§ 6.7. Algebraic Structure : *Definition* :

A system consisting of :

(*a*) *A nonvoid family of sets*

(*b*) *A set of binary compositions defined on these sets,*

and (*c*) *A set of specified axioms*

is called an **algebraic Structure or system.**

§ 6.8. Groupoid or Binary Algebra : *Definition :*

*A non empty set G equipped with one binary operation ' * ' is called groupoid*

i.e. G is a groupoid if G is *closed* for * .

It is denoted by (G, *) .

For example : $(N, +)$, $(Z, -)$. $(Q, \times)$ etc.

§ 6.9. Quasi Group :

A nonvoid set S equipped with a binary operation * is called a ***Quasi group*** if for $x, y \in S$, $x * y \in S$ and the equations

$$a * x = b \qquad \text{and} \qquad y * a = b$$

have unique solutions

For example, the algebraic structure $(Z, +)$ is a quasi group, since it is closed wrt addition + of integers and the equations

$$a + x = b \qquad \text{and} \qquad x + a = b$$

have unique solutions in Z for $a, b \in Z$. However, the algebraic structure $(Z, .)$ is not a quasi group since, for $2, 5 \in Z$, $2 . x = 5$ have no solution in Z.

§ 6.10. Loop : *Definition :*

*A quasi group (G, *) is called a loop, if it has the identity element 'e' for its composition * i.e. if there exist e such that*

$$e*a=a*e=a, \quad \forall \quad a \in G$$

§ 6.11. Semi Group : *Definition :*

*An algebraic structure (G, *) is called a semi group if the binary operation * satisfies associative property i.e.*

$[G_1]$ $\quad (a*b)*c=a*(b*c), \quad \forall \quad a,b,c \in G$

Ex.1. The algebraic structures $(N, +)$, $(Z, +)$, $(Z, \times)$, $(Q, \times)$ are semi groups but the structure $(Z, -)$ is not so because subtraction $(-)$ is not associative.

Ex.2. $(Z, +)$ is a monoid since t has the identify element 0 wrt t.

Ex.3. The structures $(P(S), \cup)$ and $(P(S), \cap)$ where P(S) is the power set of a set S are semi groups as both the operations union $(\cup)$ and intersection $(\cap)$ are associative.

Theorem 6.1. ***Let*** $(g, *)$ ***be a semigroup and*** $a \in G$ ***such that the equations***

$$a * x = b \qquad \text{and} \qquad y * a = b$$

have solutions in G for all $b \in G$. ***Then*** $(G, *)$ ***is a monoid.***

Proof. Since $a * x = b$ and $y * a = b$

have solutions in G for all $b \in G$, these are also true for $a \in G$ itself. That is

$$a * x = a \qquad \text{and} \qquad y * a = a.$$

That is, these are satisfied for some $x = e_R$ and $y = e_L$.

Let any $k \in G$. then

$$k * e_R = (y * a) * e_R = y * (a * e_R) = y * a = k$$

$$e_L * k = e_L * (a * x) = (e_L * a) * x = a * x = k$$

$$k * e_R = k \quad \text{and} \quad e_L * k = k.$$

e_R and e_L are right and left identities in G respectively.

$e_L * e_R = e_R$, since e_L is the left identity

$e_L * e_R = e_L$, since e_R is the right identity.

$e_L = e_R = e$

Hence G contains identity element and so $(G, *)$ is a monoid.

§6.12. Monoid: *Definition :* **[Raj. B.Sc., 06]**

A semi group is called monoid if there exists an identity element ' e ' in G such that:

$$e * a = a * e = a, \quad \forall \quad a \in G$$

$[G_2]$

Ex.1. The semi group $(N, \times)$ is a monoid because 1 is the identity for the multiplication. The semigroup $(N, +)$ is not so because 0, the identity for addition is not in N.

Ex. 2. $(Z, +)$ is a monoid since it has the identity element 0 wrt t.

Ex. 3. The semi groups $(P(S), \cup)$ and $(P(S), \cap)$ are monoid because ϕ and S are the identities respectively for union $(\cup)$ and intersection $(\cap)$ in $P(S)$.

§6.13. Group : *Definition :* **[Raj. B.Sc., 05, 07; Ajmer B.Sc., 07]**

*An algebraic structure of set G and a binary operation * defined in G i.e. (G, *) is a group if * satisfies the following postulates* (***Group Axioms***) :

G_1 **Associativity :** The composition * is associative in G i.e.

$$(a * b) * c = a * (b * c), \quad \forall \quad a, b, c \in G$$

G_2 **Existence of Identity:** There exist an identity element e in G such that

$$e * a = a * e = a, \quad \forall \quad a \in G$$

G_3 **Existence of Inverse:** Each element of G is invertible,

i.e. for every $a \in G$, there exist a^{-1} in G such that

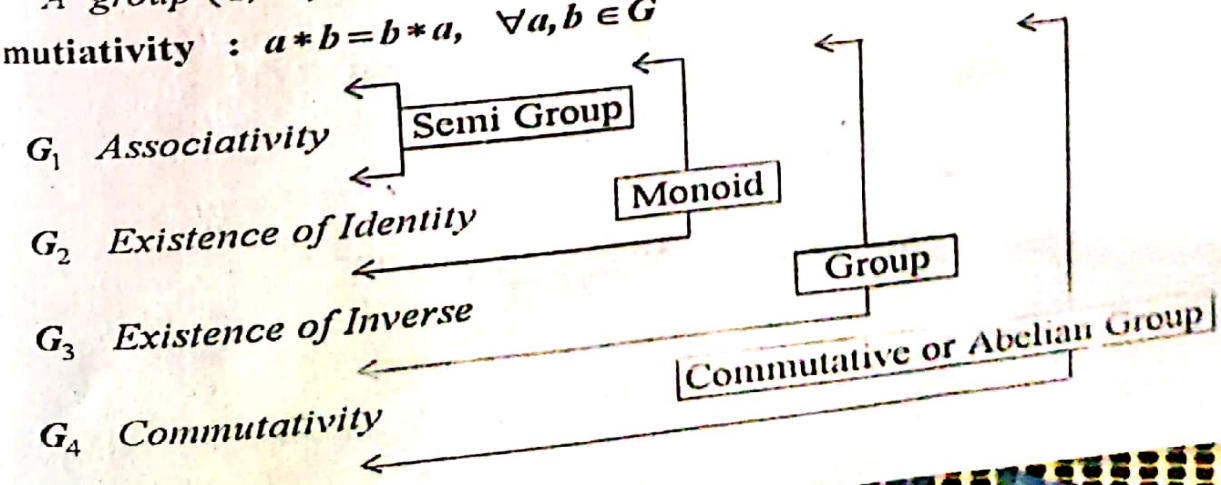
$$a * a^{-1} = a^{-1} * a = e \ (\textit{Identity})$$

Thus group $(G, *)$ is a monoid in which each of its element is invertible.

