)\in nZ$ $(\because\ x\,n\,y\in Z)$ $\therefore\ nZ$ is a subdomain of $Z$.

**e.g. 2.** $Z$ is not a subfield of $Q$. For $2,3\in Z$ and $3\neq 0\Rightarrow 3^{-1}=(1/3)\in Q$.

But $2.3^{-1}=(2/3)\notin Z$.

**e.g. 3.** Unity element of a ring need not be same as the unity element of subring.

Consider $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ the ring with unity element $\bar{1}$.

For the subring $S=\{\bar{0},\bar{2},\bar{4}\}$; we have $\bar{0}.\bar{4}=\bar{4}.\bar{0}=\bar{0}$; $\bar{2}.\bar{4}=\bar{4}.\bar{2}=\bar{2}$; $\bar{4}.\bar{4}=\bar{4}.\bar{4}=\bar{4}$

$\Rightarrow\ \bar{4}$ is the unity element of $S$. Hence unity of $Z_6\neq$ unity of S.

**Theorem 3.** *The intersection of two subrings of a ring R is a subring of R.*
**(S. K. D 08, S. V. U. 08, N. U. 00)**

**Proof.** Let $S_1, S_2$ be two subrings of $R$. Let $0 \in R$ be zero element.

Since every subring contains atleast zero element of the ring, $0 \in S_1$ and $0 \in S_2$.

$\therefore\ 0 \in S_1 \cap S_2$ and hence $S_1 \cap S_2 \neq \phi$ and $S_1 \cap S_2 \subset R$.

Let $a, b \in S_1 \cap S_2$. Then $a, b \in S_1$ and $a, b \in S_2$.

$a, b \in S_1$ and $S_1$ is a subring of $R \Rightarrow a - b \in S_1$ and $ab \in S_1$ .... (1)

$a, b \in S_2$ and $S_2$ is a subring of $R \Rightarrow a - b \in S_2$ and $a, b \in S_2$ .... (2)

From (1) and (2) we have $a, b \in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$

$\therefore\ S_1 \cap S_2$ is a subring of $R$.

## SOLVED PROBLEMS

**Ex. 1.** *Prove that* $S_1 = \{\bar{0}, \bar{3}\}, S_2 = \{\bar{0}, \bar{2}, \bar{4}\}$ *are subrings of* $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\ \bar{5}\}$ *with respect to addition and multiplication of residue classes.*

**Sol.** Since $(Z_6, +, \bullet)$ is a ring, from the property $R_4$ of the ring we have

$-\bar{0} = \bar{0}, -\bar{2} = \bar{4}, -\bar{3} = \bar{3}, -\bar{4} = \bar{2}$. $\therefore\ S_1 = \{\bar{0}, \bar{3}\}$ is a non-empty subset of $Z_6$

| + | $-\bar{0}$ | $-\bar{3}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ |

| • | $\bar{0}$ | $\bar{3}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ |

From the above tables $\bar{a}, \bar{b} \in S_1 \Rightarrow \bar{a} - \bar{b} \in S_1$ and $\bar{a} \cdot \bar{b} \in S_1$

$\therefore$ By the theorem (1), $S_1$ is a subring of $Z_6$.

$S_2 = \{\bar{0}, \bar{2}, \bar{4}\}$ is a non-empty subset of $Z_6$

| + | $-\bar{0}$ | $-\bar{2}$ | $-\bar{4}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{4}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{2}$ | $\bar{0}$ |

| • | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |

From the above tables ; $\bar{a}, \bar{b} \in S_2 \Rightarrow \bar{a} - \bar{b} \in S_2$ and $\bar{a} \cdot \bar{b} \in S_2$

$\therefore\ S_2$ is a subring of $Z_6$.

We can see that $S_1 \cap S_2 = \{\bar{0}\}$ is the trivial subring. But $S_1 \cup S_2 = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ is not a subring of $Z_6$, because $\bar{2}, \bar{3} \in S_1 \cup S_2 \Rightarrow \bar{2} + \bar{3} = \bar{5} \notin S_1 \cup S_2$.

**Ex. 2.** *Show that the set of matrices* $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ *is a subring of the ring of* $2\times 2$ *matrices whose elements are integers.* **(O.U. 03)**

**Sol.** Let $R=\left\{\begin{pmatrix} a & b \\ d & c \end{pmatrix} \middle| a,b,c,d \in Z\right\}$ be the ring of $2\times 2$ matrices and

$S=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| 0,a,b,c \in Z\right\}$. Then $S\neq\phi$ and $S\subset R$.

Let $A,B\in S$ so that $A=\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$, $B=\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ where $0,a_1,b_1,c_1,a_2,b_2,c_2\in Z$.

$\therefore\ A-B=\begin{pmatrix} a_1-a_2 & b_1-b_2 \\ 0 & c_1-c_2 \end{pmatrix}$ and $AB=\begin{pmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$

Since $a_1-a_2, b_1-b_2, c_1-c_2, a_1a_2, a_1b_2+b_1c_2, c_1c_2\in Z$;

we have $A,B\in S\Rightarrow A-B\in S$ and $AB\in S$. Hence $S$ is a subring of $R$.

**Note :** If R is a commutative ring then S is an ideal of R.

**Ex. 3.** *Let $R$ be a ring and $a\in R$ be a fixed element. Then prove that $S=\{x\in R\,|\,ax=0\}$ is a subring of $R$.*

**Sol.** If $0\in R$ is the zero element of $R$ and $a\in R$, we have $a0=0\Rightarrow 0\in S$

$\therefore\ S\neq\phi$ and $S\subset R$.

Let $x,y\in S$. Then $x,y\in R$ and $ax=0, ay=0$.

Now $a(x-y)=ax-ay=0-0=0\Rightarrow x-y\in S$.

Also $a(xy)=(ax)y=0y=0\Rightarrow xy\in S$. Hence $S$ is a subring of $R$.

**Notation.** Let $R$ be a ring and $a\in R$ be a fixed element. The intersection of the family of subrings containing '$a$' is a subring of $R$. **This subring is denoted by $R_a$ and is called the subring of $R$ generated by '$a$'.**

**Ex. 4.** *If $R$ is a ring and $C(R)=\{x\in R\,|\,xa=ax\ \forall\ a\in R\}$ then prove that $C(R)$ is a subring of $R$.*

**Sol.** For $0\in R$, the zero element of the ring, we have $0a=a0\ \forall\ a\in R$.

By the definition of $C(R)$, $0\in C(R)$. $\therefore\ C(R)\neq\phi$ and $C(R)\subset R$

Let $x,y\in C(R)$

Then $x,y\in R$ and $xa=ax, ya=ay\ \forall\ a\in R$ .... (1)

$\forall\ a\in R, a(x-y)=ax-ay=xa-ya=(x-y)a$ (By $R_6$ and (1))

Also, $\forall\ a\in R, a(xy)=(ax)y=(xa)y=x(ay)=x(ya)=(xy)a$ [By $R_5$, (1)]

$\therefore\ x, y \in C(R) \Rightarrow x-y, xy \in C(R)$. Hence $C(R)$ is a subring of $R$.

**Note.** The subring $C(R)$ is called the centre of the ring $R$.

**Ex. 5.** *If $D$ is an integral domain with unity element '1' prove that $\{n.1 \mid n \in Z\}$ is a subdomain of $D$.*

**Sol.** Let $D^1 = \{n.1 \mid n \in Z\}$ = the set of all integral multiples of unity element '1' in D.

For $0 \in Z, 0.1 = O \in D$ is the zero element in $D$. $\therefore\ D^1 \neq \phi$ and $D^1 \subset D$.

Let $a, b \in D^1$ so that $a = l.1, b = m.1$ where $l, m \in Z$.

$a - b = l.1 - m.1 = (l-m).1 = p.1$ where $p = l - m \in Z$.

Also $ab = (l.1)(m.1) = (lm).1 = q.1$ where $q = lm \in Z$.

Hence $D^1$ is a subring of $D$.

For $a, b \in D^1$ we have $ab = (l.1)(m.1) = (lm).1 = (ml).1 = (m.1)(l.1) = ba$

$\therefore\ D^1$ is commutative.

For $1 \in Z$ we have $1.1 = 1 \in D^1$ and hence $D^1$ contains unity element.

For $a, b \in D^1$; $ab = 0 \Rightarrow (l.1)(m.1) = 0 \Rightarrow (lm).1 = 0 \Rightarrow lm = 0$ ($\because 1 \neq 0$)

$\Rightarrow l = 0$ or $m = 0$ ($\because l, m \in Z$) $\Rightarrow l.1 = 0$ or $m.1 = 0 \Rightarrow a = 0$ or $b = 0$

$\therefore\ D^1$ has no zero divisors.

**Note.** Since every subdomain of $D$ contains unity element, and $D^1 = \{n.1 \mid n \in Z\}$, $D^1$ is contained in every subdomain.

## EXERCISE 10 ( *a* )

**1.** Show that $S = \{\bar{1}, \bar{3}, \bar{5}\}$ is not a subring of the ring $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ of residue classes modulo - 6.

**2.** Is the set of integers a subring of set of rational numbers w.r.t. usual addition and multiplication. ***(S. V. U 99)***

**3.** If $R$ is the ring of integers then prove that the set $S = \{mx \mid x \in R, m \text{ is a fixed integer }\}$ is a subring of $R$.

**4.** Let $R$ the ring of $2\times 2$ matrices whose elements are real numbers. Prove that the set

$$S = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \ a, b \text{ are real numbers} \right\} \text{ is a subring of } R.$$

**5.** Show that the set of all integers is a subring of $R = \{a + ib \mid a, b \in Z$ and $i^2 = -1\}$

**6.** If $R$ is a division ring show that $C(R) = \{x \in R \mid xa = ax\ \forall\ a \in R\}$ is a field.

**7.** Show that a subring of a field is an integral domain without unity.

**8(*a*).** $M_2(Z)$ be the ring of all $2\times2$ matrices over Z and let $R = \left\{\begin{pmatrix} a & a+b \\ a+b & a \end{pmatrix} | a,b \in Z\right\}$.

Is R a subring of $M_2(Z)$. **(*b*)** Is $R = \left\{\begin{pmatrix} a & a-b \\ a-b & a \end{pmatrix} | a,b \in Z\right\}$ a subring of $M_2(Z)$.

**9.** Show that the characteristic of a subdomain of an integral domain D is equal to the characteristic of D.

## 10. 2. IDEALS

The concept of an ideal of a ring is analogous to that of a normal subgroup of a group. Some of the subrings which we call ideals play a very important role as the normal subgroups in group theory.

**Definition. (Ideal).** *Let* $(R,+,\bullet)$ *be a ring. A non-empty subset U of R is called a two sided ideal or ideal if (1)* $a,b \in U \Rightarrow a-b \in U$ *and (2)* $a \in U$ *and* $r \in R \Rightarrow ar, ra \in U$. ***(O. U. 07, S. V. U. 99, N. U. 00, A. U. 03)***

**Definition. (Ideal).** *A subring U of a ring R is called a (two sided) ideal of R if for every* $r \in R$ *and every* $a \in U$ *both ra and ar are in U.*

**Note 1.** A subring $U$ of the ring $R$ satisfying $rU \subset U$ and $Ur \subset U$ for all $r \in R$ is an ideal.

**2.** The (2) condition of ideal is stronger than the (2) condition of a subring.

**3.** The condition (1), namely, $a,b \in U \Rightarrow a-b \in U$ is called module property.

**4.** If $U$ is an ideal of the ring $(R,+,\bullet)$ then $(U,+)$ is a normal subgroup of the commutative group $(R,+)$. Hence zero element in $R$ is zero element in $U$.

**Definition.** *A non-empty subset U of a ring R is called a right ideal if.*

(1) $a,b \in U \Rightarrow a-b \in U$ and (2) $a \in U, r \in R \Rightarrow ar \in U$.

*A non-empty subset U of a ring R is called a left ideal if*

(1) $a,b \in U \Rightarrow a-b \in U$ and $a \in U, r \in R \Rightarrow ra \in U$.

**Note. 1.** An ideal is both a left and a right ideal.

**2.** For commutative rings left ideals coincide with right ideals.

**e.g.1.** If $R$ is a ring and $0 \in R$ is the zero element then $U = \{0\}$ is an ideal of $R$.

For, (1) $0, 0 \in U \Rightarrow 0-0 = 0 \in U$ and (2) $0 \in U$, $\forall$ $r \in R \Rightarrow 0r = r0 = 0 \in U$.

$U = \{0\}$ is called Null ideal or zero ideal or trivial ideal.

**e.g. 2.** If $R$ is a ring then $R$ itself is an ideal of $R$. $R$ is called unit ideal or improper ideal of $R$.

**e.g.3.** Let $R$ = the ring of all integers and $U$ = the set of all even integers.

we know that $U$ is a subring of $R$.

For $a \in U$ and $r \in R$ we have

$a \cdot r$ = (even integer) (integer) = even integer $\in U$ and

$r \cdot a$ = (integer) (even integer) = even integer $\in U$.

Thus, $U$ = the set of even integers $= \{ .... -6, -4, -2, 0, 2, 4, 6 ... \}$ is an ideal of

$R$ = the set of integers $= \{ .... -3, -2, -1, 0, 1, 2, 3 ... \}$

**e.g. 4.** For any positive integer $'n'$, the set $n\,Z = \{0, \pm n, \pm 2n, .....\}$ is an ideal of Z.

**Remark.** Every subring of a ring is not an ideal. $(Z, +, \bullet)$ is a subring of the ring of real numbers $(R, +, \bullet)$. Since $1/2 \in R, 1 \in Z \Rightarrow 1/2 \,.\, 1 = 1/2 \in Z$; $Z$ is not an ideal of $R$.

Thus every ideal of ring $R$ is a subring of $R$ but not every subring of a ring $R$ is an ideal of R. ***(N. U. 95)***

**Note.** If $R$ is a ring then the null ideal $U = \{0\}$ is called trivial ideal and the unit ideal $R$ is called improper ideal of $R$. Any other ideal of $R$ is called proper non trivial ideal of $R$. $U$ is proper non trivial ideal of $R \Rightarrow U \neq R$ and $U \neq \{0\}$.

**Theorem 1.** ***If U is an ideal of a ring R with unity element and*** $1 \in U$ ***then*** $U = R$.

**Proof.** By definition of ideal, $U \subset R$.

Also $x \in R \Rightarrow x \,.\, 1 \in R \Rightarrow x \,.\, 1 \in U$ for $x \in R, 1 \in U$ (Def. of ideal) $\Rightarrow x \in U$.

$\therefore\ R \subset U$ and hence $U = R$.

**Theorem 2.** ***A field has no proper non-trivial ideals. (or)***
***The ideals of a field F are only {0} and F itself.*** ***(S. V. U. 08, S. K. U. 07, N. U. 00)***

**Proof.** Let $U$ be an ideal of $F$ so that $U \neq \{0\}$. We now prove that $U = F$

By the definition of ideal, $U \subset F$ ... (1)

Let $a \in U$ and $a \neq 0$.

For $a\ (\neq 0) \in F$ there exists $a^{-1} \in F$ so that $aa^{-1} = 1$.

$a \in U, a^{-1} \in F$ and $U$ is an ideal $\Rightarrow aa^{-1} = 1 \in U$.

$x \in F \Rightarrow x \,.\, 1 \in F \Rightarrow x \,.\, 1 \in U$ for $x \in F, 1 \in U$

$\Rightarrow\ x \in U$ $\qquad\qquad$ $\therefore\ F \subset U$ $\qquad\qquad$ ... (2)

From (1) and (2) : $U = F$. Hence ideals of $F$ are either $\{0\}$ or $F$.

**Theorem 3.** ***If R is a commutative ring and*** $a \in R$ ***then*** $Ra = \{ra \mid r \in R\}$ ***is an ideal of R.*** ***(S. K. U. 07, S. V. U. 05, K. U.04)***

**Proof.** For $0 \in R, 0a = 0 \in Ra$. $\therefore\ Ra \neq \phi$ and $Ra \subset R$.

Let $x, y \in Ra$. Then $x = r_1 a, y = r_2 a$ where $r_1, r_2 \in R$

$x - y = r_1 a - r_2 a = (r_1 - r_2)\, a = ra$ where $r = r_1 - r_2 \in R$. $\therefore\ x, y \in Ra \Rightarrow x - y \in Ra$ ... (1)

Let $x \in Ra$ and $r \in R$.

$x \,.\, r = (r_1 a)\, r \quad (\because x = r_1 a$ where $r_1 \in R) = r_1 (ar) = r_1 (ra)$

(By $R_5$ and $R$ is commutative )

$= (r_1 r)\, a = r' a$ where $r' = r_1 r \in R$.

Since $R$ is commutative, $x \,.\, r = r \,.\, x$.

$\therefore\ x \in Ra, r \in R \Rightarrow xr = rx \in Ra$ ... (2)

Hence from (1) and (2) : $Ra$ is an ideal of $R$.

**Note. 1.** If $R$ is a commutative ring and $a \in R$ then $aR = \{ ar \mid r \in R \}$ is an ideal of $R$.

**2.** If $R$ is a ring and $a \in R$ then $Ra$ is a left ideal and $aR$ is a right ideal.

**Theorem 4.** ***A commutative ring R with unity element is a field if R have no proper ideals.*** ***(K. U. 08, O. U. 07, A. U. 04, S. V. U. 04)***

**Proof.** Since the ring R has no proper non tirvial ideals, the ideals of $R$ are $\{0\}$ and $R$ only.

To prove that $R$ is a field we have to show that every $a\ (\neq 0) \in R$ has a multiplicative inverse. We know that $aR = \{ ar \mid r \in R \}$ is an ideal of $R$.

Since $a \neq 0, aR \neq \{0\}$ and hence $aR = R$. (By hypothesis)

$1 \in R \Rightarrow 1 \in a\ R \Rightarrow 1 = ab$ for some $b \neq 0 \in R$. Since $R$ is commutative, $1 = ab = ba$.

$\therefore\ a \neq 0 \in R$ has a multiplicative inverse $b \in R$. Hence R is a field.

**Note.** If $R$ is a ring with unity element and $R$ has no proper non trivial ideals then $R$ is a division ring.

**Theorem. 5.** ***The intersection of two ideals of a ring R is an ideal of R.*** ***(N. U. 07, A. U. 03, S.V. U. 99, O. U. 07)***

**Proof.** Let $U_1, U_2$ be two ideals of the ring $R$.

If $0 \in R$ is the zero element, then $0 \in U_1$ and $0 \in U_2$.

$\therefore\ 0 \in U_1 \cap U_2$ and hence $U_1 \cap U_2 \neq \phi$

Let $a, b \in U_1 \cap U_2$ and $r \in R$. Then $a, b \in U_1$ and $a, b \in U_2$.

$a, b \in U_1, r \in R$ and $U_1$ is an ideal $\Rightarrow a - b \in U_1$ and $ar, ra \in U_1$ .... (1)

$a, b \in U_2, r \in R$ and $U_2$ is an ideal $\Rightarrow a - b \in U_2$ and $ar, ra \in U_2$ .... (2)

From (1) and (2) : $a - b \in U_1 \cap U_2$ and $ar, ra \in U_1 \cap U_2$

Hence $U_1 \cap U_2$ is an ideal of $R$.

**Remark :** The union of two ideals of a ring $R$ need not be an ideal of $R$. **(*O. U. 97*)**

For the ring $Z$ of integers, $A=\{2n \mid n \in Z\}$ and $B=\{3n \mid n \in Z\}$ are two ideals .

But, for $2,3 \in A \cup B$, $3-2=1 \notin A \cup B$. $\therefore A \cup B$ is not an ideal of $Z$.

**Theorem 6.** ***If $U_1$ and $U_2$ are two ideals of a ring $R$ then $U_1 \cup U_2$ is an ideal of $R$ if and only if $U_1 \subset U_2$ or $U_2 \subset U_1$.*** ***(N. U. M12, 03)***

**Proof.** Let $U_1 \cup U_2$ be an ideal of $R$. We now prove that $U_1 \subset U_2$ or $U_2 \subset U_1$.

If possible, suppose that $U_1 \not\subset U_2$ and $U_2 \not\subset U_1$.

Since $U_1 \not\subset U_2$ there exists an element $a \in U_1$ and $a \notin U_2$.

Since $U_2 \not\subset U_1$ there exists an element $b \in U_2$ and $b \notin U_1$.

$a \in U_1$ and $b \in U_2 \Rightarrow a, b \in U_1 \cup U_2$

$a, b \in U_1 \cup U_2$ and $U_1 \cup U_2$ is an ideal $\Rightarrow a-b \in U_1 \cup U_2$

$\Rightarrow a-b \in U_1$ or $a-b \in U_2$

But $a-b \in U_1 \Rightarrow a-(a-b)=b \in U_1$ ... (1)

$a-b \in U_2 \Rightarrow b+(a-b)=a \in U_2$ ... (2)

Both (1) and (2) contradict $a \notin U_2, b \notin U_1$

$\therefore$ Our supposition is wrong. Hence $U_1 \subset U_2$ or $U_2 \subset U_1$.

**Conversely,** let $U_1 \subset U_2$ or $U_2 \subset U_1$

Then $U_1 \cup U_2 = U_2$ or $U_1$ and hence $U_1 \cup U_2$ is an ideal.

**Note.** If $S_1, S_2$ are two subrings of a ring prove that $S_1 \cup S_2$ is also a subring iff either $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$. ***(N. U. 11)***

## SOLVED PROBLEMS

**Ex. 1.** *Give an example of a subring which is not an ideal.*

**Sol.** The set of rational numbers $(Q, +, \bullet)$ is a subring of the ring of real numbers $(R, +, \bullet)$.

For $(2/3) \in Q$ and $\sqrt{3} \in R$ we have $(2/3).\sqrt{3} \notin Q$.

$\therefore$ The subring Q is not an ideal of $R$.

**Ex. 2.** *If $U_1, U_2$ are two ideals of a ring $R$ then $U_1+U_2=\{x+y \mid x \in U_1, y \in U_2\}$ is also an ideal of $R$.* ***(S.K.D. 08, S. V. U. 08, A. U. 04, K.U. 03, 05)***

**Sol.** Let $0 \in R$ be the zero element.

Then $0 \in U_1, 0 \in U_2$ implies that $0+0=0 \in U_1+U_2$. $\therefore U_1+U_2 \neq \phi$ and a subset of R.

Let $a, b \in U_1+U_2$ and $r \in R$.

Then $a=x_1+y_1, b=x_2+y_2$ where $x_1, x_2 \in U_1$; $y_1, y_2 \in U_2$

$a-b=(x_1+y_1)-(x_2+y_2)=x+y$ where $x=x_1-x_2 \in U_1, y=y_1-y_2 \in U_2$

$ar=(x_1+y_1)r=x_1r+y_1r=x'+y'$ where $x'=x_1r \in U_1, y'=y_1r \in U_2$

$ra = r(x_1 + y_1) = rx_1 + ry_1 = x'' + y''$ where $x'' = rx_1 \in U_2, y'' = ry_1 \in U_2$.

$\therefore\ a, b \in U_1 + U_2$ and $r \in R \Rightarrow a - b \in U_1 + U_2$ and $ar, ra \in U_1 + U_2$

Hence $U_1 + U_2$ is an ideal of $R$.

**Note.** Since $U_1 \subset U_1 + U_2$ and $U_2 \subset U_1 + U_2, U_1 + U_2$ is an ideal of $R$ containing both $U_1$ and $U_2$.

## 10. 3. PRINCIPAL IDEAL

If $R$ is a commutative ring with unity from Theorem (3) Art. 2.2 we observed that for a given $a \in R$ the set $\{ra \mid r \in R\}$ is an ideal in $R$ that contains the element '$a$'.

**Definition.** *Let R be a commutative ring with unity and* $a \in R$. *The ideal* $\{ra \mid r \in R\}$ *of all multiples of 'a' is called the principal ideal generated by 'a' and is denoted by* $(a)$ *or* $\langle a \rangle$. **(K. U. 04)**

An ideal $U$ of the ring $R$ is a principal ideal $\Rightarrow U = \langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$.

**e.g.1.** The null ideal or trivial ideal $\{0\}$ of a ring $R$ is the principal ideal generated by the zero element of $R$. That is null ideal $= \langle 0 \rangle$.

**e.g. 2.** The unit ideal or improper ideal $R$ of a ring $R$ is the principal ideal generated by the unity element '1' of the ring $R$. That is $R = \langle 1 \rangle$.

**e.g. 3.** $Z$ is a commutative ring with unity element.

The principal ideal generated by $2 \in Z = \langle 2 \rangle = \{2n \mid n \in Z\} =$ the set of all even integers.

**e.g. 4.** A field $F$ has only null ideal $= \langle 0 \rangle$ and unit ideal $= F = \langle 1 \rangle$ which are principal ideals.

**Definition. (Principal ideal ring).** *A commutative ring R with unity is a principal ideal ring if every ideal in R is a principal ideal .* **(K. U. 04)**

$D$ is a principal ideal domain $\Rightarrow$ every ideal $U$ in $D$ is in the form $U = \langle a \rangle$ for some $a \in D$.

**Theorem. 1.** ***A field is a principal ideal ring.*** **(K. U. 04, N. U. 95)**

**Proof.** A field $F$ has only two ideals, namely, $U = \langle 0 \rangle$ and $U = F = \langle 1 \rangle$.

But $U = \langle 0 \rangle$ and $U = \langle 1 \rangle$ are principal ideals. $\therefore$ the field $F$ is a principal ideal ring.

**Theorem. 2.** ***The ring of integers Z is a principal ideal ring. (or) Every ideal of Z is a principal ideal.*** **(A. U. 07, N. U. M12, 04, S. V. U. 08)**

**Proof.** Let $U$ be ideal of $Z$ and $U = \{0\}$. Then $U$ is generated by the zero element.

$\therefore\ U = \langle 0 \rangle$ is a principal ideal. Let $U$ be an ideal of $Z$ and $U \neq (0)$.

$\therefore$ there exists $a \in U$ so that $a \neq 0$. $a \in U, U$ is an ideal $\Rightarrow -a \in U$.

Since $U \subset Z$, one of $a, -a$ must be a positive integer.

$\therefore$ the set of positive integers $U^+$ in $U$ is non - empty.

$\therefore$ by well - ordering principle $U^+$ has a least member, say, $b$.

We now prove that $U = \langle b \rangle$ = the principal ideal generated by '$b$'.

Let $x \in U$. Since $x, b$ are integers and $b \neq 0$ there exist $q, r \in Z$ such that $x = bq + r;\ 0 \leq r < b$ (Division algorithm).

$b \in U, q \in Z$ and $U$ is an ideal $\Rightarrow bq \in U$. $x \in U, bq \in U \Rightarrow x - bq = r \in U$.

Now $r \in U, 0 \leq r < b$ and $b$ is the least member in $U^+ \Rightarrow r = 0$.

$\therefore\ x - bq = r \Rightarrow x - bq = 0 \Rightarrow x = bq$.

Hence $x \in U \Rightarrow x = bq$ for $q \in Z \Rightarrow U = \{bq \mid q \in Z\} = \langle b \rangle$.

$\therefore$ every ideal $U$ of $Z$ is a principal ideal. Hence $Z$ is a principal ideal ring.

**Note. 1.** Principal ideal rings that are also integral domains, such as ring of integers $Z$ are called principal ideal domains (P.I. Ds)

**2.** If $Z$ is the ring of integers then the principal ideal generated by $a \in Z$ is $\{aq \mid q \in Z\} = \langle a \rangle$.

## 10. 4. QUOTIENT RINGS OR FACTOR RINGS

The concept of quotient ring is analogous to that of quotient groups. If $U$ is an ideal of a ring $(R, +, \bullet)$ then $(U, +)$ is a normal subgroup of the commutative group $(R, +)$. From group theory we know that the set $R/U = \{x + U = U + x \mid x \in R\}$ of all cosets of $U$ in $R$ is a group with respect to addition of two cosets defined by $(a + U) + (b + U) = (a + b) + U$ for $a + U, b + U \in (R/U)$. We know further that these cosets are disjoint.

As addition operation is commutative left coset $a + U$ is equal to right coset $U + a$.

In order to impose ring structure in $R/U$ we can define multiplication of two cosets as $(a + U)(b + U) = ab + U$ for $a + U, b + U \in R/U$.

**Theorem. 1. If $U$ is an ideal of a ring $R$ then the set $R/U = \{x + U \mid x \in R\}$ is a ring with respect to the induced operations of addition (+) and multiplication ($\bullet$) of cosets defined follows : $(a + U) + (b + U) = (a + b) + U$ and $(a + U).(b + U) = ab + U$ for $a + U, b + U \in R/U$.** *(N. U. 12, 95)*

**Proof.** Since $(R, +)$ is commutative group, the quotient group $(R/U, +)$ is also commutative.

In order to show that $(R/U, +, \bullet)$ is a ring we must show that

(1) multiplication of cosets is well defined,

(2) multiplication is associative and (3) distributive laws hold.

(1) Let $a+U=a_1+U$ and $b+U=b_1+U$.

Then $a=a_1+u_1$ and $b=b_1+u_2$ for $u_1,u_2\in U$.

$ab=(a_1+u_1)(b_1+u_2)=a_1b_1+a_1u_2+u_1b_1+u_1u_2$

Since $U$ is an ideal, $a_1u_2,u_1b_1,u_1u_2\in U$

$\therefore\ ab-a_1b_1\in U$ and hence $ab+U=a_1b_1+U\Rightarrow(a+U).(b+U)=(a_1+U).(b_1+U)$

Therefore multiplication of cosets is well defined.

Let $a+U,b+U,c+U\in R/U$

(2) $[(a+U).(b+U)].(c+U)=(ab+U).(c+U)=(ab)\,c+U$

$=a\,(bc)+U\qquad(\because\ a,b,c\in R)$

$=(a+U).(bc+U)=(a+U).[(b+U).(c+U)]$

(3) $(a+U).[(b+U)+(c+U)]=(a+U).[(b+c)+U]=a\,(b+c)+U$

$=(ab+ac)+U\quad(\because\ a,b,c\in R)$

$=(ab+U)\,(ac+U)=(a+U).(b+U)+(a+U).(c+U)$

Similarly we can prove that $[(b+U)+(c+U)].(a+U)=(b+U).(a+U)+(c+U).(a+U)$

Hence $(R/U,+,\bullet)$ is a ring.

**Definition.** *Let R be a ring and U be an ideal of R. Then the set* $R/U=\{x+U\mid x\in R\}$ *with respect to induced operations of addition and multiplication of cosets defined by* $(a+U)+(b+U)=(a+b)+U;(a+U).(b+U)=ab+U$ *for* $a+U,b+U\in R/U$ *is a ring. This ring* $(R/U,+,\bullet)$ *is called the quotient ring or factor ring or residue class ring of R modulo U.*

**Note. 1.** It is convenient, sometimes, to denote coset $a+U$ in $R/U$ by the symbol $\bar{a}$ or $[a]$. Then we write sum and product of two cosets as $[a]+[b]=[a+b]$ and $[a].[b]=[ab]$.

**2.** $0+U=U$ is the zero element in the ring $R/U$.

**3.** Every ring $R$ has two improper ideals, namely, the trivial ideal $\{0\}$ and the ideal $R$.

The quotient ring of the ideal $\{0\}$ is $R/\{0\}$ or $R/\langle 0\rangle=\{x+\langle 0\rangle\mid x\in R\}$

The quotient ring of the ideal $R$ is $R/R$ or $R/\langle 1\rangle=\{x+\langle 1\rangle\mid x\in R\}$

**4.** $(a+U)+(b+U)=(a+b)+U;(a+U)\,(b+U)=ab+U$

**5.** $(a+U)^2=(a+U)\,(a+U)=a^2+U$

**6.** $a+U=b+U\Leftrightarrow(a-b)\in U$.

**7.** $a+U=U\Leftrightarrow a\in U$

**Theorem. 2.** ***If R/U is the quotient ring prove that***
***(i) R/U is commutative if R is commutative and***
***(ii) R/U has unity element if R has unity element*** **(O. U. 01)**

**Proof.** (*i*) $R$ is commutative $\Rightarrow ab=ba\ \forall\ a,b\in R.$

Let $a+U, b+U \in R/U$. $(a+U)(b+U) = ab+U = ba+U = (b+U).(a+U)$

$\therefore$ $R/U$ is commutative.

(*ii*) $R$ has unity element $\Rightarrow$ there exists $1 \in R$ so that $a1 = 1a = a \ \forall \ a \in R$.

Let $a+U \in R/U$. For $1 \in R$ we have $1+U \in R/U$

We now prove that $1+U$ is the unity element.

$(a+U)(1+U) = a1+U = a+U$ and $(1+U)(a+U) = 1a+U = a+U \ \forall \ a+U \in R/U$

$\therefore$ $1+U$ is the unity element in $R/U$.

**Note.** In the quotient ring $R/U$, the unity element $= 1+U$.

**e.g.1**. Consider $Z_6 = \{0,1,2,3,4,5\}$, the ring of integers modulo 6. **(*A. U. 07*)**

$U = \{0,3\}$ is an ideal of $Z_6$. The cosets of $U$ in $R$ are as follows :

$0+U = \{0+0, 0+3\} = \{0,3\}; 1+U = \{1+0, 1+3\} = \{1,4\}$

$2+U = \{2+0, 2+3\} = \{2,5\}; 3+U = \{3+0, 3+3\} = \{3,0\} = 0+U$

$4+U = \{4+0, 4+3\} = \{4,1\} = 1+U$ and $5+U = \{5+0, 5+3\} = \{5,2\} = 2+U$

$\therefore$ $(Z_6/U) = \{0+U, 1+U, 2+U\}$ is the quotient ring.

**Note.** We observe that two cosets are identical or disjoint and union of all cosets $= Z_6$.

**e.g. 2.** For the ring $Z$ of all integers we know that $nZ = \{nx \mid x \in Z\}$ for any $n \in Z$ is an additive subgroup of $Z$.

Let $m \in nZ$ and $r \in Z$. Then $m = na$ where $a \in Z$.

$mr = (na)\, r = n\,(ar)$ and $rm = r\,(na) = n\,(ar)$

so that $mr = rm = n\,(ar) = nb \in nZ$ where $b = ar \in Z$. Thus $nZ$ is an ideal of $Z$.

The set of all cosets of $nZ$ in $Z$, namely, $(Z/nZ) = \{x+nZ \mid x \in Z\}$ forms a ring under the induced operations of addition and multiplication.

## SOLVED PROBLEMS

**Ex. 3.** *If $U$ is an ideal of the ring $R$ and $a, b \in R$ then prove that*

$a+U = b+U \Leftrightarrow a-b \in U$.

**Sol.** Let $a+U = b+U$. $0 \in U \Rightarrow a = a+0 \in a+U$

$a+U = b+U \Rightarrow a \in b+U \Rightarrow$ there exists $x \in U$ such that $a = b+x \Rightarrow a-b = x \in U$.

Let $a-b \in U$. If $a-b = c \in U$ then $a = b+c$

$x \in a+U \Rightarrow$ there exists $d \in U$ such that $x = a+d$.

$\Rightarrow x = (b+c)+d = b+(c+d) \in b+U$ $(\because \ c+d \in U)$ $\therefore$ $a+U \subset b+U$

Similarly, we can prove that $b+U \subset a+U$. Hence $a+U = b+U$.

## 10. 5. EUCLIDEAN RINGS

**Definition.** *An integral domain R is said to be Euclidean ring or Euclidean domain if for every* $a(\neq 0)\in R$ *there is defined a non-negative integer d(a) such that*

(1) *for all* $a,b\in R, a\neq 0, b\neq 0; d(a)\leq d(ab)$ *and*

(2) *for any* $a,b\in R, b\neq 0$ *there exist* $q,r\in R$ *such that* $a=bq+r$ *where either* $r=0$ *or* $d(r)<d(b)$. **(*O. U. 07, S. K. D. 07*)**

**Note 1.** For any $a(\neq 0)\in R, d(a)\geq 0$.

**2.** For the zero element 0 of $R, d(0)$ is not defined. However some authors defined $d(0)=0$, integer.

**3.** The property (2) in the above definition is called division algorithm.

**4.** From the above definition we note that $d: R-\{0\}\to Z$ is a mapping such that

(*i*) $d(a)\geq 0\ \forall\ a\in R-\{0\}$.

(*ii*) $d(a)\leq d(a,b)\forall\ a,b\in R-\{0\}$ and

(*iii*) there exist $q,r\in R$ so that $a=bq+r$ where either $r=0$ or $d(r)<d(b)$ for any $a,b\in R$ and $b\neq 0$.

### SOLVED PROBLEMS

**Ex. 4.** *The ring of integers is an Euclidean ring.* **(*A. U. 08*)**

**Sol.** We know that the ring $(Z,+,\cdot)$ of integers is an integral domain.

Define the mapping $d: Z-\{0\}\to Z$ by by $d(a)=|a|\forall a\in Z-\{0\}$

Since $|a|>0$ we have $d(a)\geq 0\ \forall\ a\in Z-\{0\}$

For $a\neq 0, b\neq 0\in Z; ab(\neq 0)\in Z$ and $d(ab)=|ab|=|a||b|\geq|a|=d(a)$ since $|b|\geq 1$.

For $a,b\in Z, b\neq 0$; by division algorithm in integers, we have $q,r\in Z$ so that $a=bq+r$ where $0\leq r<|b|$.

*i.e.* $a=bq+r$ where $r=0$ or $0<r<|b|$

*i.e.* $a=bq+r$ where $r=0$ or $d(r)<d(b)$ $(r>0)\Rightarrow d(r)=r$ and $|b|=d(b)$

$\therefore$ $(Z,+,\cdot)$ is a Euclidean ring.

**Ex. 5.** *Prove that the ring of Gaussian integers is an Eucidean ring.*

**(*S. K. D 2007, S. V. U. 2001*)**

**Sol.** We know that $Z[i]=\{a+ib\,|\,a,b\in Z, i^2=-1\}$ of Gaussian integers is an integral domain under addition and multiplication of numbers.

Define the mapping $d: Z[i]-\{0\}\to Z$ by $d(x+iy)=x^2+y^2\ \forall\ x+iy\in Z[i]-\{0\}$

For $z=x+iy\neq 0\in Z[i]$ we have $x\neq 0$ or $y\neq 0$ and hence $x^2+y^2\geq 1$.

$\therefore\ d(z) = d(x+iy) \geq 0\ \forall\ z \in Z[i] - \{0\}$

Let $u, v \in Z[i] - \{0\}$.

Then $u = a+ib, v = c+id$ where $a,b,c,d \in Z$ and $a \neq 0$ or $b \neq 0$; $c \neq 0$ or $d \neq 0$.

$uv = (ac-bd) + i(ad+bc)$.

Now $d(uv) = (ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2)$

$\geq a^2+b^2 = d(u)$ since $c^2+d^2 \geq 1$.

Let $u, v \in Z[i]$ and $v \neq 0$.

Then $u = a+ib, v = c+id$ where $a,b,c,d \in Z$ and $c \neq 0$ or $d \neq 0$.

Consider $uv^{-1} = \dfrac{a+ib}{c+id} = \dfrac{ac+bd}{c^2+d^2} + i\dfrac{bc-ad}{c^2+d^2} = p+iq$

where $p = \dfrac{ac+bd}{c^2+d^2}, q = \dfrac{bc-ad}{c^2+d^2}$ are rational numbers.

For $p, q \in Q$ we have $p = [p] + \alpha, q = [q] + \beta$ where $[p], [q]$ are integer parts of $p, q$ and $\alpha, \beta$ are fractional parts of $p, q$ so that $0 \leq \alpha, \beta < 1$.

If $0 \leq \alpha, \beta \leq \dfrac{1}{2}$ take $m = [p], n = [q]$ and if $\dfrac{1}{2} < \alpha, \beta < 1$ take $m = [p]+1, n = [q]+1$.

Then $\gamma = |p-m| \leq \dfrac{1}{2}$ and $\delta = |q-n| \leq \dfrac{1}{2}$ so that $p = m+\gamma$ and $q = n+\delta$.

Now $a+ib = (c+id)(p+iq) = (c+id)\{(m+\gamma) + i(n+\delta)\}$

$= (c+id)\{(m+in) + (\gamma+i\delta)\} = (c+id)(m+in) + (c+id)(\gamma+i\delta)$

$= (c+id)s + r$ where $s = m+in$ and $r = (c+id)(\gamma+i\delta)$. $\therefore$ We have $u = vs + r$

$m, n \in Z \Rightarrow s = m+in \in Z[i]$. $u, v, s \in Z[i] \Rightarrow r = u - vs \in Z[i]$.

If $r \neq 0$ then $d(r) = (c^2+d^2)(\gamma^2+\delta^2) \leq (c^2+d^2)\left(\dfrac{1}{4}+\dfrac{1}{4}\right) \leq (c^2+d^2)\dfrac{1}{2} < c^2+d^2 = d(v)$.

Hence, for $u, v \in Z[i]$ and $v \neq 0$ there exist $s = m+in, r = (c+id)(\gamma+i\delta) \in Z[i]$

so that $u = vs + r$ where $r = 0$ or $d(r) < d(v)$. $\therefore Z[i]$ is an Euclidean ring.

**Theorem 1.** ***Every field is a Euclidean ring.*** **(*O. U. 07, N. U. 08*)**

**Proof.** Let $F$ be a field and $F^*$ be the set of all non-zero elements of $F$.

Since $F$ is a field, $F$ is an integral domain.

Define the mapping $d : F^* \to Z$ by $d(a) = 0$ (zero integer) $\forall a \in F^*$

$\therefore\ d(a) \geq 0\ \forall\ a \in F^*$

Let $a, b \in F^*$. Then $a, b$ and $ab$ are non zero elements of $F$.

$\therefore\ d(a) = 0$ and $d(ab) = 0 \Rightarrow d(a) \leq d(ab)$

Let $a \in F$ and $b \in F^*$. Now $a = a1$ where 1 is the unity element of $F$.

$= a(b^{-1}b) = (ab^{-1})b$ $(\because b^{-1}b = 1)$

$= (ab^{-1})b + 0$ where '0' is the zero element of the field $F$.

$\therefore\ a = qb + r$ where $q = ab^{-1}, r = 0$

Hence, for $a \in F, b \in F^*$ there exist $q, r \in F$ so that $a = qb + r$ where $r = 0$.

$\therefore\ F$ is an Euclidean ring.

**Note.** We can prove the above theorem by defining

$d : F^* \to Z$ by $d(a) = 1$ (integer) $\forall\ a \in F^*$.

**Theorem 2.** ***Every Euclidean ring is principal ideal ring. (OR) Every ideal of an Euclidean ring is a principal ideal.*** **(N. U. 2000)**

**Proof.** Let $R$ be an Euclidean ring. Let $U$ be an ideal of $R$.

Let $U = \{0\}$ where '0' is the zero element of $R$.

Then $U = \{0\}$ is the ideal generated by $0 \in R$.

$\therefore\ U$ is a principal ideal of $R$. Let $U \neq \{0\}$.

$\therefore$ there exists $x \in U$ and $x \neq 0$ so that the set $\{d(x) \mid x \neq 0\}$ is a non-empty set of non-negative integers.

By well ordering principle there exists $b \neq 0 \in U$ so that $d(b) \leq d(x)$ where $x \neq 0 \in U$.

We now prove that $U = (b)$. Let '$a$' be any element of $U$.

By division algorithm, there exist $q, r \in R$ so that $a = bq + r$ where $r = 0$ or $d(r) < d(b)$.

$b \in U, q \in R$ and $U$ is an ideal $\Rightarrow bq \in U$.

$a \in U, bq \in U \Rightarrow a - bq = r \in U$

If $r \neq 0$ then $d(r) < d(b)$ so that we have a contradiction as $d(b) \leq d(x)\ \forall\ x \neq 0 \in U$

$\therefore\ r = 0$ and hence $a = bq$.

$\therefore\ U = \{bq \mid q \in R\} = (b)$ is the principal ideal generated by $b\ (\neq 0) \in U$.

Hence every ideal $U$ of $R$ is a principal ideal.

$\therefore\ R$ is a principal ideal ring.

**Note 1.** If $U$ is an ideal of an Euclidean ring $R$ then $U$ is a principal ideal of $R$ so that $U = (b) = \{bq \mid q \in R\}$

For, the ring $R = \left\{a + b\left(\frac{1+\sqrt{19i}}{2}\right) : a, b \in Z\right\}$ of complex numbers is a principal ideal ring but not Euclidean.

**Ex. 6.** *Prove that every Euclidean ring possesses unity element.* **(S.V.U.2000)**

**Sol.** Let R be an Euclidean ring. $\therefore$ R is an principal ideal of R.

$\therefore$ R is an ideal generated by some element c of the ring R so that $R = (c) = \{cq \mid q \in R\}$

$\therefore c \in R \Rightarrow c = ce$ for some $e \in R$.

We now prove that $e \in R$ is the unity.

Let $x \in R$. Then $x = cd$ for some $d \in R$.

Now $xe = (cd)\, e = (dc)\, e = d\,(ce) = dc = cd = x$. $\therefore xe = x \ \forall\ x \in R$

Hence $e \in R$ is the unity element.

## EXERCISE 10 ( *b* )

**1.** Prove that the subset $N = \{0,3\}$ of $Z_6 = \{0,1,2,3,4,5\}$ is an ideal of $(Z_6, +, \bullet)$ ring.

**2.** Prove that the subset $U = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a,b \in Z \right\}$ is a subring but not ideal of the ring of $2\times2$ matrices whose elements are integers.

**3.** (*a*) Show that the subset $U = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a,b \in Z \right\}$ is a left ideal but not right ideal of the ring of $2\times2$ matrices over integers.

(*b*) Show that te subset $\mathrm{U} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle/ a,b \in \mathrm{Z} \right\}$ is a right ideal but not a left idal of the ring $(\mathrm{M}_2, +, \bullet)$ **(S. V. U. 2010)**

**4.** Is the set of rational numbers an ideal of the ring of real numbers $(R, +, \bullet)$. **(S. V. U. 99)**

**5.** If *m* is a fixed integer prove that the set $U = \{mx \mid x \in Z\}$ is an ideal of ring of integers *Z*.

**6.** Prove that a division ring has no proper ideals.

**7.** If *R* is a ring and $a \in R$ show that the set $U = \{x \in R \mid ax = 0\}$ is a right ideal of *R*.

**8.** Write the principal ideal generated by 4 in the ring of integers $(Z, +, \bullet)$.

**9.** Prove that $N = \{(0,n) \mid n \in Z\}$ is an ideal of $Z \times Z = \{(m,n) \mid m,n \in Z\}$ under addition and multiplication.

**10.** Prove that $z/nz = \{x + nz \mid x \in z\}$ forms a ring. (**Hint** : See **e.g.** (2) in Art. 10.6)

**11.** If *U* is a left ideal of a ring *R* and $\alpha(U) = \{x \in R \mid xu = 0 \ \forall\ u \in U\}$ prove that $\alpha(U)$ is a two sided ideal of *R*. **(S. V. U. 03)**

**12.** If *p* is prime element of Euclidean ring R and $a,b \in R$ show that $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ **(A. U. 08)**

# Homomorphism of Rings, Maximal and Prime Ideals

**11.1.** In groups, we have learnt that one way of knowing more information about a group, is to examine its interaction with other groups by using homomorphism. The concept of homomorphism in rings is analogous to that of homomorphism in groups. The homomorphism in rings is a mapping which preserve the relations $a+b=c$ and $ab=d$, the addition and multiplication operations.

**Definition. (Homomorphism).** *Let $R, R'$ be two rings. A mapping $f: R \to R'$ is said to be a homomorphism if (a) $f(a+b)=f(a)+f(b)$ and (b) $f(ab)=f(a)\,f(b)$ for all $a, b \in R$.* **(K. U. 08, O. U. 01)**

**Note. 1.** The operations $+, \bullet$ on the left hand side of the properties (*a*), (*b*) are that of the ring *R*, while the operations $+, \bullet$ on the right hand side of the properties (*a*), (*b*) are that of the ring $R'$.

**2.** Since $R, R'$ are commutative groups under addition clearly property (*a*) shows that a ring homomorphism is a group homomorphism from $(R, +)$ to $(R', +)$.

**Definition.** *If $f: R \to R'$ is a homomorphism of a ring R into R′ then the image set $f(R)=\overline{R}=\{f(x) \mid x \in R\}$ is called the f - homomorphic image of R.*

**Definition.** *Let $R, R'$ be two rings. A homomorphism $f: R \to R'$ is called an epimorphism or onto homomorphism if $f$ is* onto mapping.

A homomorphism $f: R \to R'$ *is called a monomorphism if $f$ is one-one mapping.*

*A homomorphism $f: R \to R'$ is called an isomorphism if $f$ is both one-one and onto mapping.*

*A homomorphism $f: R \to R$ of a ring R into itself is called an endomorphism.*

*A homomorphism $f: R \to R$ which is both one-one and onto is called an automorphism.* **(O. U. 01)**

**Notation.** If $f: R \to R'$ is an onto homomorphism or epimorphism then $R'$ is the homomorphic image of *R* and we write $R \simeq R'$.

If $f: R \to R'$ is an isomorphism then we say that *R* is isomorphic to $R'$ or $R, R'$ are isomorphic and we write $R \cong R'$.

**Note 1.** If $f : R \to R'$ is an onto homomorphism then $f(R) = R'$.

**2.** If $U$ is an ideal of the ring $R$, then $R/U = \{ x+U \mid x \in R \}$ is also a ring w.r.t. addition and multiplication of cosets. Then the mapping $f : R \to R/U$ defined by $f(x) = x+U$ for all $x \in R$ is called the natural homomorphism from $R$ onto $R/U$. ***(N. U. 97)***

**3.** A homomorphism is used to simplify a ring while retaining certain of its features. An isomorphism is used to show that two rings are algebraically identical.

**e.g. 1.** Let $R, R'$ be two rings and $f : R \to R'$ be defined by $f(x) = 0' \ \forall \ x \in R$, where $0' \in R'$ is the zero element.

Let $a, b \in R$. Then $f(a) = 0', f(b) = 0'$ and hence $f(a+b) = 0', f(ab) = 0'$.

Then $a+b, a\,b \in R$.

$f(a+b) = 0' = 0'+0' = f(a) + f(b)$ and $f(ab) = 0' = 0'.0' = f(a).f(b)$.

$\therefore$ $f$ is a homomorphism from $R$ into $R'$. This is called **Zero homomorphism.**

**e.g. 2.** Let $R$ be a ring and $f : R \to R$ be defined by $f(x) = x \ \forall \ x \in R$.

Let $a, b \in R$ so that $a+b, a\,b \in R$.

By definition, $f(a+b) = a+b = f(a) + f(b)$ and $f(ab) = ab = f(a)\ f(b)$.

Also for each $y \in R$ (codomain) there exists $y \in R$ (domain) so that $f(y) = y$

$\Rightarrow f$ is onto mapping.

Further for $a, b \in R$, $f(a) = f(b) \Rightarrow a = b \ \Rightarrow f$ is one-one mapping.

Hence $f$ is an automorphism. This is called **Identity homomorphism.**

**e.g. 3.** Let $Z$ be the ring of integers and $f : Z \to 2Z$ be defined by $f(n) = 2n \ \forall \ n \in Z$. ***(K. U. 12, O. U. 07)***

Let $m, n \in Z$. Then $m+n, mn \in Z$. Then $f(m+n) = 2\,(m+n) = 2m+2n = f(m)+f(n)$.

But $f(mn) = 2\,(mn) \neq (2m)\,(2n) = f(m)\ f(n)$. $\therefore$ $f$ is not a ring homomorphism.

Although, the group $(Z,+)$ is isomorphic to the group $(2Z,+)$, the ring $(Z, +, \cdot)$ is not isomorphic to the ring $(2Z, +, \cdot)$.

**Theorem 1.** ***Let $f : R \to R'$ be a homomorphism of a ring $R$ into the ring $R'$ and $0 \in R, 0' \in R'$ be the zero elements. Then (1) $f(0) = 0'$ (2) $f(-a) = -f(a) \ \forall \ a \in R$ and (3) $f(a-b) = f(a) - f(b)$ for all $a, b \in R$.***

**Proof.** (1) For $0 \in R$ we have $0 + 0 = 0$.

$\therefore$ $f(0+0) = f(0) \Rightarrow f(0) + f(0) = f(0) + 0'$ ($\because$ $f$ is homomorphism)

$\therefore$ $f(0) = 0'$ (by left cancellation law in $R'$)

(2) For $a \in R$ there exists $-a \in R$ so that $a+(-a)=0$.

$\therefore f(a+(-a)) = f(0) \Rightarrow f(a)+f(-a) = f(0) = 0'$. ($\because f$ is homomorphism)

$\therefore f(-a) = -f(a)$. ($\because f(a), f(-a) \in R'$, ring)

(3) For $a,b \in R$; $f(a-b) = f(a+(-b)) = f(a)+f(-b)$

$= f(a)-f(b)$ ($f(-b) = -f(b)$ By (2))

**Note 1.** A homomorphism maps the zero element of $R$ into the zero element of $R'$.

**2.** A homomorphism maps the negative '$-a$' of each element $a \in R$ into the negative in $R'$ of the corresponding element $a'$.

**Remark.** If the rings $R, R'$ have unity elements 1, 1' respectively then it does not necessarily follow that $f(1)=1'$ is true.

However if $R'$ is an integral domain then $f(1)=1'$ is true.

**Theorem 2.** ***The homomorphic image of a ring is a ring.*** **(*S. V. U. 04*)**

**Proof.** Let $R, R'$ be two rings and $f: R \to R'$ be a homomorphism.

By definition, homomorphic image of $R = \bar{R} = f(R) = \{ f(x) \in R' \mid x \in R \}$.

To prove that $f(R)$ is a ring, we show that $f(R) = \bar{R}$ is a subring of $R'$.

For $0 \in R, f(0) = 0' \in R'$. $\therefore f(0) = 0' \in \bar{R}$ and hence $\bar{R} \subset R'$.

Let $a', b' \in \bar{R}$.

$\therefore$ There exist $a, b \in R$ so that $f(a) = a', f(b) = b'$.

Since $a, b \in R$ we have $a-b, ab \in R$ and hence $f(a-b), f(ab) \in \bar{R}$.

Now $a'-b' = f(a)-f(b) = f(a-b) \in \bar{R}$ (Theorem (1))

$a'b' = f(a)f(b) = f(ab) \in \bar{R}$. (Homomorphism property (2))

Thus $a', b' \in \bar{R} \Rightarrow a'-b', a'b' \in \bar{R}$.

$\therefore \bar{R}$ is a subring of $R'$ and hence $\bar{R}$ is a ring.

**Corollary.*The homomorphic image of a commutative ring is a commutative ring.***

**Proof.** Let $R$ be a commutative ring and $\bar{R} = f(R)$ be its homomorphic image.

$a', b' \in \bar{R} \Rightarrow a'b' = f(a)f(b)$ where $a, b \in R$

$= f(ab) = f(ba) = f(b)\, f(a) = b'a'$. ($\because R$ is commutative)

$\therefore f(R) = \bar{R}$ is commutative.

**Theorem 3.** *If $f: R \to R'$ be an isomorphism from the ring R to the ring $R'$ then*

*(i) $f(0) = 0'$ where $0, 0'$ are the zero elements of $R, R'$.* ( *O. U.97*)

*(ii) for each $a \in R$, $f(-a) = -f(a)$.*

*(iii) $R'$ is a commutative ring if R is a commutative ring,*

*(iv) $R'$ is an integral domain if R is an integral domain. and*

*(v) $R'$ is a field if R is a field.*

**Proof.** For **(*i*), (*ii*)** and **(*iii*)** see the proof of Theorem (1) of Art 3.1 and its corollary.

**(*iv*)** Since $f(0) = 0'$ and $f$ is one-one we have that $0 \in R$ is the only element whose image is $0' \in R'$. Let $a', b' \in R'$ and $a' \neq 0', b' \neq 0'$.

Then there exist $a, b \in R$ and $a \neq 0, b \neq 0$ so that $f(a) = a'$, $f(b) = b'$.

$a, b \in R, a \neq 0, b \neq 0$ and $R$ has no zero divisors $\Rightarrow ab \neq 0$. ($R$ is I.D.)

$\Rightarrow f(ab) \neq f(0)$ ($\because f$ is one-one )

$\Rightarrow f(a)\, f(b) \neq 0' \Rightarrow a'b' \neq 0'$. $\therefore$ $R'$ is without zero divisors.

Let $1 \in R$ be the unity element. Then $f(1) \in R'$ and say $f(1) = 1'$.

For $a' \in R'$ there exist unique $a \in R$ so that $f(a) = a'$.

For each $a' \in R', a'1' = f(a) f(1) = f(a1) = f(a) = a'$.

$\therefore$ $a'1' = 1'a' = a' \Rightarrow f(1) = 1'$ is the unity element of $R'$.

Hence $R'$ is an integral domain.

**(*v*)** If $R$ is a field then (*a*) $R$is commutative, (*b*) $R$ has unity element and

(*c*) every non-zero element of $R$ has multiplicative inverse.

By (*iii*) and (*iv*) $R'$ is commutative and has unity element $1' = f(1)$ for $1 \in R$.

Let $a' \in R'$ and $a' \neq 0'$. There exists $a \in R$ so that $f(a) = a'$.

$a = 0 \Rightarrow f(a) = f(0) \Rightarrow a' = 0'$ and hence $a \neq 0$.

Since $R$ is a field, there exists $a^{-1} \in R$ so that $aa^{-1} = 1 = a^{-1}a$.

$\therefore$ $f(aa^{-1}) = f(1) \Rightarrow f(a)\, f(a^{-1}) = 1' = f(a^{-1})\, f(a)$.

Hence $f(a^{-1}) = f(a)^{-1}$ is the multiplicative inverse of $f(a) = a'$.

$\therefore$ $R'$ is a field.

**Theorem 4.** *Let $R, R'$ be two rings and $f: R \to R'$ be a homomorphism. For every ideal $U'$ in the ring $R'$, $f^{-1}(U')$ is an ideal in R.*

**Proof.** Let $U = f^{-1}(U') = \{ x \in R \mid f(x) \in U' \}$.

$f(0) = 0' \in U' \Rightarrow 0 \in f^{-1}(U') = U$. $\therefore U \neq \phi$ and $U \subset R$.

Let $a, b \in U$. By the def. of $U = f^{-1}(U')$; $f(a), f(b) \in U'$.

$U'$ is an ideal, $f(a), f(b) \in U' \Rightarrow f(a) - f(b) \in U'$

$\Rightarrow f(a-b) \in U' \Rightarrow a - b \in f^{-1}(U') = U$ $\therefore a, b \in U \Rightarrow a - b \in U$ ... (1)

Let $a \in U, r \in R$. Then $f(a) \in U'$ and $f(r) \in R'$.

Since $U'$ is an ideal in $R'$; $f(a)f(r), f(r)f(a) \in U'$

$\Rightarrow f(ar), f(ra) \in U' \Rightarrow ar, ra \in U$. $\therefore a \in U, r \in R \Rightarrow ar, ra \in U$ .... (2)

Hence $U = f^{-1}(U')$ is an ideal in $R$.

**Note.** If $S'$ is a subring of $R'$ then $f^{-1}(S')$ is a subring of $R$.

**Theorem. 5.** ***Let $R, R'$ be two rings and $f : R \to R'$ be a homomorphism. For every ideal $U$ in $R$, $f(U)$ is an ideal in $\bar{R} = f(R)$.***

**Proof.** $f(U) = \{ f(x) \mid x \in U \}$.

$0 \in U \Rightarrow f(0) = 0' \in f(U) \Rightarrow f(U) \neq \phi$ and $f(U) \subset f(R)$.