§6.14. Abelian group or Commutative group: *Definition :*

*A group $(G, *)$ is said to be abelian or commutative if * is commutative also.*

G_4 **Commutiativity** : $a * b = b * a, \quad \forall a, b \in G$



§ 6.15. Finite and Infinite groups :

A group $(G, *)$ is said to be finite if its underlying set G is a finite set and a group which is not finite is called an infinite group.

§ 6.16. Order of a group : *Definition :*

The number of elements in a finite group is called the order of the group.

It is denoted by $O(G)$ or $|G|$.

If $(G, *)$ is an infinite group, then it is said to be of infinite order.

Illustrative Examples

Ex. 1. ***Show that the set $\{1, -1, i, -i\}$ where $i = \sqrt{(-1)}$ is a finite abelian group for multiplication of complex numbers..***

Sol. Let $G = \{1, -1, i, -i\}$.

We prepare the composition table for $(G, \times)$ as follows :

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

On observing the table, it is clear that :

(1) All the entries in the table are elements of G. So multiplication of complex numbers has induced a binary composition in G.

(2) The number 1 is the identity element for the multiplication composition.

(3) The inverses of $1, -1, i, -i$ are $1, -1, -i$ and i respectively.

Since the associativity and commutativity of the multiplication of numbers is obvious, so G is a finite (of order 4)abelian group for multiplication.

Ex. 2. ***Show that the set Q^+ of the positive rational numbers forms an abelian group for the operation *defined as :***

$$a*b = \frac{ab}{2} \qquad \forall\ a, b \in Q^+$$

[Raj. BE III (CS), 13]

Sol. $\because a \in Q^+, b \in Q^+ \Rightarrow a*b = \frac{ab}{2} \in Q^+$

$\therefore$ * is a binary composition in Q^+

Verification of group axioms in $(Q^+, *)$:

$[G_1]$ Associativity : Let $a, b, c \in Q^+$, then

$$(a*b)*c = \frac{ab}{2}*c = \frac{1}{2}\left(\frac{ab}{2} \cdot c\right) = \frac{abc}{4}$$

and $$a*(b*c) = a*\frac{bc}{2} = \frac{1}{2}\left(a \cdot \frac{bc}{2}\right) = \frac{abc}{4}$$

$$(a*b)*c=a*(b*c)$$

$\therefore$ Therefore * is an associative operation.

Existence of identity :

$2\in Q^+$ is the identity element of the operation *

because for $a\in Q^+$, $\quad 2*a=a*2=\frac{a.2}{2}=a$

Existence of Inverse :

For every $a\in Q^+$, $\frac{4}{a}\in Q^+$ $(\because a\neq 0)$ which is the inverse of a

Since $\quad \frac{4}{a}*a=a*\frac{4}{a}=\frac{a\left(\frac{4}{a}\right)}{2}=2$

So every element of Q^+ is invertible.

Commutativity : For any $a,b\in Q^+$

$$a*b=\frac{ab}{2}=\frac{ba}{2} \qquad [\because \text{multiplication is commutative}]$$
$$=b*a$$

$\therefore$ the composition * is commutative.

Hence $(Q^+,*)$ is an abelian group.

Ex. 3. ***Show that*** $G=\left\{\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}:a\in R_0\right\}$ ***is a commutative group under matrix multiplication.*** **[Raj. B.Sc., 16]**

Sol. Let $A=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}, B=\begin{pmatrix} b & 0\\ 0 & 0\end{pmatrix}$ be any two elements of G,

where $a,b\in R_0$; then $\quad AB=\begin{pmatrix} ab & 0\\ 0 & 0\end{pmatrix}$ $\quad \because a\in R_0, b\in R_0\Rightarrow ab\in R_0$

$\therefore AB\in G$ which shows that G is *closed* for matrix multiplication.

Verification of group axioms in (G, ×) :

(1) Since Matrix multiplication is *associative*.

Therefore this is associative in G also.

(2) $E=\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}\in G$ is the identity element because

$$EA=AE=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}=A,\ \forall\ A\in G$$

(3) For every $A=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\in G$, $A_1=\begin{pmatrix} 1/a & 0\\ 0 & 0\end{pmatrix}\in G$ $(\because a\in R_0\Rightarrow 1/a\in R_0)$

$AA_1=A_1A=E$ because

$$A_1 A \equiv A A_1 = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = E \quad \text{(Identity)}$$

$[G_4]$ Since $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}, BA = \begin{pmatrix} ba & 0 \\ 0 & 0 \end{pmatrix}$

and $ab = ba$ (by commutativity of multiplication of real numbers),

Therefore $AB = BA$

As such matrix multiplication is *commutative* in G

Hence G is a commutative group for matrix multiplication.

Ex.4. ***Show that*** $Z_5 = \{0,1,2,3,4\}$ ***is an abelian group for the operation*** $'+_5'$ ***defined as follows :***

$$a +_5 b = \begin{cases} a+b, \text{ if } a+b<5 \\ a+b-5, \text{ if } a+b \geq 5 \end{cases}$$

[Raj. B.Sc., 15]

Sol. The composition table of $(Z_5, +_5)$ is as follows :

$+_5$	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

From the table it is observed that

(1) All the elements are members of Z_5 therefore $'+_5'$ is a binary composition in Z_5.

(2) 0 is the identity element for the composition.

(3) The inverse of 0, 1, 2, 3, 4 are 0, 4, 3, 2, and1 respectively.

Again the base of $'+_5'$ is the addition composition of numbers which is associative and commutative.

Therefore $'+_5'$ is also associative and commutative.

Hence $(Z_5, +_5)$ is a commutative group.

Ex.5. ***Show that the set*** $\{f_1, f_2, f_3, f_4, f_5, f_6\}$ ***is a finite non-abelian group for the operation "composite of functions" where*** $f_i, i = 1,2,...6$ ***are transformations on the infinite complex plane defined by:***

$$f_1(z) = z,\ f_2(z) = \frac{1}{z},\ f_3(z) = 1 - z,\ f_4(z) = \frac{z}{z-1},\ f_5(z) = \frac{1}{1-z},\ f_6(z) = \frac{z-1}{z}$$

[Udaipur, 17; Raj. BE III (CS), 14]

Sol. Let $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ and o denote composite of functions. Now calculating all the possible products under this operation, we have the following :

$$f_1 o f_2(z) = f_1[f_2(z)] = f_1\left(\frac{1}{z}\right) = \frac{1}{z} = f_2(z)$$

$f_3 o f_4(z) = f_3[f_4(z)] = f_3\left(\frac{z}{z-1}\right) = 1-\frac{z}{z-1}$

$f_4 o f_5(z) = f_4[f_5(z)] = f_4\left(\frac{1}{1-z}\right) = \frac{1}{z} = f_2(z)$

$f_5 o f_6(z) = f_5[f_6(z)] = f_5\left(\frac{z-1}{z}\right) = z = f_1(z)$ etc.

Hence we obtain the following composition table of (G, o) :

o	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

The group axioms can be easily verified from the above composition table. Therefore is a finite group.

Moreover since the table is not symmetrical about the leading diagonal so it is a non mutative finite group.