Let $a', b' \in f(U)$. There exist $a, b \in U$ such that $f(a) = a', f(b) = b'$.

$\therefore a' - b' = f(a) - f(b) = f(a-b) \in f(U)$ ($\because a, b \in U$ and $U$ is an ideal) ... (1)

Let $a' \in f(U)$ and $r' \in f(R) = \bar{R}$.

There exist $a \in U, r \in R$ such that $f(a) = a', f(r) = r'$

$a \in U, r \in R$ and $U$ is an ideal $\Rightarrow ar, ra \in U \Rightarrow f(ar), f(ra) \in f(U)$

$\Rightarrow f(a).f(r), f(r).f(a) \in f(U)$ ($\because f$ is homomorphism )

$\Rightarrow a'r', r'a' \in f(U)$ ... (2)

From (1) and (2) : $f(U)$ is an ideal in $f(R) = \bar{R}$.

**Note.1.** If $f : R \to R'$ is **onto homomorphism** then for every ideal $U$ in $R$, $f(U)$ is an ideal in $R'$.

**2.** The above theorem is true for a subring.

## 11. 2. KERNEL OF A HOMOMORPHISM

**Definition. (Kernel).** *Let $R, R'$ be two rings and $f : R \to R'$ be a homomorphism. The set $\{ x \in R \mid f(x) = 0' \}$ where $0' \in R'$ is the zero element, is defined as the Kernel of the homomorphism $f$.* ***(S. V. U. 00, N. U. 95, O. U. 08)***

The kernel of the homomorphism $f : R \to R'$ is denoted by **Ker $f$** or **$I$ ($f$).**

**Note.1.** If $f : R \to R'$ is a homomorphism then Ker $f = f^{-1}\{0'\} \subset R$.

**2.** For $0 \in R$ we have $f(0) = 0'$. Therefore $0 \in$ Ker $f$ and hence Ker $f \neq \phi$.

**e.g. 1.** Consider the Zero homomorphism $f : R \to R'$ defined by $f(x) = 0' \ \forall \ x \in R$.

Ker $f = \{ x \in R \mid f(x) = 0' \} = \{ x \in R \mid \forall \ x \in R \} = R$.

**e.g. 2.** Consider the identity homomorphism $f : R \to R$ defined by $f(x) = x \ \forall \ x \in R$.

Ker $f = \{ x \in R \mid f(x) = 0 \} = \{ x \in R \mid x = 0$ only $\}$ ($\because \ f(0) = 0$) $= \{ 0 \}$.

**Theorem 1.** ***If $f$ is a homomorphism of a ring $R$ into a ring $R'$ then Ker $f$ is an ideal of $R$.*** **(*S. V. U. 00, N. U. 07, O. U. 03*)**

**Proof.** If $0 \in R$ is the zero element of $R$ then $f(0) = 0'$, the zero element of $R'$.

$\therefore \ 0 \in$ Ker $f$ and hence Ker $f \neq \phi$ , Ker $f \subset R$.

Let $a, b \in$ Ker $f$ and $r \in R$. Then $f(a) = 0', f(b) = 0'$.

$f(a-b) = f(a) - f(b) = 0' - 0' = 0' \Rightarrow a - b \in$ Ker $f$

$f(ar) = f(a) \ f(r) = 0' \ \ f(r) = 0'$ and $f(ra) = f(r) \ f(a) = f(r) \ 0' = 0' \Rightarrow ar, ra \in$ Ker $f$.

$\therefore \ a, b \in$ Ker $f, r \in R \Rightarrow a - b \in$ Ker $f$ and $ar, ra \in$ Ker $f$.

Hence Ker $f$ is an ideal of $R$.

**Theorem 2.** ***If $f$ is a homomorphism of a ring $R$ into the ring $R'$ then $f$ is an into isomorphism if and only if Ker $f = \{0\}$.*** **(*A. U. 12, 08, S. K. D.08, S.V. U. 00, K. U. 05*)**

**Proof.** Let $f$ be an into isomorphism. That is, $f$ is one-one homomorphism.

We prove that Ker $f = \{0\}$.

$a \in R, f(a) = 0' \Rightarrow f(a) = f(0) \Rightarrow a = 0$ ($\because \ f$ is one-one )

$\therefore \ 0 \in R$ is the only element in $R$ so that $f(0) = 0'$.

$\therefore$ By definition, Ker $f = \{0\}$.

**Conversely,** let Ker $f = \{0\}$. We now prove that $f$ is one-one.

$a, b \in R$ and $f(a) = f(b) \Rightarrow f(a) - f(b) = 0' \Rightarrow f(a-b) = 0'$

$\Rightarrow a - b \in$ Ker $f = \{0\} \Rightarrow a - b = 0 \Rightarrow a = b$. $\therefore \ f$ is one-one.

**Note.** Ker $f = \{0\} \Leftrightarrow f$ is one-one..

**Theorem 3.** ***If $U$ is an ideal of a ring $R$ then the quotient ring $R/U$ is a homomorphic image of $R$.*** **(*S. V. U. 05, O. U. 05*)**

***Or***

***Every quotient ring of a ring is a homomorphic image of the ring.***

**Proof.** We know that $R/U = \{ x+U \mid x \in R \}$ is a ring with respect to addition and multiplication of cosets defined as $(a+U)+(b+U) = (a+b)+U$

and $(a+U).(b+U) = ab+U$ where $a+U, b+U \in R/U$.

Let $f : R \to R/U$ be a mapping defined by $f(a) = a+U$ for all $a \in R$.

For $a, b \in R, a = b \Rightarrow a+U = b+U \Rightarrow f(a) = f(b)$.

$\therefore$ the mapping $f$ is well defined.

For $a, b \in R ; f(a+b) = (a+b)+U = (a+U)+(b+U) = f(a)+f(b)$

and $f(ab) = ab+U = (a+U).(b+U) = f(a).f(b)$

$\therefore$ $f$ is a homomorphism.

Let $x+U \in R/U$. Then $x \in R$ and for this $x \in R$ we have $f(x) = x+U$.

$\therefore$ for each $x+U \in R/U$ there exists $x \in R$ so that $f(x) = x+U$.

$\therefore$ $f$ is onto mapping.

Hence $f : R \to R/U$ is an onto homomorphism.

**Note.** Ker $f = \{ x \in R \mid f(x) = 0+U \} = \{ x \in R \mid x+U = 0+U \}$

$= \{ x \in R \mid x \in U \} = U$.

In view of this result, the above theorem can also be stated as follows :

"Every ideal in a ring $R$ is the Kernel of some homomorphism defined on $R$".

$f : R \to R/U$ is called **Canonical homomorphism.**

**e.g.** $Z_6 = \{0,1,2,3,4,5\}$ under addition and multiplication modulo - 6 is a ring.

$U = \{0,3\}$ is an ideal of $Z_6$ and $Z_6/U = \{0+U, 1+U, 2+U\}$ = set of 3 elements.

Take $Z_3 = \{0,1,2\}$.

By the correspondence $f(0) = 0+U, f(1) = 1+U$ and $f(2) = 2+U$; $Z_3$ and $Z_6/U$ are isomorphic.

**Theorem 4. (Fundamental theorem of homomorphism)**

***Let $R, R'$ be two rings and $f : R \to R'$ be homomorphism with Kernel U. Then $\overline{R}$ is isomorphic to $R/U$.*** **(*N. U. 97, O. U. 07, S. V. U. 99, K. U. 12, 05, 08, S. K. U. 05*)**

**Proof.** $a \in$ Ker $f = U \Rightarrow f(a) = 0'$ where $0'$ is the zero element of $R'$.

Since $U$ is an ideal of $R, R/U = \{ x+U \mid x \in R \}$ is the quotient ring of cosets under addition and multiplication of cosets.

Since $f : R \to R'$ is homomorphism, $f(R) = \overline{R}$ is a ring.

That is, for each $f(x) \in \overline{R}$ we have $x \in R$.

Define $\phi = R/U \to \overline{R}$ by $\phi(x+U) = f(x) \; \forall \; x+U \in R/U$

$a+U, b+U \in R/U$ and $a+U = b+U \Leftrightarrow a-b \in U$

$\Leftrightarrow \quad f(a-b) = 0' \Leftrightarrow f(a) - f(b) = 0' = f(0) \Leftrightarrow f(a) = f(b) \Leftrightarrow \phi(a+U) = \phi(b+U)$.

$\therefore$ $\phi$ is well defined and one-one mapping.

Let $y \in \bar{R}$.

Since $f : R \to \bar{R}$ is onto, there exists $x \in R$ so that $f(x) = y$. For this $x \in R$ we have $x+U \in R/U$.

$\therefore$ for each $y \in \bar{R}$ there exists $x+U \in R/U$ so that $\phi(x+U) = f(x) = y$.

$\therefore$ $\phi$ is onto mapping.

Let $a+U, b+U \in R/U$. Then $a, b \in R$.

$\phi[(a+U)+(b+U)] = \phi[(a+b)+U] = f(a+b)$ (Definition of $\phi$)

$= f(a) + f(b) = \phi(a+U) + \phi(b+U)$ ($\because f$ is homomorphism)

$\phi[(a+U)(b+U)] = \phi[a.b+U] = f(ab)$

$= f(a)\, f(b) = \phi(a+U)\, \phi(b+U)$ ($\because f$ is homomorphism)

$\therefore$ $\phi$ is a homomorphism.

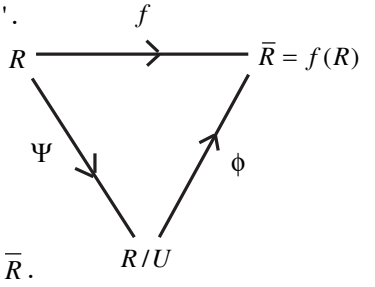
Hence $\phi$ is an isomorphism from $R/U$ to $\bar{R} = f(R)$.

**Note. 1.** Every homomorphic image of a ring $R$ is isomorphic to some quotient ring there of.

**2.** If $f : R \to R'$ is onto homomorphism from a ring $R$ to the ring $R'$ and $U$ is an ideal of $R$ then $R/U$ is isomorphic to $R'$.

Then $f(R) = \bar{R} = R'$. In the above proof replace $\bar{R}$ by $R'$.

**3.** $\bar{R} = f(R)$ = the homomorphic image of $R$.




Let $\Psi : R \to R/U$ be the Canonical homomorphism.

By fundamental theorem $\phi : R/U \to \bar{R}$ is isomorphism.

For $x \in R$ we have $\Psi(x) = x+U \in R/U$.

For this $x+U \in R/U$ we have $\phi(x+U) = f(x) \in f(R) = \bar{R}$.

Also, for $x \in R$ we have $f(x) \in f(R) = \bar{R}$. Therefore, $\phi \bullet \Psi = f$.

## SOLVED PROBLEMS

**Ex. 1.** *Is the ring* $2Z$ *isomorphic to ring* $3Z$ ?

**Sol.** $2Z = \{2n \mid n \in Z\}$ and $3Z = \{3n \mid n \in Z\}$.

Define $f : 2Z \to 3Z$ by $f(2x) = 3x \; \forall \; 2x \in 2Z$. Let $2m, 2n \in 2Z$.

$f(2m+2n) = f(2(m+n)) = 3(m+n) = 3m+3n = f(2m)+f(2n)$

$f(2m\,.\,2n) = f(2(2mn)) = 3(2mn) \neq 3m\,.\,3n = f(2m)\,f(2n)$

$\therefore$ The correspondence $f$ does not preserve multiplication.

$\therefore$ Ring $2Z$ is not isomorphic to ring $3Z$.

**Ex. 2.** *Let $Z_4, Z_{10}$ be modulo-4 and modulo - 10 rings. If $f: Z_4 \to Z_{10}$ is defined by $f(x) = 5x \;\forall\; x \in Z_4$ then prove that $f$ is a homomorphism.*

**Sol.** Let $a, b \in Z_4$. Let $a+b = 4q_1 + r_1$ and $a\,.\,b = 4q_2 + r_2$ where $0 \le r_1, r_2 < 4$.

$f(a+b) = f(r_1) = 5r_1 = 5(a+b-4q_1)$

$= 5a+5b-20q_1 = 5a+5b$ (modulo 10) $= f(a)+f(b)$ in $Z_{10}$.

$f(a\cdot b) = f(r_2) = 5r_2 = 5(ab-4q_2) = 5ab-20q_2$

$= 5ab\,(\text{mod}10) = 25ab\,(\text{mod}10) = 5a\,.\,5b = f(a)\,.\,f(b)$ in $Z_{10}$.

$\therefore$ $Z_4$ is homomorphic to $Z_{10}$.

**Ex. 3.** *Prove or disprove that $f: M_2(Z) \to Z$ defined by*

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a \;\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(Z)$$ *is a ringhomomorphism.*

**Sol.** Let $A_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, A_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in M_2(Z)$ where $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in Z$.

By definition of $f$, $f(A_1) = a_1$, $f(A_2) = a_2$.

$$f(A_1 + A_2) = f\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix} = a_1+a_2 = f(A_1)+f(A_2)$$

$\therefore f$ preserves addition.

$$f(A_1\,.\,A_2) = f\begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix} = a_1a_2+b_1c_2 \neq a_1a_2 = f(A_1)\,.\,f(A_2)$$

$f$ does not preserve multiplication. $\therefore f$ is not a homomorphism.

**Ex. 4.** *Let $Z(\sqrt{2}) = \{m+n\sqrt{2} \mid m,n \in Z\}$ be a ring under addition and multiplication of numbers. Prove that $f: Z(\sqrt{2}) \to Z(\sqrt{2})$ defined by*

$f(m+n\sqrt{2}) = m-n\sqrt{2} \;\;\forall\; m+n\sqrt{2} \in Z(\sqrt{2})$ *is an automorphism. Also find Ker f.*

**Sol.** Let $a, b \in Z(\sqrt{2})$ so that $a = m_1 + n_1\sqrt{2}$, $b = m_2 + n_2\sqrt{2}$ where $m_1, n_1, m_2, n_2 \in Z$.

Then we have $a+b = (m_1+m_2)+(n_1+n_2)\sqrt{2}$ and

$ab = (m_1m_2+2n_1n_2)+(m_1n_2+m_2n_1)\sqrt{2}$. Clearly $f$ is well defined.

By definition of $f$ ;

$f(a+b) = (m_1+m_2)-(n_1+n_2)\sqrt{2} = (m_1-n_1\sqrt{2})+(m_2-n_2\sqrt{2}) = f(a)+f(b)$ and

$f(ab) = (m_1m_2 + 2n_1n_2) - (m_1n_2 + m_2n_1)\sqrt{2} = (m_1 - n_1\sqrt{2})(m_2 - n_2\sqrt{2}) = f(a)f(b)$

$\therefore$ $f$ is an endomorphism.

$a, b \in Z(\sqrt{2})$ ; $f(a) = f(b) \Rightarrow m_1 - n_1\sqrt{2} = m_2 - n_2\sqrt{2}$

$\Rightarrow$ $m_1 = m_2$ and $n_1 = n_2 \Rightarrow m_1 + n_1\sqrt{2} = m_2 + n_2\sqrt{2} \Rightarrow a = b$

$\therefore$ $f$ is one-one. Let $y = m + n\sqrt{2} \in Z(\sqrt{2})$, the co-domain of $f$.

Then $x = m - n\sqrt{2} \in Z(\sqrt{2})$, the domain of $f$, exists so that

$f(x) = f(m - n\sqrt{2}) = m - (-n\sqrt{2}) = m + n\sqrt{2} = y$ .

$\therefore$ For each $y \in Z(\sqrt{2})$ there exists $x \in Z(\sqrt{2})$ so that $f(x) = y$ .

$\therefore$ $f$ is onto. Hence $f$ is an automorphism.

$f(m + n\sqrt{2}) = m - n\sqrt{2} = 0$, zero element of $Z(\sqrt{2}) \Rightarrow m = 0, n = 0 \Rightarrow m + n\sqrt{2} = 0$, zero element. $\therefore$ $\ker f = \{0\}$ .

**Ex. 5.** *Let Zbe the ring of intergers and $Z_n$ be the ring of residue classes modulo n. If a mapping $f : Z \to Z_n$ is defined by $f(x) = \bar{r}$ $\forall$ $x \in Z$ where $x \equiv r \pmod n$ ) prove that f is a homomorphism. Also find Ker f.*

**Sol.** Let $x, y \in Z$ .

By the definition of $f$ ; $f(x) = \bar{r}$, $f(y) = \bar{s}$ where $x \equiv r \pmod n$ and $y \equiv s \pmod n$.

Clearly $f$ is well defined. We know that $(i)$ $x \equiv r \pmod n$ ,

$y \equiv s \pmod n \Rightarrow x + y \equiv r + s \pmod n$ and $xy \equiv rs \pmod n$ and $(ii)$ $\overline{r+s} = \bar{r} + \bar{s}, \overline{rs} = \bar{r}\,\bar{s}$ .

Now $f(x + y) = \overline{r+s} = \bar{r} + \bar{s} = f(x) + f(y)$ and $f(xy) = \overline{rs} = \bar{r}\ \bar{s} = f(x)f(y)$ .

$\therefore$ $f$ is a homomorphism. Hence $Z_n$ is a homomorphic image of Z.

This is called the natural homomorphism from Z to $Z_n$ .

**Ex. 6.** *Let C be the ring of Complex numbers and $M_2(R)$ be the ring of $2\times2$ matrices. If $f : C \to M_2(R)$ is defined by $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ then prove that f is an into isomorphism or monomorphism. Also find Ker f* **(A. U. 00)**

**Sol.** Let $Z_1, Z_2 \in C$ and $Z_1 = x_1 + iy_1, Z_2 = x_2 + iy_2$ where $x_1, y_1, x_2, y_2 \in R$ .

Then $f(Z_1) = f(x_1 + iy_1) = \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix}$ and $f(Z_2) = f(x_2 + iy_2) = \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix}$

$$f(Z_1 + Z_2) = f((x_1 + x_2) + i\,(y_1 + y_2)) = \begin{pmatrix} x_1 + x_2 & y_1 + y_2 \\ -(y_1 + y_2) & x_1 + x_2 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} = f(Z_1) + f(Z_2)$$

$$f(Z_1 \cdot Z_2) = f((x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)) = \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + x_2y_1 \\ -(x_1y_2 + x_2y_1) & x_1x_2 - y_1y_2 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} = f(Z_1) \cdot f(Z_2)$$

$\therefore f$ is a homomorphism from C to $M_2(R)$.

$$f(Z_1) = f(Z_2) \Rightarrow \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} \Rightarrow x_1 = x_2, y_1 = y_2$$

$\Rightarrow x_1 + iy_1 = x_2 + iy_2 \Rightarrow Z_1 = Z_2$. $\therefore f$ is one - one.

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Z)$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ there is no complex number $a + ib \in C$ satisfying the correspondence.

$\therefore f$ is not onto. Hence $f$ is a monomorphism or into isomorphism.

**Note.** Instead of $M_2(R)$ if we take ring of $2\times2$ matrices $= S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in R \right\}$ then $f : C \to S$ will be isomorphism onto. $1 = 1 + 0i \in C$ is the unity in C, and

$$f(1) = f(1 + 0i) = \begin{pmatrix} 1 & 0 \\ -0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{unit matrix in } M_2(R)$$

$$f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \text{zero element in } M_2(R) \Rightarrow a = 0, b = 0$$

$\Rightarrow a + ib = 0 + i0 = 0 =$ Zero element in C. $\therefore$ Ker $f = \{0\}$

**Ex. 7.** *Let $R$ be the ring of integers and $R'$ be the set of even integers in which addition is same as that of integers and multiplication $(*)$ is defined by $a * b = ab/2 \ \forall \ a, b \in R'$. Prove that $R$ is isomorphic to $R'$.*

**Sol.** We know that $R' = \{2n \mid n \in Z\}$ is a commutative group under addition.

Let $a, b, c \in R'$ so that $a = 2m, b = 2n, c = 2p$ where $m, n, p \in Z$.

$a, b \in R' \Rightarrow a * b = (ab/2) = (2m)(2n)/2 = 2(mn) = 2q$ where $q \in Z$.

$\therefore \ *$ is a binary operation in $R'$.

$$a, b, c \in R' \Rightarrow (a * b) * c = \frac{ab}{2} * c = \frac{(ab/2)c}{2} = \frac{abc}{4} = \frac{a(bc/2)}{2} = a * \left(\frac{bc}{2}\right)$$

$$= a * (b * c) \qquad \therefore \ * \text{ is associative in } R'.$$

$$a, b, c \in R' \Rightarrow a * (b + c) = \frac{a(b + c)}{2} = \frac{ab}{2} + \frac{ac}{2} = a * b + a * c.$$

Similarly, $(b + c) * a = b * a + c * a$. $\therefore \ *$ is distributive over addition.

$a, b \in R'$ and $a * b = \frac{ab}{2} = \frac{ba}{2} = b * a \Rightarrow *$ is commutative in $R'$.

Hence $(R', +, *)$ is a commutative ring.

Define $f : R \to R'$ by $f(x) = 2x \ \forall \ x \in R$. Obviously $f$ is well defined.

Let $x, y \in R$ so that $x + y, xy \in R$. Then $f(x) = 2x, f(y) = 2y$.

Now $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$ and

$$f(xy) = 2(xy) = \frac{(2x)\,(2y)}{2} = 2x * 2y = f(x) * f(y).$$

$\therefore$ $f$ is a homomorphism from $R$ into $R'$.

$x, y \in R, f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y \Rightarrow f$ is one-one.

Let $b \in R'$. Then $b = 2a$ where $a \in R$ and for $a \in R$ we have $f(a) = 2a = b$.

$\therefore$ for each $b \in R'$ there exists $a \in R$ so that $b = f(a) \Rightarrow f$ is onto.

Hence $f$ is an isomorphism from $R$ to $R'$.

**Ex. 8.** *Prove that any homomorphism defined on a field is either isomorphism or zero homomorphism. Or, prove that a field has no proper homomorphic image.*

**Sol.** Let $F$ be a field and $R$ be a ring and $f : F \to R$ be a homomorphism.

Then we know that Ker $f$ is an ideal of the field $F$.

Since a field has no proper ideals either Ker $f = F$ or Ker $f = \{0\}$ where '0' is the zero element of $F$.

Let Ker $f = F$.

By definition of Ker $f$, we have $f(x) = 0' \ \forall \ x \in F$ where $0' \in R$ is the zero element.

$\therefore$ homomorphic image of $F = f(F) = \{0'\}$.

Hence, in this case, $f$ is a zero homomorphism. Let Ker $f = \{0\}$.

$\therefore$ By theorem (2) Art. 3.2, $f$ is an into isomorphism from $F$ to $R$.

Hence, in this case, homomorphic image of $F = f(F)$ is also a field.

**Ex. 9.** *Prove that $Z / \langle n \rangle$ or $Z / nZ$ is isomorphic to $Z_n$.*

**Sol.** Define $f : Z \to Z_n$ as $f(x) = \bar{r} \ \forall \ x \in Z$.

Then $f$ is a homomorphism (See Ex. 2.)

$\forall \ \bar{r} \in Z_n$ we have $r \in Z$ and for this $r \in Z$, $f(r) = \bar{r}$ $(\because r \equiv r \bmod n)$.

$\therefore$ $f : Z \to Z_n$ is onto homomorphism.

But Ker $f = nZ = \langle n \rangle$.

By fundamental theorem ; $Z / \text{Ker } f \cong Z_n$ *(i.e.,)* $Z / \langle n \rangle \cong Z_n$.

Further, if $n$ is a prime = $p$ then $Z_p$ is a field.

$Z / \langle p \rangle \cong Z_p \Rightarrow$ that a quotient ring of an integral domain is isomorphic to the field $Z_p$.

Hence a quotient ring of an integral domain may be a field.

**Note.** $Z_6 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$ is a ring and $U = \{ \bar{0}, \bar{3} \}$ is an ideal of $Z_6$.

$Z_6 / U = \{ \bar{0} + U, \bar{1} + U, \bar{2} + U \}$ contains only 3 elements.

If we define $\phi : Z_3 \to Z_6 / N$ as $\phi(\bar{0}) = \bar{0} + U$, $\phi(\bar{1}) = \bar{1} + U$, $\phi(\bar{2}) = \bar{2} + U$,

then $\phi$ is an isomorphism.

## EXERCISE 11

**1.** Is the ring $2Z$ is isomorphic to the ring $4Z$ ?

**2.** Show that $f : Z_5 \to Z_{10}$ defined by $f(x) = 5x \; \forall \; x \in Z_5$ does not preserve addition.

**3.** Show that $f : Z_4 \to Z_{12}$ defined by $f(x) = 3x \; \forall \; x \in Z_4$ does not preserve multiplication.

**4.** If $f : R \to R$ is defined by $f(x) = 2x$, is $f$ a homomorphism of rings? Give reasons.

**(*N. U. 1995*)**

**5.** If $F_1, F_2$ are two fields and $f : F_1 \to F_2$ is a non-zero ring homomorphism then prove that $f(a^{-1}) = (f(a))^{-1}$ for $a \neq 0 \in F_1$.

**6.** Let $R$ be a ring with unity element and $R'$ be a ring having atleast two elements. If $f : R \to R'$ is an onto homomorphism then prove that the ring $R'$ also has unity element.

**7.** In the above example (6) if $f$ is not onto homomorphism, does the ring $R'$ have unity element? Explain by giving an example.

**8.** Let $R = \{ m + i\,n \mid m, n \in Z \}$ be the ring of Gaussian integers and $Z$ be the ring of integers.

Is the function $f : R \to Z$ defined by $f(m + i\,n) = m \; \forall \; m + i\,n \in R$, a homomorphism?

**9.** Prove that $f : J[i] \to J[i]$ defined by $f(m + i\,n) = m - i\,n$ is an automorphism of the ring of Gaussian integers. (Hint. See Ex. (4) ) **(*O. U. 04* )**

**10.** Let $R' = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \, a \in R \right\}$ where $R$ is the ring of real numbers. Prove that $f : R' \to R$ defined by $f\left( \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \right) = a \; \forall \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in R'$ is an isomorphism.

**11.** Let $S=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a,b,c \in Z\right\} \subset M_2(Z)$. Prove that $f : S \to Z$ defined by $f\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a \; \forall \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in S$ is a ring homomorphism.

**12.** Let $Z[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in Z\}$ and let $M=\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} | a,b \in Z\right\} \subset M_2(Z)$. Show that the rings $Z[\sqrt{2}]$ and M are isomorphic.

**13.** $R$ is a commutative ring so that $px = 0$ for all $x \in R$ where $p$ is a prime. Prove that $f : R \to R$ defined by $f(x) = x^p \; \forall \; x \in R$ is a homomorphism.

**14.** Prove that $f : C \to C$, where C is the field of complex numbers, defined by $f(a+ib) = a - ib \; \forall \; a+ib \in C$ is a ring isomorphism.

## 11. 3. MAXIMAL IDEALS

The concept of maximal ideal of a ring is analogons to the idea of maximum normal subgroup in Group Theory.

**Definition. (Maximal Ideal).** *A maximal ideal M of a ring R is an ideal different from R such that there is no proper ideal U of R properly containing M.*

(or)

*Let R be a ring and M be an ideal of R so that* $M \neq R$. *M is said to be a maximal ideal of R if whenever U is an ideal of R such that* $M \subset U \subset R$ *then either* $R = U$ *or* $U = M$. ***(N.U. 97; O.U. 00)***

**Note 1.** $M$ is a maximal ideal of R if any ideal $U$ of $R$ containing $M$ is either $R$ or $M$.

**2.** An ideal $M$ of a ring $R$ is called a maximal ideal if $M$ is not included in any other ideal of $R$ except $R$ itself. That is, the only ideal that properly contains a maximal ideal is the entire ring.

**3.** If $M$ is a maximal ideal of the ring $R$ then there exists no ideal $U$ of $R$ so that $M \subset U \subset R$.

**Theorem. 1.** ***In the ring Z of integers the ideal generated by prime integer is a maximal ideal.*** ***(S. V. U. 05)***

**Proof.** Let $p$ be prime integer and $M = \langle p \rangle = pZ = \{pn \mid n \in Z\}$ be the ideal generated by $p$.

Let $U$ be any ideal so that $M \subset U \subset Z$

Since every ideal of Z is a principal ideal, $U$ is a principal ideal so that $U = \langle q \rangle$ where $q$ is an integer.

$M \subset U \subset Z \Rightarrow \langle p \rangle \subset \langle q \rangle \subset Z \Rightarrow p \in \langle q \rangle \Rightarrow p = qm, m \in Z$.

Since $p$ is a prime, either $q = 1$ or $m = 1$

$m = 1 \Rightarrow p = q \Rightarrow \langle p \rangle = \langle q \rangle \Rightarrow M = U$ ; $q = 1 \Rightarrow \langle q \rangle = Z \Rightarrow U = Z$

$\therefore$ $M$ is a maximal ideal.

**Note.** An ideal generated by compostie integer is not a maximal ideal.

Consider $M = \langle 6 \rangle = \{ ..., -12, -6, 0, 6, 12, ... \}$, the ideal generated by composite integer 6.

There exists ideal $U = \langle 3 \rangle = \{ ..., -12, -9, -6, -3, 0, 3, 6, ... \}$ so that $M \subset U \subset Z$

**Theorem. 2.** ***If M is a maximal ideal of the ring of integers Z then M is generated by prime integer.*** **(*O. U. 05, S. V. U. 04*)**

**Proof.** Let $M = \langle n \rangle$ where $n \in Z$ be maximal ideal of $Z$.

We prove that $n$ is a prime integer.

If possible, suppose that $n = ab$ where $a$, $b$ are prime integers.

Then $U = \langle a \rangle$ is an ideal of $Z$ and $U \supset M$ so that $M \subset U \subset Z$

Since $M$ is maximal ideal of $Z$, by the definition either $U = Z$ or $M = U$.

**Case (*i*).** Let $U = Z$. Then $U = \langle a \rangle = \langle 1 \rangle$ so that $a = 1$

$\therefore$ $n = ab = b \Rightarrow n$ is a prime integer.