Ex. 6. ***If S is the set of real numbers other than -1, then show that (S, o) is a group where o is the operation defined as :***

$$a o b = a + b + ab, \quad \forall \ a, b \in S$$ **[Raj. B.Sc., 07; Kota B.Sc., 06]**

Sol. Let $a, b \in S \ \therefore a \neq -1, b \neq -1$

First of all we see that $aob \neq -1$, because if $aob = -1$, then

$aob = -1 \Rightarrow a + b + ab = -1 \Rightarrow a + b + ab + 1 = 0$

$\Rightarrow (a+1)(b+1) = 0 \Rightarrow a = -1$ or $b = -1$

which is not possible, $\therefore aob \neq -1$

Again $a \in R, b \in R \Rightarrow a + b + ab \in R$

$\therefore a \in S, b \in S \Rightarrow aob = a + b + ab \in S$

Therefore o is a binary composition in S.

Verification of group axioms in (S, o) :

Let $a, b, c \in S$, then

$$(aob)oc = (a+b+ab)oc = (a+b+ab) + c + (a+b+ab)c$$

$$= a + b + c + ab + bc + ca + abc$$

and $$ao(boc) = ao(b+c+bc) = a + (b+c+bc) + a(b+c+bc)$$

$$= a + b + c + ab + bc + ca + abc$$

$\therefore (aob)oc = ao(boc)$

Therefore o is an associative composition.

$[G_2]$ $0 \in S$ is the identity element of the operation o because for $a \in S$

$$0 \; o \; a = 0 + a + 0 \; a = a \quad \text{and} \quad a \; o \; 0 = a + 0 + a0 = a$$

$[G_3]$ For every $a \in S$, $\dfrac{-a}{a+1} \in S$ $\quad (\because a \neq -1)$

which is the inverse of a because

$$\left(\frac{-a}{a+1}\right) o \, a = \left(\frac{-a}{a+1}\right) + a + \left(\frac{-a}{a+1}\right) a = 0 \quad \text{and} \quad a \, o \left(\frac{-a}{a+1}\right) = a + \frac{-a}{a+1} + a\left(\frac{-a}{a+1}\right) = 0$$

From the above discussion, (S, o) is a group.

Ex.7. If $G = \{(a,b) \mid a,b \in R, a \neq 0\}$ *and* o *is the operation defined in* G *as* $(a,b) o (c,d) = (ac, bc+d)$; *then show that* (G, o) *is a non-abelian group.*

Sol. Verification of group axioms in (G, o):

$[G_1]$ Let $(a,b);(c,d);(e,f)$ be any elements of G, then

$$[(a,b) \, o \, (c,d)] \, o \, (e,f) = (ac, bc+d) \, o \, (e,f)$$

$$= ((ac)e, (bc+d)e + f) \quad = (ace, bce + de + f)$$

and $(a,b) \, o \, [(c,d) \, o \, (e,f)] = (a,b) \, o \, (ce, de+f)$

$$= (a(ce), b(ce) + de + f) \quad = (ace, bce + de + f)$$

$\therefore \; [(a,b) \, o \, (c,d)] \, o \, (e,f) = (a,b) \, o \, [(c,d) \, o \, (e,f)]$

Therefore o is associative.

$[G_2]$ Here $(1,0) \in G$ is the identity element of the operation

because for every $(a,b) \in G$

$$(1,0) \, o \, (a,b) = (1a, 0a+b) = (a,b) \quad \text{and} \quad (a,b) \, o \, (1,0) = (a1, b1+0) = (a,b)$$

$[G_3]$ If $(a,b) \in G$, then $a \neq 0$

$$\therefore \; a \neq 0, a, b \in R \Rightarrow \frac{1}{a} \in R, \frac{-b}{a} \in R \quad \Rightarrow \left(\frac{1}{a}, \frac{-b}{a}\right) \in G$$

Again $(a,b) \, o \left(\dfrac{1}{a}, -\dfrac{b}{a}\right) = \left(a \cdot \dfrac{a}{a}, b \cdot \dfrac{1}{a} - \dfrac{b}{a}\right) = (1,0)$

and $\left(\dfrac{1}{a}, \dfrac{-b}{a}\right) o \, (a,b) = \left(\dfrac{1}{a} \cdot a, \dfrac{-b}{a} \cdot a + b\right) = (1,0)$

$\therefore \left(\dfrac{1}{a}, -\dfrac{b}{a}\right) \in G$ is the inverse of (a, b)

Thus the inverse of every element of G also exists in G

Hence (G, o) is a group.

$[G_4]$ The composition of the group is not commutative because if a, b, c, d are different real numbers, then

$$(a,b) \, o \, (c,d) = (ac, bc+d)$$

$$\neq (ca, da+b)=(c,d)\, o\, (a,b)$$

$$\Rightarrow (a,b)\, o\, (c,d)\neq (c,d)\, o\, (a,b)$$

As such (G, o) is a non abelian group.

§ 6.17. Some Important Properties of Groups :

For convenience, we shall now generally use the symbol ' * ' for the group composition shall write $a*b$ simply as ab unless there is any ambiguity.

Theorem 6.2. (Uniqueness of identity) :

The identity element in a group is unique. **[Raj. BE III (CS), 15]**

Proof : Let $(G, *)$ be a group having two identities e and e', then

e is identity of $G \Rightarrow ee'=e'$ ...(1)

e' is identity of $G \Rightarrow ee'=e$ ...(2)

ee' is a unique element of G.

Hence from (1) and (2), it is proved that $e' = e$

Therefore the identity element of a group is unique . ●

Theorem 6.3. (Uniqueness of inverse)

The inverse of an element in a group is unique. **[Raj. BE III (CS), 14]**

Proof : Let a be any element of the group $(G, *)$ which has two inverses b and c in the

$$a^{-1}=b \Rightarrow ba=e=ab$$

and $$a^{-1}=c \Rightarrow ca=e=ac$$

Now $$ba=e \Rightarrow (ba)\,c=ec$$

$$\Rightarrow b(ac)=c \quad [\text{by } G_1 \text{ and } G_2]$$

$$\Rightarrow be=c \quad [\text{by (2)}]$$

$$\Rightarrow b=c \quad [\text{by } G_2]$$

Therefore the inverse of every element of a group is unique. ●

Remark. The inverse of the identity of a group is itself.

Theorem 6.4. ***If G is a group then for*** $a,b\in G$:

(a) $\left(a^{-1}\right)^{-1}=a$ **[Raj. B.Sc., 16]**

(b) $(ab)^{-1}=b^{-1}a^{-1}$ **(Reversal law)** **[Bikaner, 06]**

i.e. ***the inverse of the product of two elements is the product of their inverses in the*** ***reverse order.***

Proof : (a) Since a^{-1} is the inverse of a, therefore $aa^{-1}=e=a^{-1}a$

$$\Rightarrow a^{-1}a=e=aa^{-1}$$

$$\Rightarrow \text{inverse of } a^{-1}=a, \quad \text{i.e. } \left(a^{-1}\right)^{-1}=a.$$

Remark. *For the additive operation* $-(-a)=a$

(b) Since $a,b,a^{-1},b^{-1},ab,b^{-1}a^{-1}$ all are element of G therefore

$$(ab)\left(b^{-1}a^{-1}\right)=a\left(bb^{-1}\right)a^{-1} \quad [\text{by } G_1]$$

$$=aea^{-1} \quad [\text{by } G_3]$$

$= aa^{-1}$

$= e$ [by G_3]

$\therefore \quad (ab)(b^{-1}a^{-1}) = e$ ...(1)

Again $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$

$= b^{-1}eb$ [by G_1]

$= b^{-1}b$ [by G_3]

$= e$ [by G_2]

$\therefore \quad (b^{-1}a^{-1})(ab) = e$ ...(2)

From (1) and (2), $(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$

$\Rightarrow \quad (ab)^{-1} = b^{-1}a^{-1}$

Generalised reversal law :

By the principle of induction, the above theorem can be generalised as:

$$(abc...p)^{-1} = p^{-1}...c^{-1}b^{-1}a^{-1}$$

Remarks 1. *If the composition is addition (+), then this can be written as :*

$$-(a+b) = (-b)+(-a)$$

2. *If G is a commutative group, then for* $a, b \in G$ $(ab)^{-1} = a^{-1}b^{-1}$

Theorem 6.5. ***Cancellation laws:***

If a,b,c are elements of a group G, then :

(a) $ab = ac \Rightarrow b = c$ ***(Left cancellation law)***

(b) $ba = ca \Rightarrow b = c$ ***(Right cancellation law)***

Proof : $\because \quad a \in G \Rightarrow a^{-1} \in G$ [by G_3]

$\therefore \quad ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [by G_1]

$\Rightarrow eb = ec$ [by G_3]

$\Rightarrow b = c$ [by G_2]

Similarly it can be proved that

$ba = ca \Rightarrow b = c$

Theorem 6.6. ***If a, b are elements of a group G, then the equations*** $ax = b$ ***and*** $ya = b$ ***have unique solutions in G***

Proof : $\because \quad a \in G \Rightarrow a^{-1} \in G$ [by G_3]

$\therefore \quad a \in G, b \in G \Rightarrow a^{-1}b \in G$

Now $a(a^{-1}b) = (aa^{-1})b$ [by G_1]

$= eb$ [by G_3]

$= b$

Therefore $x=a^{-1}b$ is a solution of the equation $ax=b$ in G

Uniqueness: Let the equation $ax=b$ have two solutions $x=x_1$ and $x=x_2$ in G then

$ax_1=b$ and $ax_2=b \Rightarrow ax_1=ax_2$

$\Rightarrow x_1=x_2$ [by left cancellation law]

Therefore the solution of $ax=b$ is unique in G

Similarly its can also be proved that the solution of the equation $ya=b$ is unique in G

§6.18. Order of an element of a group : *Definition* :

If a is of finite order; then the least positive integer n such that $a^n=e$ is called order of a. It is denoted by $O(a)$.

§6.19. Properties of the order of an element of a group :

The order of the identity of every group is 1 and it is the only element of order 1.

The order of every element of a finite group is finite and less than or equal to the order of the group *i.e.*, $O(a) \leq O(G), \quad \forall \ a \in G$

If order of an element a of a group $(G,*)$ is n, then $a^m = e$, *iff* m is a multiple of n.

For any element a of a group G : $O(a)=O(x^{-1}ax), \ \forall \ x \in G$

If the order of an element a of a group G is n, then the order of a^p is also n provided p and n are relatively prime.

§6.20. Complex of a group : *Definition :*

Any non empty sub set H of a group G is called a complex of the group G

§6.21. Subgroup : *Definition :*

A non empty subset H of a group G is called a subgroup of G if:

(i) H is stable (closed) for the composition defined in G i.e.

$$a \in H, b \in H \Rightarrow ab \in H$$

and (ii) H itself is a group for the composition induced by that of G

Proper and Improper (or Trivial) subgroup :

Every group G of order greater than 1 has atleast two subgroups which are :

(i) G (*itself*)

(ii) $\{e\}$ *i.e. the group of the identity alone.*

The above two subgroups are known as ***Improper*** or ***Trivial*** subgroups.

A subgroup other than these two is known as a ***Proper*** subgroup.

Properties of Subgroup.

a) The identity of H is the same as that of G,

b) The inverse of any elelment a of H is the same as the inverse of the same regarded as an element of G

c) The order of any element a of H is the same as the order of a in G.

d) A non void subset H of a group G is a subgroup iff

$$a \in H, b \in H \Rightarrow ab^{-1} \in H$$

e) A nonvoid finite subset H of a group G is a subgroup

iff $\quad a \in H, b \in H \Rightarrow ab \in H$

The following theorems can be easily proved :

Theorem 6.7. ***A non void subset H of a group G is a subgroup iff***

$$a \in H, b \in H \Rightarrow ab^{-1} \in H.$$

Proof : ($\Rightarrow$) : Let H be a subgroup of the group G and $b \in H$

then $b \in H \Rightarrow b^{-1} \in H$ [by existence of inverse in G]

$\therefore \quad a \in H, b \in H \Rightarrow a \in H, b^{-1} \in H$

$\Rightarrow ab^{-1} \in H$ [by closure property in H]

Therefore if H is a sub group of G, then the condition is necessary.

Conversely ($\Leftarrow$) : Suppose the given condition is true in H, then we shall prove that H will be a sub group.

$\because H \neq \phi \qquad \therefore$ Let $a \in H$

Now by the given condition,

$$a \in H, a^{-1} \in H \Rightarrow aa^{-1} = e \in H$$

Therefore identity exists in H.

Again by the same condition,

$$e \in H, a^{-1} \in H \Rightarrow ea^{-1} = a^{-1} \in H$$

Thus the inverse of every element exist in H.

Finally, $a \in H, b \in H \Rightarrow a \in H, b^{-1} \in H$

$$\Rightarrow a(b^{-1})^{-1} = ab \in H$$

H is closed for the operation of G.

Therefore H is a sub group of G which proves that the given condition is sufficient for H to be a sub group.

Remark. *If the operation of the group is addition (+), then the above condition will be :*

$$a \in H, b \in H \Rightarrow (a - b) \in H$$

Using the complex property, the above condition may also be written in the form of the following **corollary:**

A nonvoid subset H of a group G is a subgroup iff :

(a) $HH^{-1} \subset H$ **(b)** $HH^{-1} = H$

§ 6.22. Intersection of subgroups :

Theorem 6.8. ***The intersection of any two subgroups of a group G is again a subgroup of G***

[Raj. BE III (CS), 14,,17]

Proof : Let H_1 and H_2 be two sub groups of a group G.

$$\because e \in H_1, e \in H_2 \Rightarrow e \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 \neq \phi$$

Now let $a, b \in H_1 \cap H_2$, then

$$a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1 \text{ and } a, b \in H_2$$

$\Rightarrow ab^{-1} \in H_1$ and $ab^{-1} \in H_2$ [$\because H_1$ and H_2 are subgroups]

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

$\therefore \quad H_1 \cap H_2$ is a subgroup of G.