**Case (*ii*).** Let $M = U$

Then $U = \langle a \rangle = M \Rightarrow a \in M \Rightarrow a \in \langle n \rangle \Rightarrow a = r\,n$ for some $r \in Z$.

$\therefore$ $n = ab = (r\,n)\,b = n\,(r\,b) \Rightarrow 1 = r\,b \Rightarrow r = 1, b = 1$.

$\therefore$ $n = a\,(1) = a \Rightarrow n$ is a prime integer.

From cases (*i*) and (*ii*) we have that $n$ is a prime integer.

**Note. 1.** For the ring of integers $Z$, any ideal generated by prime integer is a maximal ideal.

**2.** A ring may have more than one maximal ideal. For example, the ring $Z$ has $\langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, ....$ as maximal ideals.

**Theorem. 3.** ***An ideal in Z is a maximal ideal if and only if it is generated by a prime integer.*** **(*O. U. 04* )**

**Proof.** Write the proofs of Theorems (1) and (2).

**Theorem. 4.** ***An ideal U of a commutative ring R with unity is maximal if and only if the quotient ring R/U is a field.***

**(*A. U. 12, N. U. 08,O.U. 07, S.K.U. 01, 05, K.U. 05, S.V.U, 08*)**

**Proof.** $R$ is commutative ring with unity and $U$ is an ideal $\Rightarrow$ the quotient ring $R/U = \{ x + U \mid x \in R \}$ is commutative and has unity element. (Art. 2.6)

Zero element of $R/U = 0 + U = U$ where $0 \in R$ is the zero element in $R$.

Unity element of $R/U = 1 + U$ where $1 \in R$ is the unity element in $R$.

It is to be noted that $a+U=U$ zero element of $R/U \Leftrightarrow a \in U$

(1) Suppose that $U$ is a maximal ideal of $R$. We prove that $R/U$ is a field.

To prove that $R/U$ is a field we have to show that every non-zero element of $R/U$ has multiplicative inverse.

Let $x+U \in R/U$ and $x+U$ be non-zero element. Then $x \notin U$

If $\langle x \rangle$ is the principal ideal of $R$ then $\langle x \rangle + U$ is also an ideal of $R$.

( $\because$ sum of two ideals is also an ideal. Ex. 4)

$x \notin U \Rightarrow U \subset \langle x \rangle + U$

Now we have, $U \subset \langle x \rangle + U \subseteq R$ and $U$ is maximal ideal $\Rightarrow \langle x \rangle + U = R = \langle 1 \rangle$

$\Rightarrow$ there exists $a \in U$ and $\alpha \in R$ such that $a + x\alpha = 1$

$\therefore 1+U = (a+x\alpha)+U = (a+U)+(x\alpha+U)$ (sum of cosets)

$= U + (x\alpha+U) = (0+U)+(x\alpha+U)$ $(\because a \in U \Rightarrow a+U=U)$

$= x\alpha + U = (x+U)(\alpha+U)$ (Product of cosets)

$\therefore$ for non-zero element $x+U \in R/U$ there exists $\alpha+U \in R/U$ such that $(x+U)(\alpha+U)=1+U$.

Hence every non-zero element of $R/U$ is invertible.

$\therefore$ $R/U$ is a field.

(2) suppose that $R/U$ is a field. We prove that $U$ is maximal ideal.

Let $U'$ be an ideal of $R$ so that $U' \supset U$ and $U' \neq U$

Now we show that $U' = R$

Since $U' \supset U$ and $U' \neq U$, there exists $\alpha \in U'$ such that $\alpha \notin U$

$\alpha \notin U \Rightarrow \alpha + U$ is non-zero element of $R/U$

$R/U$ is a field of $\alpha+U$ is non-zero element of $R/U$

$\Rightarrow \alpha+U$ has multiplicative inverse, say $x+U$.

$\therefore (\alpha+U)(x+U) = 1+U$

$\Rightarrow \alpha x + U = 1+U \Rightarrow 1-\alpha x \in U \subset U'$ $(\because a+U=b+U \Rightarrow a-b \in U)$

$x \in R, \alpha \in U'$ and $U'$ is an ideal $\Rightarrow \alpha x \in U'$.

$\alpha x \in U', 1-\alpha x \in U' \Rightarrow \alpha x + (1-\alpha x) = 1 \in U'$

$\therefore 1 \in U'$ and $U'$ is an ideal $\Rightarrow U' = R$. Hence $U$ is a maximal ideal.

## 11. 4. PRIME IDEALS

**Definition. (Prime Ideal)** *An ideal $U \neq R$ of a commutative ring $R$ is said to be prime ideal if for all $a,b \in R$ and $a,b \in U \Rightarrow a \in U$ or $b \in U$.*

**e.g.** For an integral domain $R$, the null ideal is a prime ideal.

$\because\ a,b \in R,\ ab \in \langle 0\rangle \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$

**Theorem.** ***An ideal $U \neq R$ of a commutative ring R, is a prime ideal if and only if $R/U$ is an integral domain.*** **(S. K. U. 07, 05 S. V. U. 01, O. U. 05)**

**Proof.** Let $R/U$ be an integral domain.

We now prove that $U$ is a prime ideal of $R$.

$\forall\ a,b \in R$ and $a,b \in U \Rightarrow ab+U = U \Rightarrow (a+U).(b+U) = 0+U$

$\Rightarrow a+U = 0+U$ or $b+U = 0+U$ ( $0+U$ is the zero element of $R/U$ )

$\Rightarrow a \in U$ or $b \in U$. $\therefore\ U$ is a prime ideal of $R$.

**Conversely,** let $U$ be a prime ideal of $R$.

We now prove that $R/U$ is an integral domain.

$a+U, b+U \in R/U$ and $(a+U).(b+U) = 0+U$

$\Rightarrow ab+U = 0+U \Rightarrow ab \in U \Rightarrow a \in U$ or $b \in U$ ( $\because\ U$ is prime ideal)

$\Rightarrow a+U = 0+U$ or $b+U = 0+U$

$\therefore\ R/U$ has no zero divisors and hence is an integral domain.

**Corollary.** ***Every maximal ideal of a commutative ring R with unity is a prime ideal.*** **(K. U. 03, N. U. 01, O. U. 97)**

**Proof.** Let $U$ be a maximal ideal of a ring $R$.

By Theorem (3) of Art. 3.3; $R/U$ is a field. $\Rightarrow$ $R/U$ is an integral domain.

By Theorem (4) of Art. 3.3; $U$ is a prime ideal.

Thus every maximal ideal of $R$ is a prime ideal.

**Note. 1.** The converse of the above corollary is not true.

That is, a prime ideal of a commutative ring with unity need not be a maximal ideal.

Consider the integral domain $Z$ of integers.

The null ideal $= \langle 0\rangle$ of $Z$ is a prime ideal. But $\langle 0\rangle$ ideal is not maximal ideal.

There exists ideal $= \langle 2\rangle$ of $Z$ such that $\langle 0\rangle \subset \langle 2\rangle \subset Z$ and $\langle 2\rangle \neq \langle 0\rangle, \langle 2\rangle \neq Z$.

**Ex.** If $R = \{0,2,4,6\}$ is a ring with respect to addition and multiplication modulo 8, then show that $M = \{0,4\}$ is a maximal ideal of R but not a prime ideal . **(O. U. 11)**

**Sol.** For $0,0 \in M, 0-0 = 0 \in M$ , For $0,4$ or $4,0 \in M$ ,

$0-4 = 8-4 = 4 \in M$ , $4-0 = 4 \in M$ . For $4,4 \in M, 4-4 = 0 \in M$ .

For $0 \in M, 0,2,4,6 \in R$ we have $0.0 = 0, 0.2 = 0, 0.4 = 0, 0.6 = 0 \in M$

For $4 \in M, 0,2,4,6 \in R$ we have $4.0 = 0 \in M, 4.2 = 8 = 0 \in M, 4.4 = 16 = 0 \in M,$
$4.6 = 24 = 0 \in M$ .

$\therefore$ M is an ideal of R.

$U_1 = \{0,2,4\}$ is not an ideal, for, $2,4 \in U_1$ we have $2 - 4 = -2 = 6 \notin U_1$

$U_2 = \{0,4,6\}$ is not an ideal, for, $6,4 \in U_2$ we have $6 - 4 = 2 \neq U_2$ .

$\therefore$ There is no ideal U of R such that $M \subset U \subset R$ .

$\therefore M = \{0,4\}$ is a maximal ideal.

For $2,6 \in R$ and $2.6 = 12 = 4 \in M$ does not imply either $2 \in M$ or $6 \in M$

$\therefore$ M is not a prime ideal.

## 11. 5. FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

If an integral domain is such that every non-zero element of it has a multiplicative inverse then it is a field. But many integral domains do not form fields. Though the integral domain of integers is not a field, it is such that it can be embedded in the field of rational numbers. In this section we show that every integral domain can be regarded as being contained in a certain field. The minimal field containing an integral domain is called field of quotients of an integral domain.

**Theorem.** ***Every integral domain can be embedded in a field. (or)***
***An integral domain D can be embedded in a field F such that every element of F can be regarded a quotient of two elements of D.*** **(A. U. 08)**

**Proof.** Let $D$ be an integral domain with at least two elements.

Consider $S = \{(a,b) \mid a,b \in D, b \neq 0\}$. Then $S \neq \phi$ and $S \subset D \times D$.

For all $(a,b),(c,d) \in S$ define a relation ~ on $S$ as $(a,b) \sim (c,d)$ if and only if $ad = bc$.

We now prove that ~ is an equivalence relation on $S$.

(1) For each $(a,b) \in S$ we have $ab = ba$ which implies that $(a,b) \sim (a,b)$.

(2) $(a,b),(c,d) \in S$ and $(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)$.

(3) $(a,b),(c,d),(e,f) \in S$ and $(a,b) \sim (c,d),(c,d) \sim (e,f) \Rightarrow ad = bc, cf = de$.

$\Rightarrow (ad)f = (bc)f, cf = de \Rightarrow (af)d = b(de) = d(be) \Rightarrow af = be \quad (\because d \neq 0)$

$\Rightarrow (a,b) \sim (e,f)$

$\therefore$ '~' is an equivalence relation on $S$. The equivalence relation ~ partitions the set $S$ into equivalence classes which are either identical or disjoint.

For $(a,b) \in S$ let $a/b$ denote the equivalence class of $(a,b)$. Then $a/b = \{(x,y) \in S \mid (x,y) \sim (a,b)\}$. If $a/b, c/d$ are the equivalence classes of $(a,b),(c,d) \in S$ then either $a/b = c/d$ or $a/b \cap c/d = \phi$. It is evident that $a/b = c/d$ if and only if $ad = bc$.

Let $F$ denote the set of all the equivalence classes or the set of quotients.

Then $F = \left\{ \frac{a}{b} \,\middle|\, (a,b) \in S \right\}$. Since $D$ has at least two elements, say, $0, a \in D$

we have quotients $\frac{0}{a}, \frac{a}{a} \in F$ and $\frac{0}{a} \neq \frac{a}{a}$.

$\therefore$ the set $F$ has at least two elements.

For $\frac{a}{b}, \frac{c}{d} \in F$ define addition $(+)$ and multiplication $(\bullet)$ as

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} . \frac{c}{d} = \frac{ac}{bd}$.

Since $D$ is without zero divisors, $b \neq 0, d \neq 0 \in D \Rightarrow bd \neq 0$.

So $\frac{ad+bc}{bd}, \frac{ac}{bd} \in F$

Now we prove that the addition and multiplication defined above are well defined.

Let $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. Then $ab' = a'b$ and $cd' = c'd$ ... (I)

Now (I) $\Rightarrow ab'dd' = a'bdd'$ and $bb'cd' = bb'c'd$

$\Rightarrow ab'dd' + bb'cd' = a'bdd' + bb'c'd \Rightarrow (ad+bc)b'd' = (a'd'+b'c')bd$

$\Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$

Also (I) $\Rightarrow ab'cd' = a'bc'd \Rightarrow (ac)(b'd') = (a'c')(bd) \Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$.

$\therefore$ Addition and multiplication of quotients are well defined binary operations on $F$.

We now prove that $(F, +, \bullet)$ is a field.

(1) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$; $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)\,f + (bd)\,e}{(bd)\,f}$

$= \frac{a(df) + (cf+de)b}{b(df)} = \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) \Rightarrow$ addition is assocative.

(2) For $\frac{a}{b}, \frac{c}{d} \in F$; $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{bc+ad}{db} = \frac{c}{d} + \frac{a}{b} \Rightarrow$ addition is commutative.

(3) For $u \neq 0 \in D$ we have $\frac{0}{u} \in F$ such that $\frac{0}{u} + \frac{a}{b} = \frac{0b+ua}{ub} = \frac{ua}{ub} = \frac{a}{b} \; \forall \; \frac{a}{b} \in F$.

$\therefore \frac{0}{u} \in F$ is the zero element.

(4) Let $\frac{a}{b} \in F$. Then $\frac{-a}{b} \in F$ such that $\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-a)b}{b^2} = \frac{0}{b^2} = \frac{0}{u}$ $(\because 0u = 0b^2)$

$\therefore$ every element in $F$ has additive inverse.

(5) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$ ; $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$

$\therefore$ multiplication is associative.

(6) For $\frac{a}{b}, \frac{c}{d} \in F$ ; $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$

$\therefore$ multiplication is commutative.

(7) for $u \neq 0 \in D$ we have $\frac{u}{u} \in F$ such that $\frac{a}{b} \cdot \frac{u}{u} = \frac{au}{bu} = \frac{a}{b} \; \forall \; \frac{a}{b} \in F$

$\therefore \frac{u}{u} \in F$ is the unity element.

(8) Let $\frac{a}{b} \in F$ and $\frac{a}{b} \neq \frac{0}{u}$. Then $au \neq 0$ which implies that $a \neq 0$ as $u \neq 0$.

$\therefore b \neq 0$ and $a \neq 0 \Rightarrow \frac{b}{a} \in F$.

$\therefore$ for $\frac{a}{b}\left(\neq \frac{0}{u}\right) \in F$ there exists $\frac{b}{a} \in F$ such that $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{u}{u}$ $(\because (ab)u = (ba)u)$

$\therefore$ every non-zero element in $F$ has multiplicative inverse.

(9) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$ ; $\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{a(cf + de)}{b(df)} = \frac{(acf + ade)\,(bdf)}{(bdf)\,bdf)}$

$= \frac{acf \;\; bdf + ade \; bdf}{(bdf)\; bdf)} = \frac{acf}{bdf} + \frac{ade}{bdf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$

Similarly we can prove that $\left(\frac{c}{d} + \frac{e}{f}\right) \cdot \frac{a}{b} = \frac{c}{d} \cdot \frac{a}{b} + \frac{e}{f} \cdot \frac{a}{b}$.

$\therefore$ multiplication is distributive over addition.

In view of (1), (2), (3), (4), (5), (6), (7), (8) and (9) $(F, +, \bullet)$ is a field.

Now we have to prove that $D$ is embedded in the field $F$, that is, we have to show that there exists an isomorphism of $D$ into $F$.

Define the mapping $\phi : D \to F$ by $\phi(a) = \frac{ax}{x} \;\; \forall \;\; a \in D$ and $x(\neq 0) \in D$.

$a, b \in D$ and $\phi(a) = \phi(b) \Rightarrow \frac{ax}{x} = \frac{bx}{x} \Rightarrow (ax)x = (bx)x$

$\Rightarrow (a - b)x^2 = 0 \Rightarrow a - b = 0$ since $x^2 \neq 0 \quad \Rightarrow a = b$. $\quad \therefore \phi$ is one - one.

For $a, b \in D$ ; $\phi(a + b) = \frac{(a + b)x}{x} = \frac{(a + b)xx}{xx} = \frac{axx + bxx}{xx} = \frac{ax}{x} + \frac{bx}{x} = \phi(a) + \phi(b)$

$\phi(ab) = \frac{(ab)x}{x} = \frac{(ab)xx}{xx} = \frac{ax}{x} \cdot \frac{bx}{x} = \phi(a)\; \phi(b)$

$\therefore \phi$ is a homomorphism. Hence $\phi$ is an isomorphism of $D$ into $F$.

$\therefore$ the integral domain $D$ is embedded in the field $F$.

**Note. 1.** Every element in the field $F$ is in the form of a quotient of two elements in $D$. So, the field $F$ is called "field of quotients of $D$"

**2.** The equivalence class of $(a,b) \in S$ is also denoted as $[(a,b)]$ or $[a,b]$ or $(\overline{a,b})$.

Then $[(a,b)] = [(c,d)] \Leftrightarrow ad = bc$, $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$,

$[(a,b)] . [(c,d)] = [(ac, bd)]$,

the zero element of $F = [(0,1)]$ and the unity element of $F = [(1,1)]$

**3.** If $D$ is the ring of integers then the field $F$, constructed in the above theorem, would be the field $Q$ of rational numbers.

## 11. 6. PRIME FIELDS

**Definition.** *A field is said to be prime if it has no subfield other than itself .*

The field $Z_p = \{0,1,2,...,p-1\}$ where $p$ is a prime and the field $Q$, of the set of all rational numbers are prime fields. The field of real numbers $R$ is not a prime field.

We now establish that any field $F$ contains a subfield isomorphic to $Z_p$ or contains a subfield isomorphic to $Q$.

**Theorem. 1.** ***If R is a ring with unity element '1' then $f : Z \to R$ defined by $f(x) = n . 1 \; \forall \; n \in Z$ is a homomorphism.***

**Proof.** Let $m, n \in Z$. Then $f(m) = m . 1$, $f(n) = n . 1$.

$f(m+n) = (m+n) . 1 = m . 1 + n . 1 = f(m) + f(n)$

Let $m > 0, n > 0$.

$(mn) . 1 = 1+1+...+1$ ($mn$ times) $= \{(1+1+...+1)\, m \text{ times}\}$ $\{(1+1+...+1)\, n \text{ times}\}$

$= (m . 1)\,(n . 1)$ (using Distributivity in the ring $R$)

Similarly, $\forall \; m, n \in Z$ we can prove that $(m\,n) . 1 = (m . 1)\,(n . 1)$ using Distributivity.

$\therefore \; f(m\,n) = (m\,n) . 1 = (m . 1)\,(n . 1) = f(m) f(n)$.

Hence $f : Z \to R$ is a homomorphism.

**Theorem.2.** ***If R is a ring with unity element '1' and characteristic of $R = n > 0$ then R contains a sub ring isomorphic to $Z_n$.***

**Proof.** Consider the homomorphism $f : Z \to R$ defined by $f(m) = m . 1 \; \forall \; m \in Z$.

$\therefore$ Ker $f$ is an ideal of $Z$.

But every ideal in $Z$ is the form $\langle s \rangle = sZ$ where $s \in Z$.

Characteristic of ring $R = n > 0 \Rightarrow n$ is the least positive integer such that $n . 1 = 0$.

$\therefore$ Ker $f = nZ = \langle n \rangle$

By fundamental Theorem, $f(Z) \subseteq R$ is isomorphic to $Z/nz = Z/\langle n \rangle$.

But $Z/nz = Z/\langle n \rangle$ is isomorphic to $Z_n$. (See Ex. 7)

$\therefore$ $f(Z) \subseteq R$ is isomorphic to $Z_n$.

**Theorem.3.** ***If R is a ring with unity element '1' and characteristic of*** $R = 0$ ***then R contains a subring isomorphic to Z.***

**Proof.** Consider the homomorphism $f : Z \to R$ defined by $f(m) = m.1 \; \forall \; m \in Z$.

Characteristic of $R = 0 \Rightarrow m.1 \neq 0 \;\; \forall \;\; m \in Z$ and $m \neq 0$.

Ker $f = \{ m \in Z \mid f(m) = m.1 = 0 \} = \{0\}$. $\therefore$ $f(Z) \subseteq R$ is isomorphic to $Z$.

**Corollary.** ***A field F of prime characteristic*** $= p$ ***contains a subfield isomorphic to*** $Z_p$ ***and a field F of characteristic zero contains a subfield isomorphic to Q, the field of rational numbers.***

**Proof.** Let $F$ be the field of characteristic $= p$, a prime.

Then $p$ is the least positive integer such that $p.1 = 0$.

$\therefore$ Ker $f = p\,Z = \langle p \rangle$

Hence, by the above theorem; $F$ contains a subfield isomorphic to $Z_p$.

Let $F$ be the field of characteristic = 0.

By the above Theorem; $F$ contains a subring isomorphic to $Z$.

But the field F contains a field of quotients of $Z$ which is the field $Q$ of rational numbers.

Thus we have established that apart from isomorphism the only prime fields

are $Q$ and $Z_p$.

# Rings of Polynomials

## 12.1. POLYNOMIALS IN AN INDETERMINATE

In our earlier classes we have studied polynomials with some of the operations like adding, multiplying and factoring. Further we have studied their continuity, Derivative and Integral as functions.

Now we study polynomials as elements of a ring and its algebraic properties.

**Definition.** *Let R be a ring. A sequence* $(a_0, a_1, a_2, ..., a_n, ...)$ *of elements of R, with atmost a finite number of non-zero terms, is called a polynomial over the ring R.*

Since polynomial is a sequence with atmost a finite number of non-zero terms, $(a_0, a_1, ..., a_n, ...)$ is a polynomial over the ring $R$

$\Leftrightarrow$ there exists $n \in N$ such that $a_i = 0 \ \forall \ i > n$. So, we can write $f = (a_0, a_1, ..., a_n)$.

**Definition. (Another form)** *Let R be a ring. A polynomial* $f(x)$ *in the indeterminate* $'x'$ *with coefficients in R is* $a_0 + a_1x + a_2x^2 + ... + a_nx^n + ... = \sum_{i=0}^{\infty} a_i x^i$ *where* $a_i \in R$ *and* $a_i = 0$ *for all but a finite number of values of i.* **(O.U. 03)**

If $a_i = 0 \ \forall \ i > n$ then we can write $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$.

$a_0, a_1, a_2, ....., a_n, .....$ are called coefficients of $f(x)$.

$a_0, a_1x, a_2x^2, ..., a_nx^n, ...$ are called the constant term, the $x$ term, the $x^2$ term, ..... the $x^n$ term, ..... of $f(x)$.

The two forms of the definition are equivalent.

That is $f = (a_0, a_1, ..., a_n) \Leftrightarrow f(x) = a_0 + a_1x + ... + a_nx^n$.

**e.g.** If $Z$ is the ring of integers then $f(x) = 2 + 0x + 1x^2$, $g(x) = 2 + 1x + (-1)x^2$ are polynomials.

**Notation.** The set of all polynomials defined over the ring $R$ or with coefficients in the ring $R$ is denoted by $R[x]$.

The set of all polynomials defined with coefficients in the field $F$ is denoted by $F[x]$.

**Definition. (Zero polynomial).** *If* $'O'$ *is the zero element in the ring R, then* $f = (0, 0, ...., 0, .....)$ *is called zero polynomial.*

Zero polynomial is denoted by $O = (0, 0, ..., 0, ...)$ or $O(x) = 0 + 0x + 0x^2 + ...$.

**Definition. (Constant Polynomial).** *An element in the ring R is called a constant polynomial. That is, if* $a_0 \in R$ *then* $(a_0, 0, 0, ...) = a_0$ *is the constant polynomial which can be identified with the element* $'a_0'$ *of the ring.*

## 12. 2. ALGEBRA OF POLYNOMIALS

**Definition. (Equality of two polynomials).** *Two polynomials* $f = (a_0, a_1, ..., a_m)$ *and* $g = (b_0, b_1, ..., b_n)$ *in* $R[x]$ *are said to be equal if* $a_i = b_i \ \forall \ i \geq 0$. *We write* $f = g$.

$f(x) = a_0 + a_1x + ... + a_mx^m$ *and* $g(x) = b_0 + b_1x + ... + b_nx^n$ *are equal*

*i.e.* $f(x) = g(x) \Leftrightarrow a_i = b_i$ *for* $i = 0,1,2,...$ *i.e. their corresponding coefficients are equal.*

**Definition. (Addition of two polynomials)**

*Let* $f = (a_0, a_1, ..., a_m)$ *and* $g = (b_0, b_1, ..., b_n)$ *be two polynomials in* $R[x]$. *The sum of* $f$ *and* $g$ *denoted by* $f + g = (c_0, c_1, ..., c_p)$ *where* $c_i = a_i + b_i$ *for each* $i$.

Thus $f + g = (a_0 + b_0, a_1 + b_1, ...)$ or $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... = \sum_{i=0}^{\infty} (a_i + b_i)\, x^i$

The process of finding the sum of two polynomials is called addition.

**Note. 1.** To add two polynomials we have to add their corresponding coefficients and collect the terms.

**2.** If $f(x) = a_0 + a_1x + ... = \sum_{i=0}^{\infty} a_i\, x^i$ and $g(x) = b_0 + b_1x + ... = \sum_{j=0}^{\infty} b_j\, x^j$

then $f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k)\, x^k$ .

**e.g.** Let $f(x) = 1 + x,\ g(x) = 3 - 2x + x^2$ with coefficients in the ring $Z$ of integers.

By the definition.: $f(x) + g(x) = (1 + 1x + 0x^2) + (3 + (-2)x + 1x^2)$

$$= (1 + 3) + (1 - 2)x + (0 + 1)x^2 = 4 - x + x^2 .$$

**Definition. (Multiplication of two polynomials)**

*Let* $f = (a_0, a_1, ..., a_m)$ *and* $g = (b_0, b_1, ..., b_n)$ *be two polynomials in* $R[x]$.

*The product of f and g denoted by* $f \,.\, g$ *or* $f\ g = (d_0, d_1, ..., d_q)$ *where*

$$d_k = a_0b_k + a_1b_{k-1} + ... + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i} .$$

Thus $f \,.\, g = (a_0b_0 + a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, .....)$ or

$$f(x).\, g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ...$$

The process of finding the product of two polynomials is called Multiplication.

**Note. 1.** $d_k = \sum_{i=0}^{k} a_i\, b_{k-i} = \sum_{i+j=k} a_i\, b_j$ **Imp.** $f(x).g(x) = \sum_{k=0}^{\infty} d_k x^k = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i\, b_j\right) x^k$

**2.** From the definitions of sum and product of two polynomials $f, g$ we clearly observe that $f+g$ and $f.g$ are polynomials in $R[x]$.

**3.** The operations of addition $(+)$ and multiplication $(\bullet)$ in $f+g$ and $f.g$ of $f, g \in R[x]$ are respectively different from addition $(+)$ and multiplication $(\bullet)$ in $a+b$ and $a.b$ of $a, b \in R$.

**e.g.** Let $f(x) = 1+x$ and $g(x) = 3-2x+x^2$ with coefficients in the ring $Z$ of integers.

Here $f(x) = 1+1.x = a_0 + a_1x + a_2x^2 \Rightarrow a_0 = 1, a_1 = 1, a_2 = 0$, $a_3 = a_4 = \ldots = 0$.

$g(x) = 3+(-2)x+1.x^2 = b_0 + b_1x + b_2x^2 \Rightarrow b_0 = 3, b_1 = -2, b_2 = 1, b_3 = b_4 = \ldots = 0$.

By the definition of product of $f$ and $g$ we have

$f(x).g(x) = d_0 + d_1x + d_2x^2 + d_3x^3 + \ldots$ where $d_k = \sum_{i+j=k} a_i\, b_j$.

$d_0 = a_0b_0 = (1)(3) = 3$; $d_1 = a_0b_1 + a_1b_0 = (1)(-2) + (1)(3) = 1$;

$d_2 = a_0b_2 + a_1b_1 + a_2b_0 = (1)(1) + (1)(-2) + (0)(3) = -1$;

$d_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = (1)(0) + (1)(1) + (0)(-2) + (0)(3) = 1$

$d_4 = a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0 = (1)(0) + (1)(0) + (0)(1) + (0)(-2) + (0)(3) = 0$,

$d_5 = d_6 = \ldots. = 0$.

$\therefore\ f(x)\ g(x) = (1+x)(3-2x+x^2) = 3+1x+(-1)x^2+1x^3$.

If we multiply $f(x)$ and $g(x)$ in the high school style we get the same answer.

## 12. 3. DEGREE OF A POLYNOMIAL.

**Definition.** *Let $f = (a_0, a_1, a_2, \ldots)$ be a non-zero polynomial over a ring R. The largest integer $i > 0$ for which $a_i \neq 0$ is called the degree of f.* ***The degree of zero polynomial is not defined. The degree of constant polynomial is zero.*** **(A. U. 07, O.U. 03)**

Degree of $f(x) = \deg f(x) = n \Leftrightarrow f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ where

$a_n \neq 0$ and $a_i = 0\ \forall\ i > n$.

**Definition. (Leading coefficient of a polynomial)**

*If the degree of the polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n$ is n then $a_n \neq 0$ is called the leading or highest coefficient in $f(x)$.*

**Note.** Deg $f(x)$ is a non-negative integer.

**e.g. 1.** Deg $f(x) = 4 + 2x + 3x^4$ where $f(x) \in Z[x]$ is 4 and the leading coefficient = 3.

**e.g. 2.** If $f(x) = 3/2 \in Q[x]$, the ring of polynomials over Q then deg $f(x) = 0$.

**Theorem.** *Let $f(x), g(x)$ be two non-zero polynomials of $R[x]$, where $R$ is a ring. Then* (*i*) $\deg(f(x)+g(x)) \le \max\{\deg f(x), \deg g(x)\}$ *if* $f(x)+g(x) \neq O(x)$

(*ii*) $\deg(f(x).g(x)) \le \deg f(x) + \deg g(x)$ *if* $f(x)\,g(x) \neq O(x)$ *where* $O(x)$ *is the zero polynomial.* (*S. V. U. 01, O. U. 01*)

**Proof.** Let $f(x) = a_0 + a_1x + \ldots + a_mx^m$, $g(x) = b_0 + b_1x + \ldots + b_nx^n$

so that deg $f(x) = m$, deg $g(x) = n$.