Generalisation : *If $H_1, H_2, \ldots, H_n$ be a finite family of sub groups of G; then $H_1 \cap H_2 \cap \ldots \cap H_n$ is also a subgroup of G*

Most Important Remark : ***The union of two subgroups is not necessarily a subgroup.***

Example 1. The group $G = (Z, +)$ has two subgroups

$H = \{2n : n \in Z\}$ and $K = \{3n : n \in Z\}$, then their union

$$HUK = \{\ldots -6, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\}$$

is not a subgroup of G because this is not closed for +.

Example 2. $2 \in H \cup K, 3 \in H \cup K$

but their sum $2 + 3 = 5 \notin H \cup K$

shows that $H \cup K$ is not closed for addition.

Theorem 6.9. ***The union of two subgroups is a subgroup iff one is contained in the***

[Udaipur, 15]

Proof : $(\Rightarrow)$: Let H_1 and H_2 be two subgroups of a group G.

First suppose that $H_1 \cup H_2$ is a subgroup of G, then we have to show that either $H_1 \subset H_2$ or $H_2 \subset H_1$.

Now let us suppose that $H_1 \not\subset H_2$,

then $H_1 \not\subset H_2 \Rightarrow \exists\, a \in H_1$ and $a \notin H_2$ ...(1)

Let $b \in H_2$, then

$$a \in H_1, b \in H_2 \Rightarrow a \in H_1 \cup H_2 \text{ and } b \in H_1 \cup H_2$$

$$\Rightarrow ab \in H_1 \cup H_2 \qquad [\because H_1 \cup H_2 \text{ is a subgroup}]$$

$$\Rightarrow ab \in H_1 \quad \text{or} \quad ab \in H_2$$

Now $ab \in H_2, b \in H_2 \Rightarrow (ab)b^{-1} = a \in H_2$

which contradicts our assumption (1).

Therefore $ab \notin H_2$. Hence $ab \in H_1$

But $ab \in H_1 \Rightarrow a^{-1}(ab) = b \in H_1$

$$\Rightarrow H_2 \subset H_1$$

Conversely $(\Leftarrow)$: Now suppose that $H_1 \subset H_2$ or $H_2 \subset H_1$, then

$$H_1 \cup H_2 = H_2 \text{ or } H_1$$

$\Rightarrow$ $H_1 \cup H_2$ is also a subgroup of G.

Ex. 6. ***For any group G, prove that its centre***

$$Z(G) = \{x \in G \mid xg = gx, \ \forall\, g \in G\} \text{ is a subgroup of } G$$

Sol. $\because e \in G \Rightarrow eg = ge, \quad \forall\ g \in G$

$$\Rightarrow e \in Z(G) \Rightarrow Z(G) \neq \phi$$

Therefore let $x_1, x_2 \in Z(G)$

$\therefore x_1 g = g x_1$ and $x_2 g = g x_2$, $\quad \forall\ g \in G$

Now $x_2 g = g x_2 \Rightarrow x_2^{-1}(x_2 g)x_2^{-1} = x_2^{-1}(g x_2)x_2^{-1}$

$\Rightarrow (x_2^{-1}x_2)(g x_2^{-1}) = (x_2^{-1}g)(x_2 x_2^{-1})$

$\Rightarrow e(g x_2^{-1}) = (x_2^{-1}g)e$

$\Rightarrow g x_2^{-1} = x_2^{-1} g$

$\Rightarrow x_2^{-1} \in Z(G)$

$\therefore x_2 \in Z(G) \Rightarrow x_2^{-1} \in Z(G)$

Again $(x_1 x_2^{-1})g = x_1(x_2^{-1}g)$ [by associativity]

$= x_1(g x_2^{-1})$ [$\because x_2^{-1} \in Z(G)$]

$= (x_1 g)x_2^{-1}$ [by associativity]

$= (g x_1)x_2^{-1}$ [$\because x_1 \in Z(G)$]

$= g(x_1 x_2^{-1})$ [by associativity]

$\therefore \quad x_1 x_2^{-1} \in Z(G)$

Thus we see that

$$x_1 \in Z(G), x_2 \in Z(G) \Rightarrow x_1 x_2^{-1} \in Z(G)$$

Therefore $Z(G)$ is a sub group of G. **Hence Proved.**

§ 6.23. Cyclic Group. ***Definition :***

A group G is a cyclic group if there exists an element $a \in G$ *such that* $G = [a]$

i.e. every element of G can be expressed as some integral power of a.

a is called the ***generator*** of G.

$$G = \{\ldots a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\}$$

If the operation of the group G is addition $(+)$, then

$$G = [a] = \{\ldots -3a, -2a, -a, 0, a, a, 2a, 3a, \ldots\}$$

Properties of cyclic groups :

1. Every cyclic group is abelian.
2. If a is a generator of a cyclic group G, then a^{-1} is also its generator.
3. The order of a finite cyclic group is equal to the order of its generator i.e., O (Finite cyclic group) $= O$ (generator of group)

Proof : Let $G = [a]$ be a finite cyclic group and $O(a) = n$

Let $H = \{a, a^2, a^3, \ldots, a^n = e\}$

Clearly H is a sub group of G whose order is n.

Case 1. When $m \leq n$: If $a^m \in G$, then $a^m \in H$

$\therefore H \subset G$

Case 2. $m > n$: $m = q n + r$, ...(1)

$\Rightarrow a^m = a^{qn+r}$ $0 \leq r < n, \quad q, r \in Z$

[by division algorithm]

$$=(a^n)^q \cdot a^r = ea^r$$

$$=a^r \in H$$

$$G \subset H \qquad \ldots(2)$$

$$G = H$$

$\therefore$ (1) and (2) $\Rightarrow$ $O(H) = n$

But $O(G) = n = O(a)$

$\therefore$ *Cor. A finite group of order n is cyclic iff it has an element of order n.*

Proof : ($\Rightarrow$) Let $G = [a]$ be a finite cyclic group of order n.

Then by the above theorem, an element a exists in G such that

$$O(a) = O(G) = n$$

Conversely ($\Leftarrow$) : Let G be a finite cyclic group of order n inwhich an element a such that $O(a) = n$

Now if $H = [a]$, then $H \subset G$ and by the above theorem

$$O(a) = n \Rightarrow O(H) = n$$

$$\Rightarrow O(H) = O(G)$$

Similarly G is finite group such that

$$H \subset G \text{ and } O(G) = O(H)$$

$$\Rightarrow G = H = [a]$$

$\Rightarrow$ G is a cyclic group generated by a.

Every infinite cyclic group has two and only two generators.

Every subgroup of a cyclic group is also cyclic.

If $G = [a]$ is a cyclic group of order n and $H = [a^s]$, then H is a cyclic subgroup of G is of order n/d where d is HCF of n and s .