Then $a_m \neq 0$ and $a_i = 0 \ \forall\ i > m$; $b_n \neq 0$ and $b_j = 0 \ \forall\ j > n$.

(*i*) From the definition, $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$

$$= c_0 + c_1x + c_2x^2 + \ldots$$

If $r = \max\{m, n\}$ then $c_r \neq 0$ and $c_i = 0 \ \forall\ i > r$.

$\therefore$ deg $(f(x) + g(x)) \le r$ *i.e.* deg $(f(x) + g(x)) \le \max\{m, n\}$

(*ii*) From the definition, $f(x)\,g(x) = a_0b_0 + (a_0b_1 + a_1b_0)\,x + \ldots$

$= d_0 + d_1x + d_2x^2 + \ldots$ where $d_s = \sum_{i+j=s} a_i\,b_j$

Let $s > m+n$. Then $i + j = s \Rightarrow i > m$ or $j > n$. But $i > m \Rightarrow a_i = 0$ and $j > n \Rightarrow b_j = 0$.

$\therefore$ $a_i\,b_j = 0$ for $i > m$ or $j > n \Rightarrow d_s = 0 \ \forall\ s > m+n$

Hence deg $(f(x)\,g(x)) \le m+n = \deg f(x) + \deg g(x)$.

**Corollary.** *If $f(x), g(x)$ are two non-zero polynomials of $F[x]$ where $F$ is a field then* $\deg(f(x).g(x)) = \deg f(x) + \deg g(x)$.

**Proof.** Let deg $f(x) = m$, deg $g(x) = n$ so that $a_m \neq 0, b_n \neq 0 \in F$.

$\therefore$ $a_m\,b_n \neq 0$ ( $\because$ the field $F$ has no zero divisors)

But $d_{m+n} = \sum_{i+j=m+n} a_i\,b_j = a_0b_{m+n} + a_1b_{m+n-1} + \ldots$

$$+ \ldots + a_m\,b_n + a_{m+1}b_{n-1} + \ldots + a_{m+n}b_0 = a_mb_n \neq 0.$$

$\therefore$ deg $(f(x).g(x)) \ge m+n$.

But from case (*ii*) of the above theorem, deg $(f(x).g(x)) \le m+n$.

Hence deg $(f(x).g(x)) = m+n = \deg f(x) + \deg g(x)$.

**Note. 1.** If the ring $R$ has no zero divisors or $R$ is an integral domain and $f(x), g(x) \in R[x]$ then deg $(f(x)\,g(x)) = \deg f(x) + \deg g(x)$.

**2.** If $R$ is an integral domain or field and $f(x), g(x) \in R[x]$

then $\deg f(x) \le \deg (f(x)\, g(x))$ since $\deg g(x) \ge 0$ as $g(x)$ is a non-zero polynomial.

**3.** Let $f(x), g(x) \in R[x]$ where $R$ is a ring. Let $\deg f(x) = m$, $\deg g(x) = n$. Then $a_m \neq 0$ and $a_i = 0 \ \forall \ i > m$; $b_n \neq 0$ and $b_j = 0 \ \forall \ j > n$.

If $m > n$ then leading coefficient in $f(x) + g(x) = a_m$.

If $m = n$ then leading coefficient in $f(x) + g(x) = a_m + b_n$.

If $m < n$ then leading coefficient in $f(x) + g(x) = b_n$.

Further, leading coefficient in $f(x)\, g(x) = a_m\, b_n$ where $a_m\, b_n \neq 0$.

**e.g.** Let $f(x) = 2 + 3x + 5x^2$ and $g(x) = 3 - 5x + x^3$ be two polynomials in $Z[x]$.

$f(x) = a_0 + a_1 x + a_2 x^2$ so that $a_0 = 2, a_1 = 3, a_2 = 5$ so that the largest integer $i$ having $a_i \neq 0$ is $2 \Rightarrow \deg f(x) = 2$.

$g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3$ so that $b_0 = 3, b_1 = -5, b_2 = 0$ and $b_3 = 1$ so that the largest integer $j$ having $b_j \neq 0$ is $3 \Rightarrow \deg g(x) = 3$.

We have $f(x) + g(x) = 5 - 2x + 5x^2 + x^3 = c_0 + c_1 x + c_2 x^2 + \ldots$ so that the largest integer $i$ having $c_i \neq 0$ is 3.

$\therefore \ \deg (f(x) + g(x)) = 3 = \max \{2, 3\}$.

We have $f(x)\, g(x) = 6 - x - 23x^3 + 3x^4 + 5x^5 = d_0 + d_1 x + d_2 x^2 + \ldots$ so that the largest integer $i$ having $d_i \neq 0$ is $5 \Rightarrow \deg (f(x) \,.\, g(x)) = 5 = \deg f(x) + \deg g(x)$.

## SOLVED PROBLEMS

**Ex. 1.** *Find the sum and product of* $f(x) = 5 + 4x + 2x^2 + 2x^3$ *and* $g(x) = 1 + 4x + 5x^2 + 3x^3$ *over the ring* $Z_6$. *Also find* $\deg (f(x) + g(x))$ *and* $\deg (f(x)\, g(x))$.

**Sol.** $Z_6 = \{0, 1, 2, 3, 4, 5\}$, ring of integers modulo 6.

We know that $a + b \equiv r_1 (\mathrm{mod}\, 6)$ and $a \,.\, b \equiv r_2 (\mathrm{mod}\, 6)$ for every $a, b \in Z_6$.

$$f(x) + g(x) = (5+1) + (4+4)\, x + (2+5)\, x^2 + (2+3)\, x^3 = 0 + 2x + 1x^2 + 5x^3$$

$$f(x) g(x) = (5 \,.\, 1) + (5 \,.\, 4 + 4 \,.\, 1)\, x + (5 \,.\, 5 + 4 \,.\, 4 + 2 \,.\, 1)\, x^2 + (5 \,.\, 3 + 4 \,.\, 5 + 2 \,.\, 4)\, x^3$$
$$+ (4 \,.\, 3 + 2 \,.\, 5 + 2 \,.\, 4)\, x^4 + (2 \,.\, 5 + 2 \,.\, 3)\, x^5 + (2 \,.\, 3)\, x^6$$
$$= 5 + 0\, x + 1\, x^2 + 1\, x^3 + 0\, x^4 + 4\, x^5 + 0\, x^6 .$$

We have $\deg f(x) = 3, \ \deg g(x) = 3$. $\qquad \deg (f(x) + g(x)) = 3 = \max \{3, 3\}$.

$\deg(f(x)g(x)) = 5 < \deg f(x) + \deg g(x)$ (Here $a_m b_n = 2.3 = 6 = 0 \pmod 6$)

**Ex. 2.** *Find the sum and product of* $f(x) = 2 + 3x + 4x^2 + 2x^3$ *and* $g(x) = 4 + 2x + 3x^4$ *given that* $f(x), g(x) \in Z_5[x]$. *Also find* $\deg(f(x) + g(x))$ *and* $\deg(f(x)\,g(x))$. ***(S. V. U 04)***

**Sol.** $Z_5 = \{0, 1, 2, 3, 4\}$ and $a + b = r_1 (\text{mod } 5),\ a \,.\, b \equiv r_2 \pmod 5$ for every $a, b \in Z_5$.

$f(x) + g(x) = (2+4) + (3+2)x + (4+0)x^2 + (2+0)x^3 + (0+3)x^4 = 1 + 0x + 4x^2 + 2x^3 + 3x^4$.

$f(x) \,.\, g(x) = (2.4) + (2.2 + 3.4)x + (2.0 + 3.2 + 4.4)x^2 + (2.0 + 3.0 + 4.2 + 2.4)x^3$

$+ (2.3 + 3.0 + 4.0 + 2.2)x^4 + (2.0 + 3.3 + 4.0 + 2.0)x^5 + (2.0 + 3.0 + 4.3 + 2.0)x^6$

$+ (2.0 + 3.0 + 4.0 + 2.3)x^7 = 3 + 1x + 2x^2 + 1x^3 + 0x^4 + 4x^5 + 2x^6 + 1x^7$.

$\deg f(x) = 3,\ \deg g(x) = 4$. $\deg(f(x) + g(x)) = 4 = \max\{3, 4\}$.

$\deg(f(x)\,g(x)) = 7 = 3 + 4 = \deg f(x) + \deg g(x)$. It may be noted that $Z_5$ is a field.

**4.4.** We now study the ring structure of polynomials with respect to addition and multiplication of polynomials.

**Theorem. 1.** ***If R is a ring then the set R[x] of all polynomials in the indeterminate x, is a ring with respect to addition and multiplication of polynomials.***

**Proof.** Let $f(x) = a_0 + a_1 x + \ldots + \ldots = \sum_{i=0}^{\infty} a_i x^i$, $g(x) = b_0 + b_1 x + \ldots = \sum_{j=0}^{\infty} b_j x^j$ and $h(x) = c_0 + c_1 x + \ldots = \sum_{k=0}^{\infty} c_k x^k$ be three polynomials in $R[x]$.

From the definitions of addition and multiplication of two polynomials, clearly, $f(x) + g(x)$ and $f(x) \,.\, g(x)$ are also polynomials in $R[x]$.

$\therefore$ addition and multiplication of two polynomials are binary operations in $R[x]$.

(1) $f(x) + g(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b_j x^j = \sum_{l=0}^{\infty} (a_l + b_l)\, x^l = \sum_{l=0}^{\infty} (b_l + a_l)\, x^l$

$= \sum_{j=0}^{\infty} b_j x^j + \sum_{i=0}^{\infty} a_i x^i = g(x) + f(x)$ ($a_l + b_l = b_l + a_l$ is true $\forall\ a_l, b_l \in R$).

$\therefore$ addition is commutative.

(2) $(f(x) + g(x)) + h(x) = \sum_{i=0}^{\infty} (a_i + b_i)\, x^i + \sum_{k=0}^{\infty} c_k x^k$

$= \sum_{l=0}^{\infty} ((a_l + b_l) + c_l)\, x^l = \sum_{l=0}^{\infty} (a_l + (b_l + c_l)\, x^l$

$$= \sum_{i=0}^{\infty} a_i\, x^i + \sum_{j=0}^{\infty} (b_j + c_j)\, x^j = f(x) + (g(x) + h(x))$$

$((a_l + b_l) + c_l = a_l + (b_l + c_l)$ is true $\forall\ a_l, b_l, c_l \in R)$ $\quad \therefore$ addition is associative.

(3) Zero polynomial $\mathrm{O}(x) = 0 + 0x + \ldots = \sum_{m=0}^{\infty} 0x^m$ exists in $R[x]$

such that $f(x) + \mathrm{O}(x) = \sum_{i=0}^{\infty} (a_i + 0)\, x^i = \sum_{i=0}^{\infty} a_i\, x^i = f(x)\ \forall\ f(x) \in R[x]$

$\therefore$ $\mathrm{O}(x)$ is the additive identity.

(4) If $f(x) = \sum_{i=0}^{\infty} a_i\, x^i$, $a_i \in R$ for $i = 0, 1, \ldots$ we have $-a_i \in R$ for $i = 0, 1, \ldots$

such that $a_i + (-a_i) = 0$, the zero element in $R$.

So, there exists $\phi(x) = \sum_{i=0}^{\infty} (-a_i)\, x^i \in R[x]$ such that

$f(x) + \phi(x) = \sum_{i=0}^{\infty} (a_i + (-a_i))\, x^i = \sum_{i=0}^{\infty} 0\, x^i = \mathrm{O}(x)$. $\quad \therefore$ every $f(x)$ has additive inverse.

(5) $(f(x) \,.\, g(x))\, h(x) = \left( \sum_{n=0}^{\infty} \left( \sum_{i+j=n} a_i b_j \right) x^n \right) \left( \sum_{k=0}^{\infty} c_k\, x^k \right)$

$$= \sum_{p=0}^{\infty} \left\{ \sum_{n+k=p} \left( \sum_{i+j=n} a_i b_j \right) c_k \right\} x^p = \sum_{p=0}^{\infty} \left( \sum_{i+j+k=p} (a_i b_j) c_k \right) x^p$$

$$f(x) \,.\, (g(x)\, h(x)) = \left( \sum_{i=0}^{\infty} a_i x^i \right) \left\{ \sum_{m=0}^{\infty} \left( \sum_{j+k=m} b_j c_k \right) x^m \right\}$$

$$= \sum_{q=0}^{\infty} \left\{ \sum_{i+m=q} a_i \left( \sum_{j+k=m} b_j c_k \right) \right\} x^q = \sum_{q=0}^{\infty} \left( \sum_{i+j+k=q} a_i (b_j c_k) \right) x^q$$

But $(a_i b_j)\, c_k = a_i (b_j c_k)$ is true $\forall\ a_i, b_j, c_k \in R$.

$\therefore$ $(f(x) \,.\, g(x))\, h(x) = f(x)\, (g(x) h(x)) \Rightarrow$ multiplication is associative.

(6) $f(x) \,.\, (g(x) + h(x)) = \sum_{i=0}^{\infty} a_i x^i \left( \sum_{j=0}^{\infty} (b_j + c_j) x^j \right)$

$$= \sum_{n=0}^{\infty} \left( \sum_{i+j=n} a_i (b_j + c_j) \right) x^n = \sum_{n=0}^{\infty} \left( \sum_{i+j=n} (a_i b_j + a_i c_j) \right) x^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i b_j\right)x^n + \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i c_j\right)x^n = f(x)\,.\,g(x) + f(x)\,.\,h(x)$$

Similarly, we can prove that $(g(x)+h(x))f(x) = g(x)f(x)+h(x)f(x)$

$\therefore$ Distributive laws are true.

From (1), (2), (3), (4), (5) and (6); $R[x]$ is a ring.

**Note.1.** $O(x) = 0+0x+\ldots$ is the zero element of ring $R[x]$.

**2.** Additive inverse of $f(x) = a_0 + a_1x + \ldots = \sum_{i=0}^{\infty} a_i x^i$ is $-f(x) = -a_0 - a_1x - \ldots = \sum_{i=0}^{\infty} -a_i x^i$ .

**Theorem 2.** ***The set $F(x)$ of all polynomials in an indeterminate x with coefficients in a field F is an integral domain with respect to addition and multiplication of polynomials.*** **(*O. U. 05*)**

**Proof.** If $F$ is a field then $F$ is a ring and hence from the previous theorem $F(x)$ is a ring. Now we prove that (1) $F(x)$ is commutative,

(2) $F(x)$ has unity element and (3) $F(x)$ has no zero divisors.

(1) Let $f(x) = a_0 + a_1x + \ldots = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = b_0 + b_1x + \ldots = \sum_{j=0}^{\infty} b_j x^j$

be two polynomials in $F(x)$.

From the definition : $f(x)\,g(x) = \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i b_j\right)x^n = \sum_{n=0}^{\infty}\left(\sum_{i+j=n} b_j a_i\right)x^n = g(x)f(x)$

$(\because a_i\text{'s}, b_j\text{'s} \in F)$

(2) We have $I(x) = 1+0x+0x^2+\ldots = \sum_{j=0}^{\infty} b_j x^j$ where $b_0 = 1$, the unity element in $F$ and $b_j = 0 \;\forall\; j \geq 1$.

$$f(x)\,.\,I(x) = \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i b_j\right)x^n = \sum_{n=0}^{\infty}(a_n\,.1)\,x^n = \sum_{n=0}^{\infty} a_n\,x^n = f(x)$$

$$\left(\because \sum_{i+j=n} a_i b_j = a_0b_n + a_1b_{n-1} + \ldots + a_nb_0 = 0+0+\ldots+0+a_n\,.1\right)$$

$\therefore f(x)\,.\,I(x) = I(x)\,.\,f(x) = f(x) \;\forall\; f(x) \in F[x]$.

$\therefore\; I(x) = 1+0x+0x^2+\ldots = 1$ is the unity element in $F(x)$

(3) Let $f(x) = a_0 + a_1 x + ... + a_m x^m \neq O(x)$ and $g(x) = b_0 + b_1 x + ... + b_n x^n \neq O(x)$

be two polynomials in $F(x)$

Let leading coefficient in $f(x) = a_m$ and leading coefficient in $g(x) = b_n$.

Then $a_m \neq 0, b_n \neq 0$. $a_m, b_n \in F$ and $F$ has no zero divisors.

$\Rightarrow a_m, b_n \neq 0 \Rightarrow$ leading coefficient in $f(x)\, g(x) = a_m\, b_n \neq 0$.

$\therefore$ there exists atleast one coefficient in $f(x)\, g(x)$ which is not zero element of $F$ and hence $f(x)\, g(x) \neq O(x)$.

$\therefore$ $F[x]$ has no zero divisors.

From the truth of the properties (1), (2) and (3) the ring $F[x]$ is an integral domain.

**Theorem. 3.** ***The set $D[x]$ of all polynomials with coefficients in an integral domain $D$ is an integral domain under addition and multiplication*** **(*S. V. U. 05*)**

**Proof.** (Write the proof of Theorems (1) and (2))

**Note.** If $R$ is commutative ring then $R[x]$ is also commutative.

If $R$ is a ring with unity element '1' then $R[x]$ is also a ring with unity element $I(x) = 1 + 0x + 0x^2 + ...$

If $R$ is a ring without zero divisors then $R[x]$ is also a ring without zero divisors.

**e.g.1.** If $Z$ is the ring integers then $Z[x]$ is an integral domain, because $Z$ is integral domain.

**e.g.2.** $Z_6 = \{0,1,2,3,4,5\}$ is a ring with zero divisors $\Rightarrow$ $Z_6[x]$ is a commutative ring with unity element.

**e.g. 3**. $Z_5 = \{0,1,2,3,4\}$ is a field $\Rightarrow$ $Z_5[x]$ is an integral domain.

**Imp. Note.** If $F$ is a field then $F[x]$ is only integral domain and not a field.

Let $I(x) = 1$ be the unity element in $F[x]$. Let $f(x) = 1 + x^2 \in F[x]$. Clearly $f(x) \neq O(x)$.

Let $g(x) \in F[x]$ so that $f(x) \,.\, g(x) = I(x)$.

$\therefore$ $\deg(f(x) \,.\, g(x)) = \deg I(x) \Rightarrow \deg f(x) + \deg g(x) = 0$

($\because$ $f(x), g(x) \in F[x]$ which is an integral domain)

$\Rightarrow 2 + \deg g(x) = 0$. This is impossible as $\deg g(x) \geq 0$.

$\therefore$ there is no polynomial $g(x) \in F[x]$ such that $f(x) \,.\, g(x) = I(x)$ and hence $F[x]$ is not a field.

**Note.** For non-zero constant polynomials in $F[x]$, that is, for non-zero elements in $F$ there exist multiplicative inverses. Therefore, **the non-zero constant polynomials in $F[x]$ are units in $F[x]$. The multiplicative inverse of $I(x)=1$ is itself.**

**Theorem. 4.** *If $F[x]$ is the set of all polynomials over the field $F$ then the set of all polynomials in $F[x]$ with constant term $0 \in F$ form an ideal of $F[x]$.*

**Proof.** Let $U[x]$ be the set of polynomials in $F[x]$ with constant term $= 0 \in F$.

Then $U[x] = \{a_0 + a_1x + ... + a_m\ x^m \in F[x] : a_0 = 0\}$.

Let $f(x) = a_0 + a_1x + ... + a_m\ x^m \in F[x]$. Then $f_1(x) = a_1x + ... + a_m\ x^m \in U[x]$.

$\therefore\ U[x] \neq \phi$ and $U[x] \subseteq F[x]$.

Let $f_1(x) = 0 + a_1x + ... + a_m\ x^m$, $g_1(x) = 0 + b_1x + ... + b_n\ x^n \in U[x]$.

$f_1(x) - g_1(x) = (0 + (-0) + (a_1 + (-b_1))x + ... + (a_r + (-b_r))\ x^r$ where $r = \max\{m, n\}$

$= 0 + c_1x + ... + c_rx^r \in U[x]$.

For $f(x) \in F[x]$ and $g_1(x) \in U[x]$ we have

$f(x)g_1(x) = (a_0 . 0) + (a_1 . 0 + a_0b_1)x + (a_2.0 + a_1b_1 + a_0b_2)\ x^2 + ... = d_1x + d_2x^2 + ... \in U[x]$

Also $g_1(x)f(x) = (0 . a_0) + (0 . a_1 + b_1a_0)\ x + ..... \in U[x]$

$\therefore\ U[x]$ is an ideal of $F[x]$.

**Note.** Clearly $U[x]$ is the principal ideal generated by $x \in F[x]$ and hence $U[x] = \langle x \rangle = \{x\ f(x) \mid f(x) \in F[x]\}$.

## SOLVED PROBLEMS

**Ex. 3.** *If R is a ring and $R'$ is the set of all constant polynomials in $R[x]$ prove that $R'$ is isomorphic to R.*

**Sol.** We know that $R' = \{a + 0x + 0x^2 + ... : a \in R\}$.

Define $\phi : R \to R'$ such that $\phi(a) = a + 0x + 0x^2 + ...\ \forall\ a \in R$.

(1) $a, b \in R$ and $\phi(a) = \phi(b) \Rightarrow a + 0x + 0x^2 + ... = b + 0x + 0x^2 + ... \Rightarrow a = b$

$\therefore\ \phi$ is one-one. (corresponding coefficients are equal)

(2) $\phi(R) = \{\phi(a) \mid a \in R\} = \{a + 0x + 0x^2 + ... \mid a \in R\} = R'$ $\therefore\ \phi$ is onto.

(3) Let $a, b \in R$.

$\phi(a) + \phi(b) = (a + 0x + 0x^2 + ...) + (b + 0x + 0x^2 + ...) = (a + b) + 0x + 0x^2 + ... = \phi(a + b)$.

$\phi(a)\ \phi(b) = (a + 0x + 0x^2 + ...) . (b + 0x + 0x^2 + ...) = ab + 0x + 0x^2 + ... = \phi(a)\ \phi(b)$.

$\therefore\ \phi$ is a homomorphism. From (1), (2) and (3) : $\phi : R \to R'$ is isomorphism.

**Ex. 4.** *If D is an integral domain then every unit in $D[x]$ is a unit in D.*

**Sol.** Let $1 \in D$ be the unity element and $I(x) = 1 + 0x + 0x^2 + ...$ be the unity element in $D[x]$. Let $f(x)$ be a unit in $D[x]$.

By the definition of unit, there exists $g(x) \in D[x]$ such that $f(x) . g(x) = I(x)$.

$\therefore$ deg $(f(x) . g(x))$ = deg $I(x) = 0$ ( $\because$ degree of constant polynomial = 0 )

$\Rightarrow$ deg $f(x)$ + deg $g(x) = 0$ ($\because$ $D[x]$ is integral domain)

$\Rightarrow$ deg $f(x) = 0$, deg $g(x) = 0$ ($\because$ deg $f(x)$, $g(x) \geq 0$)

$\Rightarrow f(x), g(x)$ are constant polynomials $\Rightarrow f(x) = a + 0x + 0x^2 + \ldots ; g(x) = b + 0x + 0x^2 + \ldots$

$\therefore$ $f(x)\ g(x) = ab + 0x + 0x^2 + \ldots$. Hence $f(x) . g(x) = I(x) \Rightarrow ab = 1 \Rightarrow a \in D$ is a unit.

**Ex. 5.** *Find the units in* $Z_7[x]$.

**Sol.** Since $Z_7 = \{0,1,2,3,4,5,6\}$ is a field $Z_7[x]$ is an integral domain.

$\therefore$ the units in $Z_7[x]$ are the non-zero constant polynomials.

$\therefore$ units in $Z_7[x]$ are $1 + 0x + \ldots, 2 + 0x + \ldots, 3 + 0x + \ldots, 4 + 0x + \ldots, 5 + 0x + \ldots, 6 + 0x + \ldots$.

**Ex. 6.** *Give an example of non-zero and non-constant polynomial* $f(x)$ *so that* $f(x) + f(x) = \mathrm{O}(x)$, *the zero polynomial.*

**Sol.** Consider the ring $Z_2[x]$ of polynomials over the ring $Z_2 = \{0,1\}$. Take $f(x) = 1 + x$.

$f(x) + f(x) = (1 + x) + (1 + x) = (1 + 1) + (1 + 1)x = 0 + 0x = \mathrm{O}(x)$.

## EXERCISE 12 ( *a* )

**1.** If $p(x) = 1 + x - x^2$ and $q(x) = 2 + x^2 + x^3 \in Z[x]$ find $p(x) + q(x)$ and $p(x)\ q(x)$.

**2.** If $f(x) = 2 + 3x + 5x^2$ and $g(x) = 3 + 5x + 2x^3 \in Z_6[x]$ find $f(x) + g(x), f(x) . g(x)$. Also find their degrees.

**3.** If $f(x) = 3 + 4x^2$ and $g(x) = 2 + x^3$ are in $Z_7[x]$ find $f(x) + g(x), f(x)\ g(x)$ and their degrees.

**4.** If $f(x) = 1 + 2x$ and $g(x) = 5 + 4x + 3x^2$ are polynomials in $Z_6[x]$ prove that deg $(f(x)\ g(x))$ = deg $f(x)$ + deg $g(x)$.

**5.** Proove left distributive law in $R[x]$ where $R$ is a ring.

**6.** Find the units in $Z[x]$.

**7.** If $D$ is an integral domain describe the units in $D[x]$.

**8.** If $f(x), g(x)$ are non-zero polynomials in $R[x]$ where $R$ is an integral domain then prove that $f(x)\ g(x)$ is also non-zero polynomial.

**9.** If $F$ is a field then prove that the set of all polynomials with constant term zero is an ideal generated by $x \in F[x]$.

**10.** If $f(x)=7+9x+5x^2+11x^3-2x^4$ and $g(x)=3-2x+7x^2+8x^3$ are polynomials in $Z_7[x]$ prove that $(i)$ $\deg\{f(x)+g(x)\}=4$ and $(ii)$ $\deg(f(x)\,g(x))=7$ **(S. V. U. 05)**

**11.** If $f(x)=2+3x+5x^2-4x^3$ and $g(x)=3+2x-4x^3+5x^4$ are polynomials over $Z[x]$ find $f(x)+g(x)$, $f(x).g(x)$, $\deg(f(x)+g(x))$ and $\deg(f(x).g(x))$ **(O.U. 03)**

**ANSWERS**

**1.** $3+x+x^3, 2+2x-x^2+2x^3-x^5$ **2.** $5+2x+5x^2+2x^3, x+5x^3+4x^5; 3, 5$

**3.** $5+4x^2+x^3, 6+x^2+3x^3+4x^5$; 3,5 **6.** $\pm 1$ **11.** $5+5x+5x^2-8x^3+5x^4$;

$6+13x+21x^2-10x^3-10x^4-5x^5+41x^6-20x^7$ and 4, 7.

## 12. 5. THE EVALUATION HOMOMORPHISMS

To study the problem of solving a polynomial equation we use the concept of homomorphism. In what follows, we study an important homomorphism of $F[x]$ into $E$ where $E$ is field and $F$ is a subfield of $E$.

**Theorem.** ***Let F be a subfield of the field E and F [x] be the set of all polynomials in an indeterminate x, over the field F. If $\alpha \in E$ then the mapping $\phi_\alpha : F[x] \to E$ defined by $\phi_\alpha(a_0+a_1x+...+a_nx^n)=a_0+a_1\alpha+...+a_n\alpha^n \;\forall\, a_0+a_1x+...+a_nx^n \in F[x]$ is a homomorphism.***

**Proof.** Let $f(x), g(x) \in F[x]$ and $f(x)=a_0+a_1x+...+a_mx^m$, $g(x)=b_0+b_1x+...+b_nx^n$.

Clearly, $\phi_\alpha$ mapping is well defined.

(1) $f(x)+g(x)=c_0+c_1x+...+c_px^p$ where $c_0=a_0+b_0, c_1=a_1+b_1, ..., c_p=a_p+b_p$

and $p=\max\{m,n\}$.

$$\phi_\alpha(f(x)+g(x))=\phi_\alpha(c_0+c_1x+...+c_px^p)=c_0+c_1\alpha+...+c_p\alpha^p$$

$$=(a_0+b_0)+(a_1+b_1)\alpha+...+(a_p+b_p)\alpha^p=(a_0+a_1\alpha+...+a_m\alpha^m)+(b_0+b_1\alpha+...+b_n\alpha^n)$$

$=\phi_\alpha(f(x))+\phi_\alpha(g(x))$. ($\because$ $a_i$'s, $b_j$'s and $\alpha$ are elements of field)

(2) $f(x).g(x)=d_0+d_1x+...+d_qx^q$ where

$d_k=\sum_{i+j=k} a_i\,b_j$ *i.e.*, $d_0=a_0b_0$, $d_1=a_0b_1+a_1b_0$, ...

$$\phi_\alpha(f(x)\,g(x))=\phi_\alpha(d_0+d_1x+...+d_qx^q)=d_0+d_1\alpha+...+d_q\alpha^q$$

But $\phi_\alpha(f(x)).\phi_\alpha(g(x))=(a_0+a_1\alpha+...+a_m\alpha^m)(b_0+b_1\alpha+...+b_n\alpha^n)$

$$=a_0b_0+(a_0b_1+a_1b_0)\alpha+...+\left(\sum_{i+j=q} a_ib_j\right)\alpha^q=d_0+d_1\alpha+...+d_q\alpha^q$$

$\therefore\ \phi_\alpha(f(x).g(x)) = \phi_\alpha(f(x).\phi_\alpha g(x)$.

Hence from (1) and (2) : $\phi_\alpha : F[x] \to E$ is a homomorphism.

**Definition.** *Let F be a subfield of the field E and $F[x]$, the set of all polynomials over the field F. For $\alpha \in E$, the homomorphism*

$\phi_\alpha : F[x] \to E$ *is called the Evaluation at* $\alpha$.

**Notation.** If $\phi_\alpha : F[x] \to E$ is an evaluation homomorphism at $\alpha \in E$ and $f(x) = a_0 + a_1x + ... + a_nx^n \in F[x]$ then $\phi_\alpha(f(x)) = a_0 + a_1\alpha + ... + a_n\alpha^n$ is denoted by $f(\alpha)$.

**e.g. 1.** Let $F = E = Z_7$ and $\phi_\alpha : Z_7[x] \to Z_7$ be the evaluation homomorphism at $\alpha \in Z_7$.

$\phi_2(x^2+3) = \phi_2(3+0x+1x^2) = 3+0\,(2)+1\,(2^2) = 3+0+4 = 7 = 0$ $(\because 7 \equiv 0 (\text{mod } 7))$

$\phi_0(2+3x-x^2+2x^3) = 2+3\,(0)-0^2+2\,(0^3) = 2+0-0+0 = 2$

**e. g. 2.** Let $f(x) = x \in F[x]$ and $\alpha \in E$.

$\phi_\alpha(f(x)) = \phi_\alpha(x) = \phi_\alpha(0+1x) = 0+1\alpha = \alpha$. $\quad\therefore\ \phi_\alpha(x) = \alpha$.

**Corollary.** ***Let F be a field, $\alpha \in F$ and $F[x]$ be the set of all polynomials over the field F. If $F'$ is the set of all constant polynomials in $F[x]$ then $\phi_\alpha : F' \to F$ is an isomorphism.***

**Proof.** We have $F' = \{ a + 0x + 0x^2 + ... \mid a \in F \}$.

Let $a, b \in F$ and $f(x) = a + 0x + ..., g(x) = b + 0x + ...$ be two constant polynomials.

By the definition of $\phi_\alpha$; $\phi_\alpha(f(x)) = a + 0\alpha + ... = a$ and $\phi_\alpha(g(x)) = b + 0\alpha + ... = b$

$\phi_\alpha(f(x)) = \phi_\alpha(g(x)) \Rightarrow a = b$ $\quad\therefore\ \phi_\alpha$ is one - one.

$\forall\ a \in F$ there exists $f(x) = a + 0x + ... \in F[x]$ such that $\phi_\alpha(f(x)) = a$. $\therefore\ \phi_\alpha$ is onto.

$\therefore\ \phi_\alpha : F' \to F$ is an isomorphism.

In fact $F' = F$ and hence $\phi_\alpha : F' \to F$ is identity mapping.

**Definition. (Zero of a Polynomial)** *Let F be a subfield of the field E and $\alpha \in E$.*

Let $\phi_\alpha : F[x] \to E$ be an evaluation homomorphism.

For $f(x) = a_0 + a_1x + ... + a_n\alpha^n \in F[x]$, if $f(\alpha) = \phi_\alpha(f(x)) = a_0 + a_1\alpha + ... + a_n\alpha^n = 0$ then $\alpha \in E$ is a zero of the polynomial $f(x)$ or $\alpha \in E$ is a solution of $f(x) = 0$ polynomial equation.

**Note.** In view of the above definition our elementary problem of all real solutions of polynomial equation $f(x) = 0$ is equivalent to finding all $\alpha \in R$ such that $\phi_\alpha(f(x)) = 0$ where $\phi_\alpha : [x] \to R$ is the evaluation homomorphism.

**e.g.1.** Let $Q \subset R$ and $Q[x]$ be the set of all polynomials over the field $Q$ of rational numbers. Let $f(x) = x^2 - 3x + 2$. Solving $f(x) = 0$ is equivalent to finding zeros of $f(x) = x^2 - 3x + 2$. That is, finding $\alpha \in R$ such that $\phi_\alpha(f(x)) = \phi_\alpha(x^2 - 3x + 2) = 0$.

We have $\phi_1(f(x)) = 1^2 - 3(1) + 2 = 0$, $\phi_2(f(x)) = 2^2 - 3(2) + 2 = 0$.

$\therefore$ Solutions of $f(x) = 0$ in $R = \{1, 2\}$.

**e.g. 2.** We have $R \subset C$, where $C$ is the set of all complex numbers.

Consider $f(x) = 1 + x^2 \in R[x]$.

For $\alpha \in R$, if $\phi_\alpha : R[x] \to R$ is an evaluation homomorphism,

we know that $\phi_\alpha(f(x)) = 1 + \alpha^2 \neq 0$ for any $\alpha \in R$.

Therefore $f(x) = 1 + x^2$ has no zeros in $R$.

For $\alpha \in C$, if $\phi_\alpha : R[x] \to C$ is an evaluation homomorphism,

then $\phi_\alpha(f(x)) = 1 + \alpha^2 = 0 \Rightarrow \alpha = \pm i$.

Therefore, $f(x) = 1 + x^2$ has two zeros $-i, +i$ in $C$.

**Note.** Even though $f(x) = 1 + x^2$ has no zero in $R$ we could find field $C$ containing $R$ such that $f(\alpha) = \phi_\alpha(f(x)) = 0$ for $\alpha \in C$.

## KERNEL OF EVALUATION HOMOMORPHISM

**Definition.** *Let $F$ be field and $F[x]$ be the set of all polynomials over $F$. Consider the field $E$ containing $F$. For $\alpha \in E$ we have an evaluation homomorphism $\phi_\alpha : F[x] \to E$ defined as $\phi_\alpha(f(x)) = f(\alpha)$. Kernel of the evaluation homomorphism $\phi_\alpha$ = Ker $\phi_\alpha = \{f(x) \in F[x] \mid \phi_\alpha(f(x)) = f(\alpha) = 0\}$ where '0' is the zero element in the field E.*

From the fundamental theorem of homomorphism we further know that $\phi_\alpha$ is an ideal of $F[x]$ and $F[x]/\text{Ker}\,\phi_\alpha \cong \phi_\alpha(F[x])$.

**e.g.** Consider the evaluation homomorphism $\phi_5 : Q[x] \to R$ for $5 \in R$, the set of all real numbers. The zero element in $R = 0$.

Consider $f(x) = 5 - x$, $g(x) = -5x + x^2$, $h(x) = 25 - 10x + x^2 \in Q[x]$.

We have $\phi_5(f(x)) = 5 - 5 = 0$; $\phi_5(g(x)) = -5(5) + 5^2 = 0$ and $\phi_5(h(x)) = 25 - 10(5) + 5^2 = 0$.

$\therefore$ $f(x) = 5 - x, g(x) = -5x + x^2$ and $h(x) = 25 - 10x + x^2$ are three elements in Ker $\phi_5$.

## SOLVED PROBLEMS

**Ex. 1.** *Let $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ the set of all integers modulo 7. For $5 \in Z_7$ if $\phi_5 : Z_7[x] \to Z_7$ is an evaluation homomorphism find $\phi_5\left[(3 + 4x^2)(2 + x^3)(1 + 3x^2 + x^7)\right]$.*

**Sol.** Let $f(x) = 3 + 4x^2 = 3 + 0x + 4x^2$, $g(x) = 2 + x^3 = 2 + 0x + 0x^2 + 1x^3$,

$h(x) = 1 + 0x + 3x^2 + 0x^3 + 0x^4 + 0x^5 + 0x^6 + 1x^7$.

By homomorphism property : $\phi_\alpha[f(x)\ g(x)\ h(x)] = \phi_\alpha(f(x))\ \phi_\alpha(g(x))\ \phi_\alpha(h(x))$.

$\phi_5(f(x)) = 3 + 0(5) + 4(5^2) = 3 + 5 + 4(4) = 3 + 5 + 2 = 3$

$\phi_5(g(x)) = 2 + 0(5) + 0(5^2) + 1(5^3) = 2 + 0 + 0 + 6 = 1$

$\phi_5(h(x)) = 1 + 0(5) + 3(5^2) + 0(5^3) + 0(5^4) + 0(5^5) + 0(5^6) + 1(5^7)$

$= 1 + 0 + 3(4) + 0 + 0 + 0 + 0 + 5 = 1 + 5 + 5 = 4$.

$\phi_5(f(x)\ g(x)\ h(x)) = (3)\ (1)\ (4) = 5$.

**Ex. 2.** *Find the zeros of* $f(x) = 1 + x^2 \in Z_5[x]$ *in* $Z_5$. **(*N. U. 97*)**

**Sol.** We have $Z_5 = \{0, 1, 2, 3, 4\}$.

We have $\phi_0(f(x)) = 1 + 0^2 = 1 \neq 0$, $\phi_1(f(x)) = 1 + 1^2 = 2 \neq 0$, $\phi_2(f(x)) = 1 + 2^2 = 5 = 0$,

$\phi_3(f(x)) = 1 + 3^2 = 10 = 0$, $\phi_4(f(x)) = 1 + 4^2 = 17 = 2 \neq 0$.

$\therefore$ Zeros of $f(x) = 1 + x^2$ in $Z_5 = \{\alpha \in Z_5 \mid \phi_\alpha(f(x)) = 0\} = \{2, 3\}$

We can also say that $f(x) = 1 + x^2$ is in Ker $\phi_2$ and Ker $\phi_3$.

**Ex. 3.** *Let* $Q[x]$ *be the set of all polynomials over the field Q, of rational numbers and R is the set of real numbers. For* $0 \in R$ *if* $\phi_0 : Q[x] \to R$ *is the evaluation homomorphism then prove that Q is isomorphic with* $Q[x] / Ker\ \phi_0$.

**Sol.** Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in Q[x]$. Then $\phi_0(f(x)) = a_0 \in Q$.

$\therefore$ every $f(x) \in Q[x]$ is mapped into a rational number $\in Q$ by $\phi_0$.

Thus $\phi_0(Q[x]) = Q$. Ker of $\phi_0 = \{f(x) \in Q[x] \mid \phi_0(f(x)) = 0\}$

= the set of all polynomials of $Q[x]$ with constant term $'0' = \langle x \rangle$.

By fundamental theorem, $Q \cong Q[x] / \text{Ker}\ \phi_0$.

## EXERCISE 12 ( *b* )

**1.** If $\phi_5 : Z_7[x] \to Z_7$ is an evaluation homomorphism find $\phi_5(2 + x^3), \phi_5(3 + 4x^2)$ and $\phi_5(2 + x^3)\ (3 + 4x^2)$.

**2.** Find all zeros in $Z_5$ of $2x + x^2 + 3x^3 + x^5 \in Z_5[x]$.

**3.** Prove that $1 + x^2 \in Q[x]$ is in the Kernel of $\phi_i : Q[x] \to C$.

**4.** Prove that $1 \in Z_5$ is a zero of $4 + 2x + 3x^3 + x^4 \in Z_5[x]$.

Also prove that $(-1 + x)\ (1 + 4x + 4x^2 + x^3) = 4 + 2x + 3x^3 + x^4$.

**5.** Find all the zeros of $x^2 + x - 6 \in Q[x]$ in $R$.

**6.** If $f(x), g(x), h(x) \in F[x]$ where $F$ is a field, $f(x) = g(x)\,h(x)$ and $\alpha \in E \supset F$ then prove that $f(\alpha) = 0 \Leftrightarrow g(\alpha) = 0$ or $h(\alpha) = 0$.

**7.** If $F[x]$ is the field of polynomials show that $\langle x \rangle = \{ x\, f(x) \mid f(x) \in F[x] \}$ is the Kernel of $\phi_0 : F[x] \to F$.

**ANSWERS**

**1.** 1, 5, 5 **2.** 0, 4 **5.** –3, 2

## 12. 6. FACTORISATION OF POLYNOMIALS OVER A FIELD

More important applications arise for polynomial rings of the form $F[x]$ where $F$ is a field. We now prove a division algorithm for polynomials in $F[x]$. This division algorithm is very similar to that of integers .

**THEOREM. 1. THE DIVISION ALGORITHM.**

***Let F be a field. Given two polynomials $f(x), g(x) \neq O(x)$ in $F[x]$ there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)\,g(x) + r(x)$ where $r(x) = O(x)$ or $\deg r(x) < \deg g(x)$.*** ***(K. U. 05, A. U. 07, S. V. U. 01, N. U. 07)***

**Proof.** Consider the set $S = \{ f(x) - h(x)\, g(x) \mid h(x) \in F[x] \}$.

For $O(x) \in F[x]$, $f(x) - O(x)\, g(x) = f(x) \in S \Rightarrow S \neq \phi$

Let $O(x) \in S$. Then by the definition of S, there exists $q(x) \in F[x]$ so that

$O(x) = f(x) - q(x)\, g(x) \Rightarrow f(x) = g(x)\, q(x) + O(x)$

$\Rightarrow f(x) = q(x)\, g(x) + r(x)$ where $r(x) = O(x)$. $\therefore$ the theorem is proved.

Let $O(x) \notin S$.

Then every polynomial in $S$ is a non-zero polynomial and hence non-negative degree.

Let $r(x) \in S$ be polynomial of least degree.

By definition of S, there exists $q(x) \in F[x]$ so that

$r(x) = f(x) - q(x)\, g(x) \Rightarrow f(x) = g(x)\, q(x) + r(x)$ ... (1)

Let $g(x) = a_0 + a_1 x + \ldots + a_n x^n,\ a_n \neq 0$ so that $\deg g(x) = n$.

Now we have to prove that $\deg r(x) < n$.

If possible, suppose that $\deg r(x) \geq n$.

Let $r(x) = c_0 + c_1 x + \ldots + c_m x^m,\ c_m \neq 0$ so that $m \geq n$ and $\deg r(x) = m$

Now $c_m a_n^{-1} x^{m-n} g(x) = c_m a_n^{-1} a_0 x^{m-n} + c_m a_n^{-1} a_1 x^{m-n+1} + \ldots + c_m a_n^{-1} a_{n-1} x^{m-1} + c_m x^m$

$\therefore r(x) - c_m a_n^{-1} x^{m-n} g(x) = (c_{m-1} x^{m-1} + \ldots + c_0) - (c_m a_n^{-1} a_{n-1} x^{m-1} + \ldots + c_m a_n^{-1} a_0 x^{m-n})$ ...(2)

$\therefore r(x) = c_m a_n^{-1} x^{m-n} g(x) + \alpha(x)$ where $\alpha(x) = (c_{m-1} - c_m a_n^{-1} a_{n-1}) x^{m-1} + \ldots + \ldots + c_0$

So, $\deg \alpha(x) \le m-1 \Rightarrow \deg \alpha(x) < \deg r(x)$

From (1) and (2) : $\alpha(x) = f(x) - g(x) \left\{ q(x) + c_m a_n^{-1} x^{m-n} \right\}$

$\Rightarrow \alpha(x) = f(x) - g(x)\, \beta(x)$ where $\beta(x) = q(x) + c_m a_n^{-1} x^{m-n} \in F[x]$.

$\Rightarrow \alpha(x) \in S$ ( From the definition of $S$ )

Now we have $\alpha(x), r(x) \in S$ and $\deg \alpha(x) < \deg r(x)$

This is a contradiction since $r(x)$ is the polynomial of least degree in $S$.

$\therefore$ our supposition is wrong. $\therefore \deg r(x) < n$ *i.e.*, $\deg r(x) < \deg g(x)$

Hence there exist $q(x), r(x) \in F[x]$

so that $f(x) = q(x) g(x) + r(x)$ where $r(x) = O(x)$ or $\deg r(x) < \deg g(x)$.

**Uniqueness of $q(x)$ and $r(x)$** :

If possible, suppose that $f(x) = q'(x) g(x) + r'(x)$ where

$r'(x) = O(x)$ or $\deg r'(x) < \deg g(x)$.

Then $q(x)\, g(x) + r(x) = q'(x) g(x) + r'(x) \Rightarrow (q(x) - q'(x)) g(x) = r'(x) - r(x)$.

If $q(x) - q'(x) \ne O(x)$ then $\deg (q(x) - q'(x)) g(x) = \deg (q(x) - q'(x)) + \deg g(x)$

$\Rightarrow \deg (r'(x) - r(x)) \ge \deg g(x)$.

This is a contradiction because $\deg r(x) < \deg g(x)$ and $\deg r'(x) < \deg g(x)$.

$\therefore q(x) - q'(x) = O(x)$ and $r'(x) - r(x) = O(x)$ which implies that $q'(x) = q(x)$

and $r'(x) = r(x)$. Hence $q(x), r(x) \in F[x]$ are unique.

**Note. 1.** The polynomials $q(x)$ and $r(x)$ of the above theorem are called the quotient and the remainder.

**2.** In the above theorem if $r(x) = O(x)$ then we say that $g(x)$ divides $f(x)$ or $g(x)$ is a factor of $f(x)$ in $F[x]$. We write $g(x) \mid f(x)$.

**Corollary (The Remainder Theorem.)** ***Let F be a field,*** $\alpha \in F$ ***and*** $f(x) \in F[x]$. ***Then*** $f(\alpha)$ ***is the remainder in the division of*** $f(x)$ ***by*** $(x - \alpha)$.

**Proof.** Let $\deg f(x) = n$ and take $g(x) = x - \alpha$. By the above theorem there exist $q(x), r(x)$ in $F[x]$ such that $f(x) = (x-\alpha)\,q(x) + r(x)$ where $r(x) = \mathrm{O}(x)$ or $\deg r(x) < \deg (x-\alpha)$.

But $\deg (x-\alpha) = 1$ and $\deg r(x) < \deg (x-\alpha) \Rightarrow \deg r(x) < 1 \Rightarrow r(x)$ is a constant polynomial $= r$ (say). $\therefore\ f(x) = (x-\alpha)\,q(x) + r$ where $r \in F$.

By evaluation homomorphism, $\phi_\alpha : F[x] \to F$. We have $f(\alpha) = r =$ the remainder.

Hence the remainder, obtained by dividing the polynomial $f(x)$ with $(x-\alpha)$ is $f(\alpha)$.

**Definition. (Divisibility or Factor of a Polynomial)**

*If $f(x), g(x) \in F[x]$ then we say that $g(x)$ divides $f(x)$ in $F[x]$ if there exists $q(x) \in F[x]$ such that $f(x) = g(x)q(x)$. We also say that $g(x)$ and $q(x)$ are factors of $f(x)$ in $F[x]$.*

**Notation.** If $g(x)$ divides $f(x)$ then we write $g(x) \mid f(x)$.

Otherwise we write $g(x) \nmid f(x)$

**Imp.** $g(x)$ **divides** $f(x)$ **or** $g(x)$ **is a factor of** $f(x)$

$\Leftrightarrow f(x) = g(x)\,q(x)$ **where** $q(x) \in F[x]$.

**Theorem. 2. (Factor Theorem).** ***An element $\alpha \in F$ where $F$ is a field, is a zero of $f(x) \in F[x]$ if and only if $(x-\alpha)$ is a factor of $f(x)$ in $F[x]$.*** ***(O. U. 12)***

**Proof.** Let $\alpha \in F$ be a zero of $f(x)$. Then $f(\alpha) = 0$.

Let $g(x) = x - \alpha$ so that $\deg g(x) = 1$.

By division algorithm, there exist $q(x), r(x) \in F[x]$ such that $f(x) = g(x)\,q(x) + r(x)$

*i.e.* $f(x) = (x-\alpha)\,q(x) + r(x)$ where $r(x) = \mathrm{O}(x)$ or $\deg r(x) < \deg (x-\alpha)$

Since $\deg (x-\alpha) = 1$, $\deg r(x) < \deg (x-\alpha) \Rightarrow \deg r(x) < 1$

$\Rightarrow r(x)$ is a constant polynomial $\Rightarrow r(x) = r \in F$.

Using evaluation homomorphism, $\phi_\alpha : F[x] \to F$; for $f(x) \in F[x]$

we have $\phi_\alpha(f(x)) = \phi_\alpha((x-\alpha)q(x) + r) \Rightarrow f(\alpha) = 0\ q(\alpha) + r \Rightarrow f(\alpha) = r \Rightarrow r = 0$.

$\therefore\ r(x) = \mathrm{O}(x)$ and hence $f(x) = (x-\alpha)q(x)$.

$\therefore\ (x-\alpha)$ is a factor of $f(x)$ in $F[x]$

**Conversely,** let $(x-\alpha)$ be a factor of $f(x)$ in $F[x]$.

$\therefore$ there exists $q(x) \in F[x]$ such that $f(x) = (x-\alpha)q(x)$.

By evaluation homomorphism $\phi_\alpha : F[x] \to F$ ;

$\phi_\alpha(f(x)) = \phi_\alpha((x-\alpha)q(x)) \Rightarrow f(\alpha) = \phi_\alpha(x-\alpha)\,.\,\phi_\alpha(q(x)) \Rightarrow f(\alpha) = 0\ q(\alpha) \Rightarrow f(\alpha) = 0$ .

$\therefore\ \alpha \in F$ is a zero of $f(x) \in F[x]$ .

**Note. $(x-\alpha)$ is a factor of $f(x) \Leftrightarrow f(x) = (x-\alpha)\,q(x)$ where $\deg q(x) = \deg f(x) - 1$.**

**Corollary.** ***If $f(x) \in F[x]$ is a non-zero polynomial of degree n then $f(x)$ can have atmost n zeros in F.***

**Proof.** We suppose that $f(x)$ has atleast one zero $\alpha_1 \in F$ .

By factor theorem, $f(x) = (x-\alpha_1)\,q_1(x)$ where $\deg q_1(x) = \deg f(x) - 1 = n-1$ .

$\alpha_2 \in F$ is a zero of $q_1(x) \Rightarrow q_1(x) = (x-\alpha_2)\,q_2(x)$

where $\deg q_2(x) = \deg q_1(x) - 1 = n-2$ .

$\therefore\ f(x) = (x-\alpha_1)\,(x-\alpha_2)\,q_2(x)$ where $\deg q_2(x) = n-2$ .

Continuing this process, we have $f(x) = (x-\alpha_1)\,(x-\alpha_2)\ldots(x-\alpha_r)\,q_r(x)$

where $\deg q_r(x) = n-r \geq 0$ and $q_r(x)$ has no zero in $F$.

If $\beta \in F$ and $\beta = \alpha_i, i = 1, 2, \ldots r$ then $f(\beta) = (\beta-\alpha_1)\,(\beta-\alpha_2)\ldots(\beta-\alpha_r)\,q_r(\beta) \neq 0$ as $F$ is a field having no zero divisors.

$\therefore\ \alpha_1, \alpha_2, \ldots, \alpha_r\ (r \geq n)$ are all the zeros of $f(x)$ in $F$.

**Working method for finding $q(x)$ and $r(x)$ in the Division algorithm $f(x) = g(x)\,q(x) + r(x)$.**

Using long division of the high school we can obtain quotient $q(x)$ and remainder $r(x)$ . The technique of synthetic division can be used to find factors or zeros of $f(x) \in F[x]$ .

## SOLVED PROBLEMS

**Ex. 1.** *If $f(x) = x^2 + x + 4 \in Z_{11}[x]$ find the remainder when $f(x)$ is divided by $(x-3)$ .*

**Sol.** When $f(x)$ is divided by $(x-\alpha)$ the remainder = $f(\alpha)$ .

Remainder $f(3) = 3^2 + 3 + 4 = 9 + 3 + 4 = 16 = 5$ . ($\because\ 16 \equiv 5 \pmod{11}$)

**Ex. 2.** *If $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ are polynomials in $Z_7[x]$ find $q(x)$ and $r(x)$ in $f(x) = g(x)\,q(x) + r(x)$ .*

**Sol.** $f(x) = x^6 + 3x^5 + 0x^4 + 0x^3 + 4x^2 - 3x + 2$ ; $g(x) = x^2 + 2x - 3$ .

$$
\begin{array}{l|l}
 & x^4+x^3+x^2+x-2 \\
\hline
x^2+2x-3 & x^6+3x^5+0x^4+0x^3+4x^2-3x+2 \\
 & x^6+2x^5-3x^4 \\
\hline
 & (3-2)x^5+(0+3)x^4+0x^3 \\
 & x^5+3x^4+0x^3 \\
 & x^5+2x^4-3x^3 \\
\hline
 & x^4+3x^3+4x^2 \\
 & x^4+2x^3-3x^2 \\
\hline
 & x^3+0x^2-3x \qquad (\because 4+3\equiv 0 \pmod 7) \\
 & x^3+2x^2-3x \\
\hline
 & -2x^2+0x+2 \\
 & -2x^2-4x+6 \\
\hline
 & 4x-4
\end{array}
$$

$\therefore\ q(x)=x^4+x^3+x^2+x-2\ ;\ r(x)=4x-4$ so that $\deg\, r(x)=1<\deg\, g(x)=2$.

**Ex. 3.** *Prove that the factors of* $1+x^2$ *in* $Z_2[x]$ *are* $1+x$ *and* $1+x$.

**Sol.** To prove that $p(x)$ and $q(x)$ are factors of $f(x)$ we have to show that $f(x)=p(x)\,q(x)$.

$$(1+x)\,(1+x)=(1.1)+(1.1+1.1)\,x+(1.0+1.1+0.1)\,x^2$$

$$=1+2x+1x^2=1+0x+x^2=1+x^2 \quad (\because\ 2\equiv 0 \pmod 2)$$

**Ex. 4.** *Find the factors of* $x^4+4$ *in* $Z_5[x]$.

**Sol.** Let $f(x)=x^4+4$ ; $Z_5=\{0,1,2,3,4\}$.

We observe that $f(1)=1+4=0$, $f(2)=4^4+4=0$, $f(3)=0$ and $f(4)=0$.

$\therefore\ x-1, x-2, x-3, x-4$ are factors of $f(x)$.

$\deg f(x)=4$ and $\deg\{(x-1)(x-2)(x-3)(x-4)\}$

$=\deg(x-1)+\deg(x-2)+\deg(x-3)+\deg(x-4)=4$ ($\because\ Z_5$ is field)

Leading coefficient in $f(x)=1$ and

leading coefficient in $(x-1)(x-2)(x-3)(x-4)=1$.

$\therefore\ x^4+4=(x-1)(x-2)(x-3)(x-4)$.

**Ex. 5.** *Solve the equation* $x^2+1=0$ *in the field* $Z_5$.

**Sol.** Let $f(x)=x^2+1 \in Z_5[x]$. Solving $f(x)=0$ in $Z_5$ is equivalent to finding zeros of $f(x)$ in $Z_5$.

We have $f(0)=1\neq 0, f(1)=2\neq 0, f(2)=2^2+1=5=0, f(3)=3^2+1=10=0$,

$f(4)=4^2+1=2\neq 0$. $\therefore 2,3 \in Z_5$ are the solutions of $x^2+1=0$ in $Z_5$.

## 12. 7. IRREDUCIBLE POLYNOMIALS

**Definition.** *A non constant polynomial* $p(x)$ *in* $F[x]$ *is said to be* ***irreducible over the field F*** *if whenever* $p(x)=f(x)\,g(x)$ *with* $f(x), g(x) \in F[x]$ *then one of* $f(x)$ *or* $g(x)$ *has zero degree. If* $p(x)$ *is irreducible over F then* $p(x)$ *is called an* ***irreducible polynomial in*** $F[x]$. *If* $p(x)$ *is not irreducible over F then we say that* $p(x)$ *is reducible over F.*

**Imp.** $p(x) \in F[x]$ is an irreducible polynomial $\Leftrightarrow p(x)=f(x)\,g(x)$

for $f(x), g(x) \in F[x]$, then one of $f(x)$ or $g(x)$ is a constant polynomial.

**Note.** A non constant polynomial $p(x) \in F[x]$ is an irreducible polynomial $\Leftrightarrow p(x)$ cannot be expressed as the product $f(x)\,g(x)$ with $f(x), g(x) \in F[x]$ so that both of lower degree than the degree of $f(x)$.

**Remark.** Irreducibility of a polynomial depends on the field.

That is, a polynomial $f(x)$ may be irreducible over the field *F*, but may not be irreducible over the field *E* containing *F*.

**e.g.1**. $f(x)=1+x^2$ is irreducible over the field of real numbers *R*. But $f(x)=1+x^2$ is not irreducible over the field of complex numbers *C*, as $f(x)=x^2+1=(x+i)(x-i)$ where $i^2=-1$ and $i \in C$.

$\therefore x+i, x-i$ are non-constant factors in $C[x]$ of $x^2+1 \in R[x]$.

**e.g.2.** $f(x)=x^2-2$ is irreducible over the field of rational numbers *Q*.

But $f(x)=x^2-2$ is not irreducible over the field of real numbers *R*,

as $f(x)=x^2-2=(x+\sqrt{2})(x-\sqrt{2})$ where $\sqrt{2} \in R$.

$\therefore x+\sqrt{2}, x-\sqrt{2}$ are non-constant factors of $x^2-2 \in Q[x]$ in $R[x]$.

**Note.** We know that every non-zero constant polynomial in $F[x]$ is a non-zero element of the field *F*. But every non-zero element in *F* is a unit having multiplicative inverse.

So, non-zero constant polynomials in $F[x]$ are units.

Hence $p(x)=f(x)\,g(x)$ is irreducible polynomial in $F[x] \Rightarrow f(x)$ or $g(x)$ is a unit in *F*.

$\Rightarrow p(x)=a_i\,g(x)$ where $a_i \neq 0 \in F$ is a unit.

**Theorem. 1.** *If* $f(x) \in F[x]$ *and* $\deg f(x) = 2$ *or* 3 *then* $f(x)$ *is reducible over* $F$ *if and only if* $f(x)$ *has a zero in* $F$. *(O. U. 12)*

**Proof.** Let $f(x)$ be reducible over $F$.

There exist $g(x), h(x) \in F[x]$ such that $f(x) = g(x)\,h(x)$ where the degree of $g(x)$ and $h(x)$ are both less than the degree of $f(x)$.

If $\deg f(x) = 2$ , then $\deg g(x) = 1$ , $\deg h(x) = 1$

If $\deg f(x) = 3$ , then $\deg g(x) = 2$ , $\deg h(x) = 1$ or $\deg g(x) = 1$ or $\deg h(x) = 2$ .

In either case, one of $g(x)$ or $h(x)$ is of degree 1.

Let $\deg h(x) = 1$ and $h(x) = x - \alpha$ .

$\therefore f(x) = g(x)\,(x - \alpha) \Rightarrow f(\alpha) = g(\alpha)0 = 0$ . $\therefore f(x)$ has a zero in $F$.