§6.24. Coset : *Definition :*

Let H be a subgroup of a group G and $a \in G$, then the set $aH = \{ah \mid h \in H\}$ is called a left coset of H in G

*and $Ha = \{ha \mid h \in H\}$ is called a **right** coset of H in G.*

By this definition, it is clear that corresponding to every element of G, we have a left coset and a right coset of H in G.It is obvious that

$$aH \subset G, Ha \subset G, \qquad \forall \ a \in G$$

Further we may note that $eH = H = He$

i.e., the left and the right cosets of H corresponding to the identity e coincide with H.

Hence H itself is a *left as well as a right coset* of H in G.

Properties of cosets :

1. If H is a subgroup of a group G and $a \in G$ then : $a \in aH$ and $a \in Ha$

Proof : Let e be the identity element of G so also of H.

Then for every $a \in G$, $\quad e \in H \Rightarrow ae = a \in aH$

and $\quad e \in H \Rightarrow ea = a \in Ha$

Remark. From the above, it is clear that $aH \neq \phi$, $Ha \neq \phi$, $\forall\ a \in G$

2. If H is a subgroup of a group G, then G is equal to the union of all left (right) cosets of H

   i.e. $G = \bigcup aH = \bigcup Ha$

3. If H is a subgroup of a group G, then for any $a, b \in G$:

   (a) $aH \sim bH$ and $Ha \sim Hb$

   (b) $aH \sim Ha$

4. Any two left (right) cosets of a subgroup are either identical or disjoint.

Theorem 6.10. [*Lagrange's Theorem*]. *Statement :*

The order of every subgroup of a finite group is a divisor of the order of the group.

Proof : Let H be a sub group of a finite sub group G such that

$$O(G) = n \text{ and } O(H) = m.$$

We know that $G = \bigcup_{g \in G} gH.$

Since all the left cosets of H are not different, so let H have only k different cosets *viz.* $g_1H, g_2H, \ldots, g_kh$

Thus $G = g_1H \cup g_2H \cup \ldots \cup g_kH$

Since all these left cosets are pairwise disjoint, so

$$O(G) = O(g_1H) + O(g_2H) + \ldots + O(g_kH)$$

Again $O(gH) = O(H)$, $\forall\ g \in G$

$\therefore$ $O(G) = O(H) + O(H) + \ldots + O(H)$ (k times)

$\Rightarrow$ $n = m + m + m + m + m + \ldots +$ (k times)

$\Rightarrow$ $n = mk$

$\Rightarrow$ $m \mid n$

$\Rightarrow$ $O(H)$ is a divisor of $O(G)$.

§ 6.25. *Relation of congruence modulo w.r.t. a subgroup in a group: Definition :*

Let H be a sub group of a group G and $a, b \in G$, then a is said to be "congruent mod H", to b if $ab^{-1} \in H$.

It is denoted by $a \equiv b \pmod{H}$

Theorem 6.11. ***The relation of congruency in a group G, defined below, is an equivalence relation, where H is a sub group of G :***

$$a \equiv b \pmod{H} \Leftrightarrow ab^{-1} \in H$$

Proof : (*i*) **Reflexive:** Let $a \in G$, then

$$aa^{-1} = e \in H \Rightarrow a \equiv a \pmod{H}$$

$\therefore$ the relation is reflexive.

(*ii*) **Symmetric :** Let $a \equiv b \pmod{H}$. then

$$a \equiv b \pmod{H} \Rightarrow ab^{-1} \in H$$

$\Rightarrow (ab^{-1})^{-1} \in H$ [$\because$ H is a sub group]

$\Rightarrow ba^{-1} \in H$

$\Rightarrow b \equiv a \pmod{H}$.

$\therefore$ the relation is symmetric.

(iii) **Transitive :** Let $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. then

$a \equiv b \pmod{H}, b \equiv c \pmod{H} \Rightarrow ab^{-1} \in H$ and $bc^{-1} \in H$

$\Rightarrow (ab^{-1})(bc^{-1}) \in H$

$\Rightarrow a(b^{-1}b)c^{-1} \in H$

$\Rightarrow ac^{-1} \in H$

$\Rightarrow a \equiv c \pmod{H}$

Therefore the relation is transitive.

Therefore the above congruence relation defined in G is an ***equivalence relation.***

As such this partitions G into mutually disjoint equivalence classes.

We now show that corresponding to the equivalence class of any $a \in G$ i.e.,

$$C(a) = \{x \in G \mid x \equiv a \pmod{H}\}$$

same as right coset Ha, because

$x \in C(a) \Rightarrow x \equiv a \pmod{H} \Rightarrow xa^{-1} \in H$

$\Rightarrow xa^{-1}a \in Ha \Rightarrow x \in Ha$

$\therefore$ $C(a) \subset Ha$ ...(1)

and $x \in Ha \Rightarrow xa^{-1} \in Haa^{-1} = H$

$\Rightarrow x \equiv a \pmod{H} \Rightarrow x \in C(a)$

$\therefore$ $Ha \subset C(a)$ ...(2)

(1) and (2) $\Rightarrow$ $C(a) = Ha$, $\forall$ $a \in G$

Remark. Similarly it can also be proved that the relation in G defined by

$$a \equiv b \pmod{H} \Leftrightarrow a^{-1}b \in H$$

is also an equivalence relation which partitions the group G into mutually disjoint equivalence classes wrt H.

In this case the equivalence class $c(a)$ corresponding to $a \in G$ is the left coset aH corresponding to a.

Example. ***Find all the cosets of 3Z in the group*** $(Z, +)$.

Sol. Let $H = 3Z = \{\ldots, 6, -3, 0, 3, 6, \ldots\}$,

The following distinct cosets of H in G are obtained :

$0+H = H+0 = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = H$

$1+H = H+1 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$2+H = H+2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

$3+H = H+3 = \{\ldots,-3,0,3,6,9,\ldots\} = H+0$

$4+H = H+4 = \{\ldots,-2,1,4,7,10,\ldots\} = H+1$

$5+H = H+5 = \{\ldots,-1,2,5,8,11,\ldots\} = H+2$

$6+H = H+6 = \{\ldots,0,3,6,9,\ldots\} = H+0$

....

$-1+H = H+(-1) = \{\ldots,-7,-4,-1,2,5,\ldots\} = H+2$

$-2+H = H+(-2) = \{\ldots,-8,-5,-2,1,4,\ldots\} = H+1$

$-3+H = H+(-3) = \{\ldots,-9,-6,-3,0,3,\ldots\} = H+0$

....

On observing the above cosets, it is clear that

$H+0=H+3=H+6=H+9\ldots = H+(-3)=H+(-6)\ldots$

$H+1=H+4=H+7=H+10\ldots = H+(-2)=H+(-5)\ldots$

$H+2=H+5=H+8=H+11\ldots = H+(-1)=H+(-4)\ldots$

Therefore three cosets of H in G are the following :

$$H, H+1, H+2$$

Remark. : There are n cosets of nZ in $(Z,+)$.