**Conversely,** let $f(x)$ has a zero in $F$.

Let $f(\alpha) = 0$ for $\alpha \in F$ .

$\therefore\ x - \alpha$ is a factor of $f(x)$ and hence $f(x) = (x - \alpha)\,g(x)$ so that $\deg g(x) = 1$ or 2.

$\therefore\ f(x)$ is reducible over $F$.

**Note.** We can test the irreducibility of $f(x) \in F[x]$ by finding zeros of $f(x)$ in $F$.

Consider $f(x) = x^3 + 2x + 3 \in Z_5[x]$. We have $Z_5 = \{0, 1, 2, 3, 4\}$.

For $\alpha \in Z_5$ if $f(\alpha) = 0$ then $\alpha$ is a zero of $f(x)$ and hence $(x - \alpha)$ is a factor of $f(x)$.

We have $f(0) = 3$ ; $f(1) = 1^3 + 2(1) + 3 = 2$ ; $f(2) = 2^3 + 2(2) + 3 = 3 + 4 + 3 = 0$ , $f(3) = 3^3 + 2(3) + 3 = 2 + 1 + 3 = 1$ ; $f(4) = 4^3 + 2(4) + 3 = 4 + 3 + 3 = 0$ .

$\therefore\ 2, 4 \in Z_5$ are zeros of $f(x) \Rightarrow x - 2, x - 4$ are factors of $f(x)$

$\Rightarrow\ f(x) = (x - 2)(x - 4)q(x)$ where $q(x) \in F[x]$

By long division we can find that $q(x) = x + 1$. $\therefore\ f(x)$ is reducible over $Z_5$ .

**Theorem (without proof).** *$f(x) \in Z[x]$ can be factored as the product of two polynomials of lower degree $r$ and $s$ in $Q[x]$ if and only if $f(x)$ can be factored as the product of two polynomials of the same degree $r$ and $s$ in $Z[x]$.*

**Theorem.2.** *If $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z[x]$ with $a_0 \neq 0$ and if $f(x)$ has a zero in $Q$ then $f(x)$ has a zero $= m$ in $Z$ such that $m \mid a_0$.*

**Proof.** Let $\alpha \in Q$ be a zero of $f(x)$.

$\therefore\ (x-\alpha) \in Q[x]$ is a factor of degree = 1 of $f(x)$.

By the above theorem : $f(x)$ must have a factor of degree 1 in $Z[x]$.

Let $m \in Z$ be the zero in $f(x)$ so that $(x-m)$ is a factor of degree 1 in $Z[x]$.

$\therefore\ f(x) = (x-m)(a_n x^{n-1} + .... + b_0) = a_n x^n + ..... + (-m)b_0$

$\therefore\ (-m)\, b_0 = a_0 \Rightarrow m(-b_0) = a_0$ where $m, a_0, b_0 \in Z$. $\therefore\ m \mid a_0$.

***The Eisenstein Criterion : Let*** $p \in Z$ ***be a prime and***

$f(x) = a_0 + a_1 x + ... + a_n x^n \in Z[x]$. ***If*** $p \nmid a_n$, $p \mid a_0, p \mid a_1, ..., p \mid a_{n-1}$ ***and*** $p^2 \nmid a_0$ ***then*** $f(x)$ ***is irreducible over Q, the set of all rational numbers.***

**e.g.** Consider $f(x) = x^2 - 2 \in Z[x]$. we have $a_0 = -2, a_1 = 0, a_2 = 1$.

Take $p = 2$ which is a prime. $2 \nmid 1 \Rightarrow 2 \nmid a_2, 2 \mid 0 \Rightarrow 2 \mid a_1,\ 2 \mid -2 \Rightarrow 2 \mid a_0$.

$p^2 = 4$ and $4 \nmid -2 \Rightarrow 4 \nmid a_0$.

By Eisenstein criterion $f(x) = x^2 - 2$ is irreducible over $Q$.

**Note.**The conditions $p \nmid a_n$, $p \mid a_0, p \mid a_1, ..., p \mid a_{n-1}$ and $p^2 \nmid a_0$ can also be stated as :

$$a_n \not\equiv 0 \pmod p,\ a_i \equiv 0 \pmod p \text{ for } i < n \text{ and } a_0 \not\equiv 0 \pmod{p^2}.$$

## SOLVED PROBLEMS

**Ex. 1.** *Prove that* $f(x) = x^4 + 2x + 2 \in Q[x]$ *is irreducible over* $Q$.

**Sol.** $f(x) = 2 + 2x + 0x^2 + 0x^3 + 1x^4$ so that $a_0 = 2, a_1 = 2, a_2 = 0, a_3 = 0, a_4 = 1$

Consider $p = 2 \in Z$ which is a prime.

We have $2 \nmid a_4 = 1, 2 \mid a_0 = 2, 2 \mid a_1 = 2, 2 \mid a_2 = 0, 2 \mid a_3 = 0$ and $2^2 \nmid a_0 = 2$.

By Eisenstein Criterion, $f(x)$ is irreducible over $Q$.

**Ex. 2.** *Prove that* $f(x) = 25x^5 - 9x^4 + 3x^2 - 12 \in Z[x]$ *is irreducible over* $Q$.

**Sol.** $f(x) = -12 + 0x + 3x^2 + 0x^3 - 9x^4 + 25x^5$

so that $a_0 = -12, a_1 = 0, a_2 = 3, a_3 = 0,\ a_4 = -9, a_5 = 25$.

Consider $p = 3 \in Z$ which is a prime.

We have $3 \nmid a_5 = 25, 3 \mid a_0 = -12, 3 \mid a_1 = 0, 3 \mid a_2 = 3,\ 3 \mid a_3 = 0, 3 \mid a_4 = -9$.

Also $3^2 \nmid a_0 = -12$. By Eisentein criterion $f(x)$ is irreducible over $Q$.

**Ex. 3.** *If* $f(x) = 8x^3 + 6x^2 - 9x + 24$ *verify whether* $f(x)$ *satisfies Eisenstein criterion for irreducibility.*

**Sol.** Here $a_0 = 24, a_1 = -9, a_2 = 6, a_3 = 8$.

$p = 2$ is such that $2 \mid a_3, 2 \mid a_0, 2 \nmid a_1$ $2 \mid a_2$ and $2^2 \mid a_0$.

$p = 3$ is such that $3 \nmid a_3, 3 \mid a_0, 3 \mid a_1, 3 \mid a_2$ and $3^2 \nmid a_0$.

$\therefore$ $p = 2$ does not satisfy Eisenstein criterion while $p = 3$ satisfies Eisentein criterion.

**Ex. 4.** *Prove that* $x^2 + x + 4 \in Z_{11}[x]$ *is irreducible over* $Z_{11}$.

**Sol.** $Z_{11} = \{ 0, 1, 2, ..., 10 \}$. Let $f(x) = x^2 + x + 4$.

$f(0) = 4 \neq 0, f(1) = 6 \neq 0, f(2) = 10 \neq 0, f(3) = 5 \neq 0, f(4) = 2 \neq 0, f(5) = 1 \neq 0$,

$f(6) = 2 \neq 0, f(7) = 5 \neq 0, f(8) = 10 \neq 0, f(9) = 6 \neq 0$ and $f(10) = 4 \neq 0$.

$\therefore$ $x - \alpha$ where $\alpha = 0, 1, ..., 10$ is not a factor of $f(x)$. Since $\deg f(x) = 2$, it should have two linear factors (factors of first degree) for reducibility.

$\therefore$ $f(x)$ is irreducible over $Z_{11}$.

**Ex. 5.** *Prove that* $f(x) = x^4 - 22x^2 + 1 \in Z[x]$ *is irreducible over* $Q$.

**Sol.** If $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$ then $a_0 = 1$.

$a_0 = 1$ has two factors $-1$ and 1 in Z.

$f(-1) = 1 - 22 + 1 = -20 \neq 0, f(1) = 1 - 22 + 1 = -20 \neq 0$. $\therefore$ $f(x)$ has no linear factor.

Let $x^4 - 22x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ in $Z[x]$.

Equating the corresponding coefficients,

$a + c = 0$ ... (1), $b + d + ac = -22$ ... (2), $ad + bc = 0$ ... (3)

and $bd = 1$ ... (4) where $a, b, c, d \in Z$.

$(4) \Rightarrow bd = 1 \Rightarrow b = d = 1$ or $b = d = -1$.

$b = d = 1$ and (2) result $\Rightarrow 2 + ac = -22 \Rightarrow ac = -24$.

$b = d = -1$ and (2) result $\Rightarrow -2 + ac = -22 \Rightarrow ac = -20$.

$(1) \Rightarrow a + c = 0 \Rightarrow a = -c$.

$ac = -24$ and $a = -c \Rightarrow c^2 = 24$ and $ac = -20$ and $a = -c \Rightarrow c^2 = 20$.

But $c^2 = 24$ or $c^2 = 20$ are impossible in Z.

$\therefore$ $f(x)$ has no factors of 2nd degree. Hence $f(x)$ is irreducible in $Q$.

## 12. 8. IDEAL STRUCTURE IN $F[x]$

If $F[x]$ is the set of all polynomials over a field $F$ then $F[x]$ is an integral domain.

So, $\{O(x)\}$ is a trivial ideal and $F[x]$ itself is an improper ideal of $F[x]$.

If $R$ is a commutative ring with unity and $a \in R$, We learnt in the earlier chapter, that the set $Ra = \{ ra \mid r \in R \}$ of all multiples of '$a$' is the principal ideal $= \langle a \rangle$, generated by '$a$'.

Since $F[x]$ is an integral domain, we can think of its principal ideals other than the zero trivial ideal $\{ O(x) \} = \langle O \rangle$ generated by zero polynomial and the improper ideal $= F[x] = \langle 1 \rangle$ generated by the unity polynomial.

**Theorem 1.** ***If $F[x]$ is the set of all polynomials over a field F then every ideal in $F[x]$ is a principal ideal. (or) $F[x]$ is a principal ideal ring.*** ***(O. U. 05, S. V. U. 04)***

**Proof.** Let $U[x]$ be an ideal of $F[x]$.

Let $U[x] = \{ O(x) \}$, the trivial ideal.

$\therefore U[x] = \langle O(x) \rangle$ is the principal ideal generated by the zero polynomial.

Let $U[x] \neq \{ O(x) \}$ and $g(x) \in U[x]$ be a constant polynomial.

Then $g(x) \in F$ and $g(x) \neq O(x)$ and hence a unit of F.

$\therefore U[x] = F[x] = \langle 1 \rangle$, the principal ideal.

Let $\deg g(x) \geq 1$ and be a polyomial of least degree.

Consider any element $f(x) \in U[x]$. Then $f(x), g(x) \in F[x]$.

By using Division Algorithm; there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = g(x)\,q(x) + r(x)$ where $\deg r(x) < \deg g(x)$.

Since $U[x]$ is an ideal, $g(x) \in U[x]$, $q(x) \in F[x] \Rightarrow g(x)q(x) \in U[x]$.

Also $f(x) \in U[x]$, $g(x)q(x) \in U[x] \Rightarrow f(x) - g(x)q(x) \in U[x]$.

$\therefore r(x) \in U[x]$.

Since $g(x)$ is a polynomial of least degree in $U[x]$; $\deg r(x) < \deg g(x) \Rightarrow r(x) = O(x)$.

Thus $f(x) = g(x)\,q(x) \;\forall\; f(x) \in U[x]$.

$\therefore U[x] = \langle g(x) \rangle$, the principal ideal generated by $g(x)$.

Hence every ideal $U[x]$ in $F[x]$ is a principal ideal.

**Note. 1.** Let $g(x) = 0 + 1x = x \in F[x]$ and $f(x) = a_0x + a_1x + \ldots + a_nx^n \in F[x]$.

Then $g(x)f(x) = x\,f(x) = a_0x + a_1x^2 + \ldots + a_nx^{n+1}$ having zero constant term.

Therefore $\langle x \rangle = \{ x\,f(x) \mid f(x) \in F[x] \}$ is the set of all polynomials in $F[x]$ having zero constant term.

Hence $\langle x \rangle = \{ x\,f(x) \mid f(x) \in F[x] \}$ the principal ideal generated by $x \in F[x]$, is the set of all polynomials in $F[x]$ having zero constant term.

**2.** From Ex. 3 of Art. 4.5 we observe that $\langle x \rangle =$ the set of all polynomials of $F[x]$ with zero constant term = Ker of $\phi_0$ where $\phi_0 : F[x] \to F$ is the evaluation homomorphism.

By fundamental theorem of homomorphism, $F \cong F[x]/\text{Ker}\ \phi_0$.

**Definition.** *An integral domain $D$ is a **principal ideal domain (P.I.D.)** if every ideal in $D$ is a principal ideal.*

**Definition. (Maximal ideal)** *A maximal ideal $M[x]$ of the field of polynomials $F[x]$ is an ideal different from $F[x]$ such that there is no proper ideal $U[x]$ of $F[x]$ properly containing $M[x]$.*

**Definition. (Prime ideal)** *An ideal $U[x] \neq F[x]$ of $F[x]$ is said to be prime ideal if $\forall\ f(x), g(x) \in F[x]$ and $f(x)\, g(x) \in U[x] \Rightarrow f(x) \in U[x]$ or $g(x) \in U[x]$.*

***We also observe that every maximal ideal of $F[x]$ is a prime ideal.***

**Theorem. 2.** ***An ideal $\langle p(x) \rangle \neq O(x)$ generated by $p(x) \in F[x]$ is maximal if and only if $p(x)$ is irreducible over F.***

**Proof.** Let $\langle p(x) \rangle \neq O(x)$ be a maximal ideal.

By the definition of maximal ideal, $\langle p(x) \rangle \neq F[x]$.

$\therefore\ \langle p(x) \rangle \neq \langle 1 \rangle$ and hence $p(x)$ is not a constant polynomial *i.e.* $p(x) \notin F$.

If possible, suppose that there exist $f(x), g(x) \in F[x]$ so that $p(x) = f(x)\, g(x)$

and both of lower degree than degree of $p(x)$.

$\langle p(x) \rangle$ is maximal ideal $\Rightarrow \langle p(x) \rangle$ is prime ideal.

$\therefore\ p(x) = f(x)\, g(x) \in \langle p(x) \rangle \Rightarrow f(x) \in \langle p(x) \rangle$ or $g(x) \in \langle p(x) \rangle$

$\Rightarrow p(x) \mid f(x)$ or $p(x) \mid g(x)$.

$p(x) \mid f(x) \Rightarrow p(x)$ is a factor of $f(x) \Rightarrow \deg\ p(x) < \deg\ f(x)$.

$p(x) \mid g(x) \Rightarrow p(x)$ is a factor of $g(x) \Rightarrow \deg\ p(x) < \deg\ g(x)$.

This is a contradiction. $\therefore$ Our supposition is wrong.

$\therefore\ p(x)$ is irreducible over $F$.

**Conversely,** Let $p(x)$ be irreducible over $F$.

If possible, suppose that there exists an ideal $U[x]$ such that $\langle p(x) \rangle \subseteq U[x] \subseteq F[x]$

Since every ideal of $F[x]$ is a principal ideal, $U[x] = \langle g(x) \rangle$ for some $g(x) \in U[x]$.

$\langle p(x) \rangle \subseteq U[x] = \langle g(x) \rangle \Rightarrow p(x) \in \langle g(x) \rangle \Rightarrow p(x) = g(x)\, q(x)$ for some $q(x) \in F[x]$.

Since $p(x)$ is irreducible over $F$, either $\deg g(x) = 0$ or $\deg q(x) = 0$.

$\deg g(x) = 0 \Rightarrow g(x) \in F$ and is a unit in $F[x] \Rightarrow \langle g(x) \rangle = U[x] = F[x]$.

$\deg q(x) = 0 \Rightarrow q(x)$ = constant polynomial. $\Rightarrow q(x) = a_0$ where $a_0 \in F$ and $a_0 \neq 0$.

Then $p(x) = g(x)\, q(x) \Rightarrow p(x) = g(x) \cdot a_0 \Rightarrow g(x) = (a_0^{-1})\, p(x)$

$\therefore g(x) \in \langle p(x) \rangle \Rightarrow \langle g(x) \rangle = U[x] = F[x]$.

$\therefore \langle p(x) \rangle \subset U[x] \subset F[x]$ is impossible. $\therefore \langle p(x) \rangle$ is a maximal ideal.

**Note.** If $R$ is a commutative ring with unity and $U$ is a maximal ideal of $R$, in the earlier chapter, we learnt that the quotient ring $R/U$ is a field.

**e.g. 1.** $p(x) = x^2 - 2 \in Z[x]$ is irreducible over $Q$. From the above theorem, if $p(x)$ is irreducible over $Q$ and $p(x) \in Q[x]$ then $\langle p(x) \rangle$ is a maximal ideal of $Q[x]$.

Therefore $Q[x]/\langle p(x) \rangle$ is a field.

**e.g. 2.** $p(x) = x^2 + 1 \in R[x]$ is irreducible over $R$.

Also $p(x) = x^2 + 1$ is a maximal ideal of $R[x]$ $\therefore R[x]/\langle p(x) \rangle$ is a field.

**Imp. Note**. If $\langle p(x) \rangle$ in $F[x]$ is a maximal ideal then the elements of the field $F[x]/\langle p(x) \rangle$ are cosets of the form $f(x) + \langle p(x) \rangle$ for $f(x) \in F[x]$.

Zero element in $F[x]/\langle p(x) \rangle$ is $\langle p(x) \rangle$.

## SOLVED PROBLEMS

**Ex. 1.** *Is* $Q[x]/\langle x^2 - 5x + 6 \rangle$ *a field ? Explain.*

**Sol.** $f(x) = x^2 - 5x + 6 = (x-2)(x-3)$ where $x-2, x-3$ are linear factors in $Q[x]$.

$\therefore f(x)$ is not irreducible over $Q$ and hence $\langle f(x) \rangle$ is not a maximal ideal of $Q[x]$.

Hence $Q[x]/\langle f(x) \rangle$ is not a field.

**Ex. 2.** *If* $Q[x]$ *is the field of polynomials then prove* $x^2 - 2$ *is irreducible over* $Q$. *Obtain the elements of the field* $Q[x]/\langle x^2 - 2 \rangle$.

**Sol.** We know that $x^2 - 2$ is irreducible over $Q$. Let $f(x) \in Q[x]$.

By division algorithm, $f(x) = (x^2 - 2)\, q(x) + r(x)$ where $r(x) = O(x)$ or

$\deg r(x) < \deg(x^2 - 2) = 2 \Rightarrow r(x)$ is of first degree.

$\therefore r(x) = a_0 + a_1 x$ where $a_0, a_1 \in Q$.

$\therefore$ Elements of $Q[x]/\langle x^2 - 2 \rangle$ or $Q[x]/U$ where $U = \langle x^2 - 2 \rangle$ are of the form :

$f(x)+U=f(x)+\langle x^2-2\rangle \ \forall \ f(x)\in Q[x]$ and zero element is $\langle x^2-2\rangle=U$

$f(x)+\langle x^2-2\rangle=(x^2-2)\,q(x)+a_0+a_1x+\langle x^2-2\rangle=a_0+a_1x+\langle x^2-2\rangle$

$(\because (x^2-2)\,q(x)\in\langle x^2-2\rangle)$

$=(a_0+\langle x^2-2\rangle)+a_1\,(x+\langle x^2-2\rangle)$

$(\because (a+b)+U=(a+U)+(b+U)$ and $r\,(a+U)=ra+U)$

$=a_0+a_1t$ where $t=x+\langle x^2-2\rangle=x+U$

Also $t^2-2=(x+U)^2-2=(x+U)\,(x+U)-2=x^2+U-2=(x^2-2)+U=U$.

$(\because\ x^2-2\in\langle x^2-2\rangle)$

$=$ zero element of $Q[x]/U$.

## 12. 9. UNIQUENESS OF FACTORISATION IN $F[x]$

In the integral domain $Z$ of integers, if $p, a, b\in Z$ and $p$ is a prime then we know that $p\mid ab\Rightarrow p\mid a$ or $p\mid b$. The set $F[x]$ of all polynomials over the field is an integral domain. An irreducible polynomial $p(x)\in F[x]$ may be considered as analogous to the prime element $p\in Z$.

**Theorem.1.** ***Let*** $p(x)$ ***be an irreducible polynomial in*** $F[x]$. ***For*** $r(x), s(x)\in F[x]$ ***if*** $p(x)\mid r(x)\,s(x)$ ***then either*** $p(x)\mid r(x)$ ***or*** $p(x)\mid s(x)$.

**Proof.** $p(x)$ is irreducible over $F\Rightarrow$ the principal ideal $\langle p(x)\rangle\neq O(x)$ of $F[x]$ is maximal and $\langle p(x)\rangle$ is maximal ideal $\Rightarrow\langle p(x)\rangle$ is prime ideal.

$p(x)$ divides $r(x)\,s(x)\Rightarrow r(x)\,s(x)\in\langle p(x)\rangle\ \Rightarrow r(x)\in\langle p(x)\rangle$ or $s(x)\in\langle p(x)\rangle$.

But $r(x)\in\langle p(x)\rangle\Rightarrow p(x)\mid r(x)$ and $s(x)\in\langle p(x)\rangle\Rightarrow p(x)\mid s(x)$.

$\therefore$ either $p(x)\mid r(x)$ or $p(x)\mid s(x)$.

**Note.** By mathematical induction we can prove that $p(x)\mid r_1(x)\,r_2(x)\ldots r_n(x)$

$\Rightarrow p(x)\mid r_1(x)$ or $p(x)\mid r_2(x)$ or ..... or $p(x)\mid r_n(x)$, when $p(x)$ is irreducible over $F$ and $p(x), r_1(x), \ldots, r_n(x)\in F[x]$.

**Theorem. 2.** ***Let*** $F$ ***be a field and*** $f(x)\in F[x]$ ***be a non-constant polynomial. Then*** $f(x)$ ***can be written as a product of irreducible polynomials in*** $F[x]$ ***in a unique way except for order and for unit factors in F.***

**Proof.** Let $f(x)\in F[x]$ be a non-constant polynomial.

If $f(x)$ is reducible, then $f(x)=p_1(x)\,h(x)$ where $p_1(x), h(x)\in F[x]$

with degree of both $p_1(x), h(x)$ less than the deg $f(x)$.

If both $p_1(x)$ and $h(x)$ are irreducible then our aim is achieved.

If not, at least one of them, say, $h(x)$ can be written as $h(x) = p_2(x) \cdot v(x)$ where $p_2(x), v(x) \in F[x]$ with degree of both less than the degree of $h(x)$.

Continuing the process, by induction, we arrive at a factorisation,

$f(x) = p_1(x) p_2(x) \ldots p_m(x)$ where each $p_i(x), i = 1, 2, ..., m$ is irreducible.

If possible, suppose that $f(x) = q_1(x) q_2(x) \ldots q_n(x)$ be another factorisation of $f(x)$.

$\therefore \; p_1(x)\; p_2(x) \ldots p_m(x) = q_1(x) q_2(x) \ldots q_n(x)$ ... (1)

$p_1(x) \mid f(x) \Rightarrow p_1(x) \mid q_1(x) q_2(x) \ldots q_n(x) \Rightarrow p_1(x) \mid q_i(x)$ for some $i = 1, 2, ..., n$.

Assume that $p_1(x) \mid q_1(x)$.

Since $q_1(x)$ is irreducible we have $q_1(x) = u_1\; p_1(x)$ where $u_1 \neq 0 \in F$ is a unit.

Substituting $u_1\; p_1(x)$ for $q_1(x)$ in (1) and cancelling $p_1(x)$ we get

$p_2(x) p_3(x) \ldots p_m(x) = u_1\; q_2(x) q_3(x) \ldots q_n(x)$ ... (2)

Using similar argument we have $q_2(x) = u_2\; p_2(x)$ where $u_2 \neq 0 \in F$ is a unit.

Substituting $u_2\; p_2(x)$ in (2) and cancelling $p_2(x)$ we get

$p_3(x) \ldots p_m(x) = u_1 u_2\; q_3(x) \ldots q_n(x)$

Continuing, we arrive at $1 = u_1\; u_2 \ldots u_m\; q_{m+1}(x) \ldots q_n(x)$ if $m \leq n$.

Clearly, the above equation is impossible unless $m = n$.

$\therefore$ We arrive at $1 = u_1\; u_2 \ldots u_m$.

Hence the irreducible factors $p_i(x)$ and $q_j(x)$ must be same except possibly for order and units in $F$.

**Note.** We know that from Note under Theorem (1) of Art. 4.7, the factorisation of $f(x) = x^3 + 2x + 3 \in Z_5[x]$ is $(x+1)(x-2)(x-4)$. These irreducible factors must be same except possibly for order and units in $F$ by the above theorem.

It means that $(x+1)(x-2)(x-4) = (2)(3)(x+1)(x-2)(x-4)$ $(\because 6 \equiv 1 \pmod 5)$

$= (3x+3)(2x-4)(x-4)$.

## EXERCISE 12 ( *c* )

**1.** If $f(x) = x^3 + 5x^2 + 4x + 50$ and $g(x) = x - 3$ are polynomials in $Z[x]$ find $q(x)$, the quotient and $r(x)$, the remainder of the Division algorithm.

**2.** (*a*) If $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ and $g(x) = x^2 - 2x + 3$ are polynomials in $Z_5[x]$ find $q(x)$, the quotient and $r(x)$, the remainder of the Division algorithm.

(*b*) If $f(x) = x^4 + 5x^3 - 3x^2; g(x) = 5x^2 - x + 2$ in $Z_{11}[x]$ then find $q(x), r(x)$ of division algorithm. ***(K. U. 07)***

**3.** If $f(x) = 3x^7 + 5x^6 + 2ix^5 - ix^4 + (1+i)x^3 - (2-i)x^2 + 2x - 3i$ and $g(x) = x - 2i$ are poly nomials in $C[x]$ find $q(x)$ and $r(x)$ of Division algorithm.

**4.** Find the factors of $x^4+3x^3+2x+4 \in Z_5[x]$.

**5.** Prove that $x^2-3 \in Z[x]$ is irreducible over the field of rational numbers $Q$ and reducible over the field of real numbers $R$.

**6.** Prove that $1+x^2$ is irreducible over $Z$, the set of integers but it is reducible over $Z_2=\{0,1\}$.

**7.** Prove that $(i)\ x^3+3x+2$ is irreducible over $Z_5$. $(ii)\ x^2+x+2$ is irreducible over $Z_3$.

**(A. U. 07)**

**8.** Using Eisenstein criterion prove that $x^2-2 \in Z[x]$ is irreducible over $Q$.

**9.** Prove that $x^3+3x^2-8 \in Z[x]$ is irreducible over $Q$.

**10.** Prove that $x^3-9$ is reducible over $Z_{11}$.

**11.** Is $f(x)=2x^3+x^2+2x+2 \in Z_5[x]$ an irreducible polynomial in $Z_5[x]$? why ?

**12.** Find all irreducible polynomials of degree '2' in $Z_2[x]$.

**13.** Is $Q[x]/\langle x^2-6x+6\rangle$ a field ? Explain.

**14.** Prove that $x^2+1$ is irreducible over the field $Z_{11}$. Also prove that $Z_{11}[x]/\langle x^2+1\rangle$ is a field having 121 elements.

**ANSWERS**

**1.** $x^2+8x+28\,;134$ **2.** $x^2-x-3\,;\ x+3$

**3.** $3x^6+(5+6i)x^5+(12i-12)x^4-(24+25i)x^3+(51-47i)x^2+(92+103i)x-204+184i\,;$

$-411i-368$. **4.** $(x-1)^3(x+1)$

# Problems for Practicals

1. Construct a field of two elements.
2. Give an example of a division ring which is not a field.
3. Define the characteristic of a ring. Prove that the characteristic of an integral domain $(D,+,\bullet)$ is zero or a positive integer according as the order of any non zero element of $R$ regarded as a member of the group $(D,+)$.
4. Define Boolean ring. Show that every Boolean ring is commutative.
5. Define Integral Domain and Field. Prove that every field is an integral domain.
6. If $D$ is an integral domain then prove that the set $\{n.1 : n \in Z\}$ where '1' is the unity element in $D$, is a subdomain of $D$.
7. If the characteristic of a commutative ring $R$ is 2 then prove that $(x+y)^2 = x^2 + y^2 = (x-y)^2 \ \forall\ x, y \in R$.
8. Prove that the characteristic of an integral domain is either zero or prime.
9. Do the following sets form integral domain with respect to ordinary addition and multiplication ?

   $(a)$ $D = \{a\sqrt{2} \mid a \in Q\}$ $(b)$ the set of even integers.
10. Prove that the set of Gaussian integers is an integral domain.
11. Prove that $Z_p = \{0,1,2,\ldots\ldots, p-1\}$ where $p$ is a prime, is a field.
12. Prove that $Z_5 = \{0,1,2,3,4\}$ is a commutative ring with unity under addition and multiplication modulo5. Prove that it has no zero divisors and hence an integral domain.
13. Prove that in the ring $Z_n = \{0,1,2,\ldots\ldots,n-1\}$ the zero divisors are precisely the elements that are not relatively prime to $n$.
14. Prove that the ring $Z_n = \{0,1,2,\ldots\ldots,n-1\}$ is a field if and only if $n$ is a prime.
15. In the ring of $2\times2$ matrices over the integers $Z$ : write $(i)$ Zero element $(ii)$ Unity element and $(iii)$ give an example to show that it has zero divisors.
16. In the ring of $2\times2$ matrices over the integers $Z$ give examples of $(i)$ left ideal which is not a right ideal and $(ii)$ right ideal which is not a left ideal.
17. Define idemptent element in a ring. If $R$ is a non - zero ring so that $a^2 = a \ \forall\ a \in R$ prove that characteristic of $R = 2$.
18. Define idempotent element in a ring. Show that a field contains exactly two idempotent elements.

**19.** Define the concept of evaluation homomorphism. Prove that the evaluation homomorphism $\phi_\alpha$ maps $F[x]$ isomorphically to $F$ by identity map.

**20.** Evaluate the following by using evaluation homomorphism $\phi_\alpha : Z_7[x] \to Z_7$.

(*i*) $\phi_3 : (2+3x-x^2+2x^3)$ (*ii*) $\phi_5 : (2+x^3)(1+3x^2+x^7)$

**21.** If $F$ is a subfield of a field $E$ and $f(x) \in F(x)$ then prove that the set of all zeros of $f(x)$ in $E$ is an ideal of $E$.

**22.** State division algorithm in $F[x]$. Prove that $\alpha \in F$ is a zero of $f(x) \in F[x]$ *iff* $(x-\alpha)$ is a factor of $f(x)$.

**23.** If $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1,\ g(x) = x^2 - 2x + 3 \in Z_5[x]$ find $q(x)$ and $r(x)$ of the division algorithm.

**24.** Define irreducible polynomial in $F[x]$. Prove $x^2 + x + 4$ is irreducible over the field of integers modulo 11.

**25.** Is the concept of irreducibility global ? Give an example and explain.

**26.** If $f(x)$ is a polynomial of degree 2 or 3 prove that $f(x)$ is reducible over the field $F$ *iff* it has a zero in $F$.

**27.** Show that $f(x) = x^4 - 2x^2 + 8x + 1$ is irreducible over $Q$.

**28.** State Eisenstein criterion for irreducibility. Using it prove that $x^2 - 2$ is irreducible over $Q$.

**29.** Obtain the linear factors of $x^4 + 4 \in Z_5[x]$.

**30.** Find irreducible polynomials of deg 2 in $Z_2[x]$ and $Z_3[x]$.

**31.** Show that $f(x) = 2x^3 + x^2 + 2x + 2$ has no zeros in $Z_5$.

**32.** Using Eisentein criterion prove that $x^3 + 3x^2 - 8 \in Z[x]$ is irreducible over $Q$.

**33.** Using division algorithm obtain the factors of $x^4 + 3x^3 + 2x + 4 \in Z_5[x]$ in $Z_5$.

**34.** Prove that a ring has zero divisors if and only if cancellation hold in the ring.

**35.** Show that $Z[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in Z\}$ is an integral domain under addition and multiplication of numbers.

**36.** If $R_1, R_2, \ldots\ldots, R_n$ are rings then prove that $R_1 \times R_2 \times \ldots\ldots \times R_n = \{(r_1, r_2, \ldots\ldots, r_n) / r_i \in R_i\}$ form a ring w.r.t. component wise addition and multiplication.

**37.** $R = 2Z \times Z$ is what type of ring w.r.t. addition and multiplications by components ?

**38.** Compute the products in the given ring R when - a is additive inverse of a in R.

(*i*) (12) (16) in $Z_{24}$ (*ii*) (16) (3) in $Z_{32}$ (*iii*) $(-4)$ in $Z_{15}$

(*iv*) (20) $(-8)$ in $Z_{26}$ (*v*) (2,3) (3,5) in $Z_5 \times Z_9$ (*vi*) $(-3,5)$ $(2,-4)$ $Z_4 \times Z_{11}$

**39.** Give example of a ring with unity in which unit element is same as Zero element.

**40.** Define an Idempotent element and prove that product of any two idempotent elements is again idempotent element in a commutative ring. Find all idempotent elements in $Z_6 \times Z_{12}$.

**41.** Define Boolean ring and prove that every Boolean ring is commutative.

**42.** (*i*) If S is a non empty set containing n elements. Prove that P (S) forms finite Boolean ring w.r.t. '+' and '.' defined as $A + B = (A \cap B) - (A \cup B)$, $A \,.\, B = A \cap B \;\forall A, B \in P(S)$

What is order of P(S). (*ii*) Find addition and multiplication tables when $S = \{a, b\}$.

**43.** Consider the system $(S, +, \bullet)$ such that (*i*) $(S, +)$ is a group.

(*ii*) $(S^*, \bullet)$ is a group where $S^*$ is set of all elements of S except additive identity of S.

(*iii*) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc \;\forall\; a, b, c \in S$ then show that S is a division ring.

**44.** If $m \in Z^+$ prove that $\langle Z_m, +_m, \bullet_m \rangle$ is commutative ring with unity and prove that it is an integral domain if *m* is prime.

**45.** Prove that $\{a + b\sqrt{2} / a, b \in Z\}$ with respect to usual addition and multiplication froms an integral domain.

**46.** If $\{a \in Z^+ / a < m, (a, m) \neq 1\}$ are zero divisors in $Z_m$ and then prove that $Z_m$ has no zero divisors when *m* is prime.

**47.** Solve the equation (*i*) $x^2 - 5x + 6 = 0$ (*ii*) $x^3 - 2x^2 - 3x = 0$ in $Z_{12}$

**48.** Show that the set Q of all real quaternions forms a strictly skew field w.r.t. addition and multiplication of quaternions.

**49.** Give an example of a field F (by verifying field axioms) such that $Q \subset F \subset R$ when Q, R are rational, real fields.

**50.** Define unit in an integral Domain. Find all units in the Domain of Gaussian Integers.

**51.** Find the number of units in $\langle Z_m, +_n, \bullet_n \rangle$ when $n \in Z^+$ and hence find all units of $Z_{50}$

**52.** Find the order of the matrix ring $M_2(Z_2)$ and also find all units of it.

**53.** If $(R, +, \bullet)$ is an integral domain and U is collection of all units in R, prove that $(U, \bullet)$ is a group.

**54.** If *p* is prime show that $(a+b)^p = a^p + b^p$ in $Z_p$.

**55.** If R is ring with unity, prove that characteristic of R is either 0 or *n* according as the order of unit element in $(R, +)$ is either 0 or *n* respectively.

**56.** Prove that $(F, +_{10}, \bullet_{10})$ is a field and find is characteristic when $F = \{0, 2, 4, 6, 8\}$

**57.** Find characteristic of the following rings.

(*i*) $2Z$ (*ii*) $Z \times Z$ (*iii*) $Z_3 \times 3Z$ (*iv*) $Z_3 \times Z_4$ (*v*) $Z_6 \times Z_{15}$

**58.** If R is a commutative rign with unity of characteristic 3, compute and simplify

(*i*) $(x+y)^6$ (*ii*) $(x+y)^9 \forall x, y \in R$

**59.** Show that characterstic of sub domain of an integral domain D is same as characteristic of D.

**60.** Prove that characteristic of a field is zero or prime. Justify this result by giving one example to each.

**61.** Show that $M_2(F)$, the set of all $2 \times 2$ matrices over a field F is a non- commutative ring under matrix addition and matrix multiplication.

**62.** Show that $M_2(Q)$ is a non-commutative ring under usual operations.

**63.** Show that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is unity in $M_2(F)$. Describe the unity element in $M_n(F)$.

**64.** (*a*) Find all units in the ring $Z \times Z$

(*b*) Find the solutions of the equation $x^2 + x - 6 = 0$ in the ring $Z_{14}$ by factoring the quadratic polynomial.

**65.** (*a*) Find all units in the ring $Z_5$

(*b*) Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ in $Z_{12}$.

**66.** (*a*) Find all units in the ring $Z \times Q \times Z$

(*b*) Solve the equation $3x = 2$ in the field $Z_7$.

**67.** (*a*) Find all units in the ring $Z_4$.

(*b*) Find the characteristic of the ring $Z_3 \times Z_4$.

**68.** (*a*) Find all units in the matrix ring $M_2(Z_2)$.

(*b*) Find the characteristic of the ring $Z \times Z$.

**69.** (*a*) Find all solutions of the equation $x^2 + 2x + 2 = 0$ in $Z_6$.

(*b*) Find the characteristic of the ring $Z_3 \times 3Z$.

**70.** (*a*) Find the characteristic of the ring $2Z$.

(*b*) Let R be a commutative ring with unity of characteristic 4. Compute and simplify $(a+b)^4$ for $a, b \in R$.

**71.** (*a*) Find the characteristic of the ring $Z_6 \times Z_{15}$.

(*b*) Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a+b)^6$ for $a,b \in R$.

**72.** Let $\phi_2 : Q[x] \to R$ be defined by $\phi_2(a_0 + a_1x + .... + a_nx^n) = a_0 + a_1 2 + .... + a_n 2^n$.

Then show that $\phi$ is a homomorphism. Find its kernel.

**73.** Find the kernel of the homomorphism $\phi_i : Q[x] \to C$ given by

$\phi_i(a_0 + a_1x + .... + a_2x^2 + .... + a_nx^n) = a_0 + a_1i + a_2i^2 + .... + a_ni^n$ where $i^2 = -1$

**74.** Consider the evaluation homomorphism $\phi_5 : Q[x] \to R$. Find six elements in the kernel of $\phi_5$.

**75.** Evaluate each of the following for the indicated evaluation homomorphism $\phi_a : Z_7[x] \to Z_7$

(*i*) $(x^2+3)\,\phi_2$ (*ii*) $(2x^3 - x^2 + 3x + 2)\,\phi_0$ (*iii*) $[(x^4+2x)(x^3-3x^2+3)]\,\phi_3$

**76.** (*a*) Find the characteristic of the ring $Z_3 \times Z_3$

(*b*) If $\phi_\alpha : Z_7 \to Z_7$ is the evaluation Homomorphism, then compute

$\phi_3\,[(x^4+2x)\,(x^3-3x^2+3)]$

**77.** (*a*) Find all solutions of $x^2 - 2x + 4 = 0$ in $Z_6$

(*b*) If $\phi_a : C \to C$ is the evaluation Homomorphism, then compute $\phi_2\,(x^2+3)$

**78.** In $Z_5[x]$ divide $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ by $g(x) = x^2 - 2x + 3$ to find $q(x)$ and $r(x)$

**79.** Let $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ be in $Z_7[x]$. Find $q(x)$ and $r(x)$ in $Z_7[x]$ such that $f(x) = g(x)\,q(x) + r(x)$ with (degree $r(x)) < 2$

**80.** Let $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = 3x^2 + 2x - 3$ be in $Z_7[x]$. Find $q(x)$ and $r(x)$ in $Z_7[x]$ such that $f(x) = g(x)\,q(x) + r(x)$ with (degree $r(x)) < 2$

**81.** (*a*) Consider $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$, $g(x) = x^2 + 2x - 3$ in $Z_7[x]_j$ and the division algorithm.

$f(x) = g(x)q(x) + r(x)$, $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$, then find $q(x)$ and $r(x)$.

(*b*) The polynomial $x^4 + 4$ can be factored into linear factors in $Z_5[x]$. Find this factorization.

**82.** (*a*) Find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or of degree less than the degree of $g(x)$, where $f(x) = x^5 - 2x^4 + 3x - 5, g(x) = 2x + 1$ in $Z_{11}[x]$.

(*b*) Is $2x^3+x^2+2x+2$ on irreduible polynomial in $Z_5[x]$ ? Why ? Express it as a product of irreducible polynomials in $Z_5[x]$.

**83.** (*a*) Show that $f(x)=x^2+6x+12$ is irreducible over Q. Is $f(x)$ irreducible over R ?

(*b*) Find all prime ideals and all maximal ideals of $Z_6$.

**84.** (*a*) Demonstrate that $x^4-22x^2+1$ is irreducible over Q.

(*b*) Find all prime ideals and all maximal ideals of $Z_{12}$.

**85.** (*a*) The polynomial $2x^3+3x^2-7x-5$ can be factored into linear factors in $Z_{11}[x]$. Find this factorization.

(*b*) Find all prime ideals and all maximal ideals of $Z_2\times Z_2$

**86.** (*a*) Find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x)=g(x)\,q(x)+r(x)$ with $r(x)=0$ or of degree less than the degree of $g(x)$, where $f(x)=x^4+5x^3-3x^2, g(x)=5x^2-x+2$ in $Z_{11}[x]$.

(*b*) Find all $c\in Z_3$ such that $Z_3[x]/<x^2+c>$ is a field.

**87.** Find all $c\in Z_5$ such that $Z_5[x]/<x^2+cx+1>$ is a field.

**88.** (*a*) Find $c\in Z_3$ such that $Z_3[x]/<x^3+cx^2+1>$ is a field.

(*b*) Find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x)=g(x)\,q(x)+r(x)$ with $r(x)=0$ or of degree less than the degree of $g(x)$, where $f(x)=x^6+3x^5+4x^2-3x+2$ and $g(x)=3x^2+2x-3$ in $Z_7[x]$.

**89.** Show that for a field F, the set S of all matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ for $a,b\in F$ is a right ideal but not a left ideal of $M_2(F)$. Is 'S' a sub ring of F ?

**90.** Let A and B be ideals of a commutative ring R. The quotient A : B of A by B is defined by $A:B\{r\in R/rb\in A$ for all $b\in B\}$.

Show that A : B is an ideal of R.

**91.** The polynomial $x^4+4$ can be factored into linear factors in $Z_5[x]$. Find this factorization.

**92.** Define an irreducible and reducible polynomials and show that $f(x)=x^3+3x+2$ is irreducible over $Z_5[x]$

**93.** Show that $f(x)=x^4-2x^2+8x+1$ viewed in $Q[x]$ is irreducible over Q.

**94**. State Eisenstein criterion and apply the same to prove

(*i*) $f(x) = x^3 + 7x^2 + 14x - 7$ (*ii*) $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$

(*iii*) $f(x) = x^2 - 4x + 2$ (*iv*) $f(x) = 3x - 6$ (*v*) $f(x) = x^2 + 6$

are irreducible over Q.

As a special case $f(x) = x^n - p$, is always irreducible over Q where $p$ is prime, $n$ belongs to $Z^+$.

**95.** Show that (*i*) $f(x) = x^2 + x + 1$ is irreducible over the field of integers modulo 2.

(*ii*) $f(x) = x^2 + 1$ is irreducible over the field of integers modulo 7.

(*iii*) $f(x) = x^3 - 9$ is irreducible over the field of integers modulo 31

(*iv*) $f(x) = x^3 + 2x + 3$ is irreducible over the field of integers modulo 5.

**96.** Show that $f(x) = x^2 + x + 4$ is irreducible over the field of integers modulo 11.

$f(x) = x^3 - 9$ is irreducible over the field of integers modulo 11.

**97.** Show that Eisenstein criterion is not necessary for irreducibility for $f(x) = x^3 - x + 1, f(x) = x^3 + x^2 + 3x - 1$

**98.** Show that the polynomial $C_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x^2 + x + 1$ is irreducible over Q. As special case $f(x) = x^p + 1 = x^p + a, a \in Z_p$ are irreducible over Q, where $p$ is a prime.

## OBJECTIVE TYPE QUESTIONS

### MULTIPLE CHOICE QUESTIONS:

**1.** For any two elements $a$, $b$ in a ring, $a(-b) =$

($a$) $-(ab)$ ($b$) $ab$ ($c$) $-(ba)$ ($d$) none

**2.** If $(R, +, \bullet)$ is a ring then $(R, +)$ is

($a$) a group ($b$) an abelian group ($c$) a finite group ($d$) semi group

**3.** The residue classes modulo 11 with respect addition and multiplication modulo 11 is

($a$) commutative ring ($b$) an integral domain ($c$) a field ($d$) skew field

**4.** The characteristic of the residue classes mod 8 is

($a$) 0 ($b$) 2 ($c$) 8 ($d$) none

**5.** If $F$ is a field then the number of ideals in $F$ is

($a$) 0 ($b$) 1 ($c$) 2 ($d$) infinite

**6.** If $a$, $b$ are nilpotent elements in a commutative ring then $ab$ is

($a$) nilpotent ($b$) not nilpotent ($c$) idempotent ($d$) zero

**7.** The characteristic of the field of rational numbers is .
(*a*) 0 (*b*) $\infty$ (*c*) a prime (*d*) none

**8.** For $(M_2, +, \bullet)$ ring. $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in Z \right\}$ is a
(*a*) left ideal (*b*) right ideal (*c*) subring (*d*) none

**9.** With the usual addition and multiplication, the set of all even integers is
(*a*) a ring (*b*) a field (*c*) an integral domain (*d*) none

**10.** The number of proper ideals of a field is
(*a*) 0 (*b*) 1 (*c*) 2 (*d*) none of these

**11.** The set $\{a + bi \mid a, b \in Z, i^2 = -1\}$ of Gaussian integers is
(*a*) ring (*b*) integral domain (*c*) field (*d*) none

**12.** A commutative ring satisfying cancellation laws is a
(*a*) field (*b*) skew field (*c*) integral domain (*d*) none

**13.** $M = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \in Z \right\}$. For the ring $R$ of $2 \times 2$ matrices over $Z$, $M$ is
(*a*) ideal (*b*) left ideal (*c*) right ideal (*d*) subring

**14.** In the ring $Z$ of integers the ideal generated by 7 is
(*a*) prime ideal (*b*) maximal ideal (*c*) not maximal (*d*) none

**15.** For the homomorphism $f : R \to R$ defined by $f(x) = x \; \forall \; x \in R$ Ker $f$ =
(*a*) $\{0\}$ (*b*) $R$ (*c*) $\{0, 1\}$ (*d*) none

**16.** In the ring of integers $Z$, the units are
(*a*) 0, 1 (*b*) 1 only (*c*) $1, -1$ only (*d*) none

**17.** If $a$, $b$ are two non-zero elements of an euclidean ring $R$ and $b$ is a unit in $R$, then
(*a*) $d(ab) = d(a)$ (*b*) $d(ab) > d(a)$ (*c*) $d(ab) < d(a)$ (*d*) none

**18.** In the ring $Z_6$, the associates of 2 are
(*a*) 1, 5 (*b*) 0, 2 (*c*) 2, 4 (*d*) 0, 2, 4

**19.** In the ring of integers $Z$ every integer has
(*a*) only one associate (*b*) only two associates
(*c*) need not have an associate (*d*) none

**20.** If $F$ is a field and $f : F \to R$ is a homomorphism so that Ker $f = \{0\}$ then $f$ is
(*a*) isomorphism (*b*) monomorphism (*c*) zero homomorphism (*d*) none

**21.** If $a$, $b$ are associates in an Euclidean ring then
(*a*) $d(a) < d(b)$ (*b*) $d(a) = d(b)$ (*c*) $d(b) < d(a)$ (*d*) none

**22.** In the ring $Z[i]$ of Gaussian integers $1 + i$ is
(*a*) unit (*b*) unity element (*c*) prime element (*d*) none

**23.** If $f(x), g(x)$ are two non-zero polynomials over a ring $R[x]$ then $\deg\{f(x)+g(x)\}$ is
(*a*) $= \deg f(x) + \deg g(x)$ (*b*) $\leq \max\{\deg f(x), \deg g(x)\}$
(*c*) $\geq \max\{\deg f(x), \deg g(x)\}$ (*d*) none

**24.** If $f(x) = 2+4x+2x^2$, $g(x) = 2x+4x^2$ over the ring $(I, +_6, \times_6)$ the $\deg\{f(x)+g(x)\} =$
(*a*) 0 (*b*)1 (*c*) 2 (*d*) none

**25.** For the data in problem (24), $\deg\{f(x).g(x)\} =$
(*a*) 4 (*b*) 2 (*c*) 0 (*d*) none

**26.** A polynomial $f(x)$ in $F[x]$ is reducible if it has
(*a*) proper divisors (*b*) improper divisors (*c*) prime divisors (*d*) none

**27.** The polynomial $x^2+1$ is
(*a*) reducible over real field (*b*) reducible over complex field
(*c*) irreducible over complex field (*d*) none

**28.** In the field of residues modulo 5, the remainder when $3x^3-4x^2+2x-2$ is divided by $x-3$ by
(*a*) 49 (*b*) 0 (*c*) 4 (*d*) none

**29.** If $U$ is an ideal of ring $R$ with unity 1 such that $1 \in U$ then $U$ is
(*a*) $U$ (*b*) $R$ (*c*) $\subseteq R$ (*d*) none

**30.** Let $R$ be a commutative ring with unity and $a \in R$, then $U = \{ra \mid r \in R\}$ is
(*a*) left ideal only (*b*) ideal only
(*c*) prime ideal (*d*) smallest ideal containing '*a*'

**31.** If $f(x) = a_0 + a_1x + \ldots + a_mx^m, a_m \neq 0$ and $g(x) = b_0 + b_1x + \ldots + b_nx^n, b_n \neq 0$ then $\deg\{f(x)\,g(x)\}$ *is*
(*a*) $< m+n$ (*b*) $m+n$ (*c*) $> m+n$ (*d*) $mn$

**32.** Every ring of numbers with unity is
(*a*) integral domain (*b*) division ring (*c*) field (*d*) none

**33.** The ring $R = \{a+b\sqrt{2} \mid a,b \in Q\}$ is
(*a*) integral domain (*b*) skew field (*c*) field (*d*) none

**34.** If $S_1, S_2$ are two subrings of a ring $R$ then $S_1 + S_2$ is
(*a*) subring (*b*) ideal (*c*) need not be a subring

**35.** A subring $S$ of a ring $R$ is called ideal if
(*a*) $\alpha \in S, a \in R \Rightarrow \alpha a \in S$ (*b*) $\alpha \in S, a \in R \Rightarrow a\alpha \in S$
(*c*) $\alpha \in S, a \in R \Rightarrow \alpha a, a\alpha \in S$ (*d*) none

**36.** The set $Q$ of rational numbers is
(*a*) subring (*b*) ideal
(*c*) not subring (*d*) not ideal, for the ring of real numbers

**37.** Homomophic image of an integral domain is
(*a*) *a* ring (*b*) integral domain (*c*) need not be integral domain (*d*) none

**38.** If $R$ is a non-zero ring so that $a^2 = a \; \forall \; a \in R$ then characteristic of $R =$
(*a*) 0 (*b*) 1 (*c*) 2 (*d*) prime

**39.** If the characteristic of a ring $R$ is 2 and $a, b \in R$ then $(a+b)^2 =$
(*a*) $a^2 + 2ab + b^2$ (*b*) $a^2 + ab + ba + b^2$ (*c*) $a^2 + b^2$ (*d*) none

**40.** If $p$ is a prime, the ring of integers modulo $p$ is .
(*a*) field (*b*) integral domain (*c*) skew field (*d*) none

**41.** $Z_6 = \{0,1,2,3,4,5\}$ is the ring of integers modulo 6 and $U = \{0,3\}$ is an ideal of $Z_6$. Then coset $2 + U =$
(*a*) $\{0,3\}$ (*b*) $\{2,5\}$ (*c*) $\{0,1,2,3,4,5\}$ (*d*) none

**42.** For the homomorphism $f : R \to R$ defined by $f(x) = x \; \forall \; x \in R$ Ker $f$ is
(*a*) $R$ (*b*) $\{0\}$ (*c*) $\subset R$ (*d*) none

**43.** If $f : R \to R'$ is a ring homomorphism then Ker $f$
(*a*) subring of $R$ (*b*) ideal of $R'$ (*c*) ideal of $R$ (*d*) none

**44.** The set of residue classes modulo *m,* with respect to addition and multiplication mod *m* is
(*a*) ring (*b*) integral domain (*c*) field (*d*) none

**45.** A commutative ring zero divisors is a
(*a*) field (*b*) skew field (*c*) integral domain (*d*) none

**46.** Euclidean ring has
(*a*) unity element (*b*) no unity element
(c) no principal ideal ring (*d*) none

**47.** A finite integral domain is
(*a*) field (*b*) ring (*c*) group (*d*) none

**48.** A field is a
(*a*) non commutative ring (*b*) division ring
(*c*) commutative division ring (*d*) none

49. Field $Z_p$ is of characteristic = $p$ where $p$ is
(*a*) prime (*b*) integer (*c*) even integer (*d*) composite

**FILL IN THE BLANKS:**

**50.** If $R$ is a ring without zero divisors then ..... hold in $R$.

**51.** A ring $R$ has no zero divisors if .....

**52.** A division ring has ..... divisors.

**53.** A finite integral domain is a.....

**54.** In a ring $R$ if $a^2 = a$ for $a \in R$ '$a$' is called ..... w. r. t. multiplication.

**55.** $a \neq 0 \in R, R$ is a ring, is called nilpotent element if there exists .....

**56.** If characteristic of a ring $R = 2$ and $a, b \in R$ commute then $(a-b)^2 =$ .....

**57.** A subring of $(Z_6, +_6, \times_6)$ is .....

**58.** A field has ..... ideals.

**59.** The union of two ideals of a ring *R,* ..... of *R.*

**60.** For a field every ideal is .....

**61.** A subring of $(R, +, \bullet)$ which is not an ideal is .....

**62.** In the quotient ring $R / U$ the zero element is and the unity element is .....

**63.** An ideal $U$ of a ring $R$ is prime ideal if .....

**64.** For the ring of integers any ideal generated by prime integer is a .....

**65.** For a commutativering *R,* with unity if $U$ is a maximal ideal then $R/U$ is a .....

**66.** If $f : R \to R'$ is a ring isomorphism and $R$ is an integral domain then $R'$ is .....

**67.** If $f : R \to R'$ is a ring homomorphism then Ker $f$ is .....

**68.** Every non-zero element of a field is a .....

**69.** $a \in R, R$ is Euclidean ring, is a unity iff.....

**70.** In the ring $(Z_6, +_6, \times_6)$ the associates of 2 are .....

**71.** If $f(x) = 2x^3 + 4x^2 + 3x + 2,\ g(x) = 3x^4 + 2x + 4$ over the ring $(Z_5, +_5, \times_5)$ then $f(x) + g(x) =$ .....

**72.** The units of the domainof Gaussian integers are .....

**73.** Every Euclidean ring possesses .....

**74.** If *f, g* are two non-zero polynomials over a ring $R$ and $fg \neq 0$ then deg $fg$ .....

**75.** If $p$ is a prime-elementof the Euclidean ring $R$ and $a, b \in R$ then $p \mid ab \Rightarrow$ .....

**76.** In an Euclidean ring if $p, q$ are prime and $p \mid q$ then *p, q* are .....

**77.** The mapping $f : Z[\sqrt{2}] \to Z[\sqrt{2}]$ defined by $f(m + n\sqrt{2}) = m - n\sqrt{2}\ \forall\ m + n\sqrt{2} \in Z[\sqrt{2}]$ is .....

**78.** A maximal ideal of the ring of integers is generated by.....

**79.** If $U$ is a maximal ideal of the ring $R$ then there exists no ideal $U'$ of $R$ such that .....

**80.** If $a \neq 0$ is an idempotent element of an integral domain with unity then $a =$ .....

**MARK EACH OF THE FOLLOWING TRUE OR FALSE :**

**81.** Every ring with unity element has atleast two units.

**82.** Every ring with unity element has atmost two units.

**83.** The non-zero elements of a field form a group under the multiplication in the field.

**84.** The characteristic of ring $nZ$ is $n$.

**85.** A zero divisor in a commutative ring with unity can have no multiplicative inverse.

**86.** $Q$ is a field of quotients of $Z$.

**87.** $Z_4$ is an ideal of $4Z$.

**88.** If a ring $R$ has zero divisors then every quotient ring of $R$ has zero divisors.

**89.** Every prime ideal of every commutative ring with unity is a maximal ideal.

**90.** If the degrees of $f(x), g(x) \in R[x]$ where $R$ is a ring, are 3, 4 respectively then deg $f(x)\, g(x)$ is always 7.

**91.** $x^2+3$ is irreducible over $Z_7$.

**92.** If $F$ is a field then $F[x]$ is a principal ideal ring.

**93.** If $F$ is a field then the units of $F[x]$ are precisely the non-zero elements of $F$.

**94.** The Kernel of a ring homomorphism is an ideal of the whole ring.

**95.** The rings $Z/4Z$ and $Z_4$ are isomorphic.

## ANSWERS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **1.** $a$ | **2.** $b$ | **3.** $c$ | **4.** $c$ | **5.** $c$ | **6.** $a$ | **7.** $a, c$ | **8.** $c$ | **9.** $a$ | **10.** $a$ |
| **11.** $b$ | **12.** $c$ | **13.** $b$ | **14.** $b$ | **15.** $a$ | **16.** $c$ | **17.** $a$ | **18.** $c$ | **19.** $b$ | **20.** $a$ |
| **21.** $b$ | **22.** $c$ | **23.** $b$ | **24.** $a$ | **25.** $c$ | **26.** $a$ | **27.** $b$ | **28.** $c$ | **29.** $b$ | **30.** $d$ |
| **31.** $b$ | **32.** $a$ | **33.** $c$ | **34.** $c$ | **35.** $c$ | **36.** $a$ | **37.** $c$ | **38.** $c$ | **39.** $c$ | **40.** $a$ |
| **41.** $b$ | **42.** $b$ | **43.** $c$ | **44.** $a$ | **45.** $c$ | **46.** $a$ | **47.** $a$ | **48.** $c$ | **49.** $a$ | |

**50.** cancellation laws

**51.** There exist $a, b \in R$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$

**52.** no zero divisors

**53.** field

**54.** idempotent element

**55.** $n \in N$ so that $a^n = 0$

**56.** $a^2 + b^2$

**57.** $\{\bar{0}, \bar{3}\}$

**58.** no proper

**59.** need not be an ideal

**60.** a principal ideal

**61.** $(Q, +, \bullet)$

**62.** $U, 1+U$

**63.** for all $a, b \in R$ and $ab \in U \Rightarrow a \in U$ or $b \in U$

**64.** maximal ideal

**65.** field

**66.** integral domain

**67.** an ideal of $R$

**68.** a unit

**69.** $d(a) = d(1)$

**70.** 2, 4

**71.** $3x^4 + 2x^3 + 4x^2 + 1$

**72.** $\pm 1, \pm i$

**73.** unity element

**74.** $\leq \deg f + \deg g$

**75.** $p \mid a$ or $p \mid b$

**76.** associates

**77.** automorphism

**78.** prime integer

**79.** $U \subset U' \subset R$

**80.** 1

**81.** True

**82.** False

**83.** True

**84.** False

**85.** True

**86.** True

**87.** False

**88.** False

**89.** False

**90.** False

**91.** False

**92.** True

**93.** True

**94.** True

**95.** True