§ 6.26. Transformation : ***Definition :***

A transformation of a set A is a ***bijection*** *from A to A i.e. itself.*

Thus a function f defined on A is a transformation of A if,

(*i*) $f : A \to A$. i.e., range of f is obtained in A

(*ii*) f is an ***injection*** i.e. a *one-one* map

and (*iii*) f is a ***surjection*** i.e. an *onto* map.

Permutation : ***Definition :***

A transformation of a ***finite*** *set S is called a permutation on S i.e. a permutation is a bijection on a finite set S.*

Product or Composite of permutations :

If f and g be the two permutations of any set A, then by the product of two permutations fg we mean to find their composite function

$f \circ g$. Therefore for any $x \in A$

$$fg(x) = (fog)(x) = f[g(x)]$$

Illustrative Examples

Ex. 1. ***If*** $\sigma = \begin{pmatrix} 1 & 7 & 2 & 6 & 3 & 5 & 8 & 4 \end{pmatrix}$

and $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 8 & 7 & 6 & 1 \end{pmatrix}$,

then prove that :

$$\rho\sigma\rho^{-1} = (\rho(1)\rho(7)\rho(2)\rho(6)\rho(3)\rho(5)\rho(8)\rho(4))$$

Sol. $\because$ $\sigma = (1\ 7\ 2\ 6\ 3\ 5\ 8\ 4)$

$$=\begin{pmatrix}1&7&2&6&3&5&8&4\\7&2&6&3&5&8&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8\\7&6&5&1&8&3&2&4\end{pmatrix}$$

$$\therefore\quad \rho\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&5&4&3&8&7&6&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\7&6&5&1&8&3&2&4\end{pmatrix}$$

$$=\begin{pmatrix}7&6&5&1&8&3&2&4\\6&7&8&2&1&4&5&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\7&6&5&1&8&3&2&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\6&7&8&2&1&4&5&3\end{pmatrix}\qquad\ldots(1)$$

Again $\rho^{-1}=\begin{pmatrix}2&5&4&3&8&7&6&1\\1&2&3&4&5&6&7&8\end{pmatrix}$

$$\therefore\quad \rho\sigma\rho^{-1}=(\rho\sigma)\rho^{-1}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\6&7&8&2&1&4&5&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&3&2&7&6&5\end{pmatrix}$$

$$=\begin{pmatrix}8&1&4&3&2&7&6&5\\3&6&2&8&7&5&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&3&2&7&6&5\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&2&8&7&5&4&1\end{pmatrix}=(1\ 3\ 2\ 6\ 5\ 7\ 4\ 8)$$

$$=(2\ 6\ 5\ 7\ 4\ 8\ 1\ 3)$$

$$=(r(1)\,r(7)\,r(2)\,r(6)\,r(3)\,r(5)\,r(8)\,r(4)).$$

Ex. 2. *If* $\rho=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&8&9&6&4&5&2&3&1\end{pmatrix}$, $\sigma=(1\ 3\ 4)(5\ 6)(2\ 7\ 8\ 9)$

find $\sigma^{-1}\rho\sigma$ ***and by expressing the permutation*** ρ ***as the product of disjoint cycles, fi***
ther ρ ***is an even permutation or odd permutation. Also find its order.***

Sol. $\sigma=(1\ 3\ 4)(5\ 6)(2\ 7\ 8\ 9)$

$$=\begin{pmatrix}1&3&4&5&6&2&7&8&9\\3&4&1&6&5&7&8&9&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&7&4&1&6&5&8&9&2\end{pmatrix}$$

$$\therefore\quad \sigma^{-1}=\begin{pmatrix}3&7&4&1&6&5&8&9&2\\1&2&3&4&5&6&7&8&9\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&9&1&3&6&5&2&7&8\end{pmatrix}\qquad\ldots(2)$$

Again $\rho\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&8&9&6&4&5&2&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&7&4&1&6&5&8&9&2\end{pmatrix}$

$$=\begin{pmatrix}3&7&4&1&6&5&8&9&2\\9&2&6&7&5&4&3&1&8\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&7&4&1&6&5&8&9&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&2&6&7&5&4&3&1&8\end{pmatrix}$$

$\therefore \quad \sigma^{-1}\rho\sigma=\sigma^{-1}(\rho\sigma)$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&9&1&3&6&5&2&7&8\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&2&6&7&5&4&3&1&8\end{pmatrix}$$

$$=\begin{pmatrix}9&2&6&7&5&4&3&1&8\\8&9&5&2&6&3&1&4&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&2&6&7&5&4&3&1&8\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\8&9&5&2&6&3&1&4&7\end{pmatrix}$$

$$=(1\,8\,4\,2\,9\,7)(3\,5\,6)$$

Again $\rho=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&8&9&6&4&5&2&3&1\end{pmatrix}$

$$=(1\,7\,2\,8\,3\,9)(4\,6\,5)$$

$$=(1\,9)(1\,3)(1\,8)(1\,2)(1\,7)(4\,5)(4\,6)$$

= product of 7 (odd) transpositions.

Since ρ is equal to the product of odd transpositions, therefore this is a odd permutation.

Finally, $O(p)$=LCM of $\{O(1\,7\,2\,8\,3\,9), O(4\,6\,5)\}$

=LCM of $\{6, 3\}$

$=6$

§ 6.27. Group of Permutations :

The set of all the permutations of a given non empty set A is denoted by S_A. Therefore if $A=\{a,b\}$, then

$$S_A=\left\{\begin{pmatrix}a&b\\a&b\end{pmatrix},\begin{pmatrix}a&b\\b&a\end{pmatrix}\right\}$$

If $A=\{a,b,c\}$, then

$$S_A=\left\{\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix},\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix},\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix},\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix},\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}\right\}$$

It can be easily seen that

$$O(A)=n \quad \Rightarrow \quad O(S_A)=n!$$

In the following theorem we prove that S_A is a group for the product of permutations.

Theorem 6.12. ***The set S_A of all permutations of a non void set A is a group for the product of permutations.***

Proof : Since the composition of two bijections is also a bijection, so the product of any two permutations of a set will always be a permutation of that set.

$\therefore f\in S_A, g\in S_A \Rightarrow fg\in S_A$

i.e., S_A is ***closed*** for the product of permutations.

Verification of Group axioms in S_A:

[G_1] Since the composite of functions is ***associative***, therefore for any $f,g,h\in S_A$.

$(f\,g)h=(fog)oh$
$=f\,o(goh)=f\,(gh)$

Therefore the productof permutations is ***associative.***

] The identity permutation $I_A \in S_A$ is the ***identity*** for the composition because for every $f \in S_A$

$$(I_A f)(x)=I_A[f(x)]=f(x)$$

and
$$(f I_A)(x)=f[I_A(x)]=f(x)$$

] Let $f \in S_A$, then

$$f \in S_A \Rightarrow f:A\to A \text{ is bijection}$$
$$\Rightarrow f^{-1}:A\to A \text{ is also bijection} \Rightarrow f^{-1}\in S_A$$

which is the ***inverse*** of f because $f f^{-1}=I_A=f^{-1} f$

Therefore the inverse of every permutation exist in S_A.

From the above discussion, it is proved that S_A is a group for the product of mutations.

Permutation Group. *Definition* :

The set of all permutations S_A of a non void set A is a group for the product of mutations which is called the permutation group of A.

Remark: If A is a finite set of cardinal n *i.e.* consisting of n distinct elements, then S_A is a group of order $n!$ and in that case it is generally denoted by P_A.

Note . S_A is a non commutative group because the composition of functions is not ommutative.

Cyclic Permutation :

A permutation σ of a set A is a cyclic permutation or a cycle if there exists a finite ubset $\{a_1, a_2, \ldots, a_r\}$ *of A such that :*

$$\sigma(a_1)=a_2, \sigma(a_2)=a_3 \ldots, \sigma(a_r)=a_1$$

Therefore $\sigma(x)=x$, if $x \in A$. But $x \notin \{a_1, a_2, \ldots, a_r\}$

If σ is such a permutation, then we denote it by

$$\sigma=(a_1 \quad a_2 \quad a_3 \ldots \quad a_r)$$

in which σ -image of every element is its next element and the σ -image of the last element is the first element.

Again the number of elements in this row notation is called the **length of the cycle** σ.

Even and odd permutations : ***Definition :***

A permutation σ is called an even (odd), if the total number of inversions for it, when expressed as product, it is an even (odd) number.

The set A_n of all even permutations of degree n is called ***Alternating group*** for the product of permutations.

$$O(A_n)=\frac{1}{2}n!$$

§ 6.28. Symmetric group : ***Definition :***

The group of permutation of set $\{1, 2, \ldots\ldots, n\}$ is called the symmetric group of degree n.

From this definition we may observe that

$$H \lhd G \Leftrightarrow xHx^{-1} \subseteq H, \ \forall\ x \in G \qquad \text{[another definition]}$$

Example: $H=\{1,-1\},\times]$ is a normal subgroup of $G=\{1,-1,i,-i\},\times]$ because for every $x \in G$ and $h \in H$

$$xhx^{-1} = xx^{-1}h = eh = h \in H \qquad [\because G \text{ is commutative}]$$

Remarks: The normal subgroup is also called a *special subgroup* or ***invarient subgroup*** or ***self conjugate subgroup.***

Proper and Improper Normal subgroups :

It can be observed that every group G has atleast following two normal subgroups:

(*i*) G itself

and (*ii*) {e}, the group consisting of the identity alone.

These two subgroups are called **Improper normal subgroups** of G and a normal subgroup other than these two is called a **Proper normal subgroup.**

Simple Groups : ***Definition :***

A group which has no proper normal subgroups is called a simple group

Example : Every group of prime order is simple because such a group has no proper subgroup.

Hamiltonian Group : ***Definition :***

If all the subgroups of a non Abelian group are normal, then it is called Hamiltonian group.

The existence of Normal Subgroups :

Every subgroup of a group with index 2 is a normal subgroup.

Some properties of Normal subgroups :

The following property can be easily proved as in case of subgroups.

1. Every subgroup of an abelian group is a normal subgroup.
2. A subgroup H of a group G is a normal subgroup iff:

$$H \lhd G \Leftrightarrow xHx^{-1} = H, \qquad \forall\ x \in G.$$

3. A subgroup H of a group G is a normal subgroup iff each left coset of H is right coset of H (and hence also iff each right coset of H is a left coset of H) *i.e.*

$$H \lhd G \Leftrightarrow xH = Hx, \qquad \forall\ x \in G$$

4. A subgroup H of a group G, is a normal subgroup of G iff the product of two right (left) cosets of H in G is again a right (left) coset of H in G.

Theorem 6.13. ***Every subgroup of an abelian group is a normal subgroup.***

Proof : Let H be a subgroup of any commutative group G:

If $x \in G$ and $h \in H$, then

$$xhx^{-1} = (hx)x^{-1}$$

$$= h(xx^{-1}) \qquad [\because G \text{ is commutative}]$$

$$= he = h \in H \qquad [\text{by associativity}]$$

Thus, $x \in G, h \in H \Rightarrow xhx^{-1} \in H,$

$\therefore$ H is a normal subgroup of G.

Cor. Every subgroup of a cyclic group is a normal subgroup.

Theorem 6.14. *A subgroup H of a group G is a normal subgroup iff :*

$$H \lhd G \Leftrightarrow xHx^{-1} = H, \quad \forall \ x \in G.$$

Proof : ($\Rightarrow$) Let $H \lhd G$, then

$$x \in G, h \in H \Rightarrow xhx^{-1} \in H$$

$$\Rightarrow xHx^{-1} \subset H \qquad \ldots(1)$$

Again $\forall\ x \in G, xHx^{-1} \subset H \Rightarrow x^{-1}H(x^{-1})^{-1} \subset H \qquad [\because x^{-1} \in G]$

$$\Rightarrow x^{-1}Hx \subset H$$

$$\Rightarrow x(x^{-1}Hx)x^{-1} \subset xHx^{-1}$$

$$\Rightarrow (xx^{-1})H(xx^{-1}) \subset xHx^{-1}$$

$$\Rightarrow H \subset xHx^{-1} \qquad \ldots(2)$$

(1) and (2) $\Rightarrow xHx^{-1} = H.$

$$H \lhd G \Rightarrow xHx^{-1} = H, \quad \forall \ x \in G.$$

Conversely : ($\Leftarrow$) Let $xHx^{-1} = H, \ \forall \ x \in G$ ∴

$$xHx^{-1} = H \Rightarrow xHx^{-1} \subset H$$

then

$$\Rightarrow xhx^{-1} \in H, \ \forall \ h \in H, x \in G.$$

$$H \lhd G$$

Hence $H \lhd G \Leftrightarrow xHx^{-1} = H, \ \forall \ x \in G.$

Theorems on Normal subgroups :

Proceed as in case of subgroup the following theorems can also be easily proved.

Theorem 6.15. ***The intersection of any two normal subgroups of a group is a normal subgroup.***

Proof : Let H_1 and H_2 be two normal subgroups of a group G.

Earlier we have seen that the intersection of two subgroups of a group G is again a group, so $H_1 \cap H_2$ is also a subgroup of G.

Now if $x \in G$ and $h \in H_1 \cap H_2$,

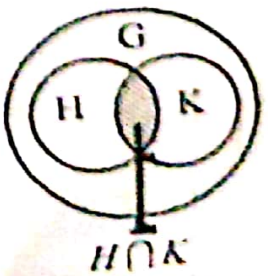
then $h \in H_1 \cap H_2 \Rightarrow h \in H_1$ and $h \in H_2$

Now, since $H_1 \lhd G$

$$\therefore \quad x \in G, h \in H_1 \Rightarrow xhx^{-1} \in H_1.$$

Similarly $H_2 \lhd G$

$$\therefore x \in G, h \in H_2 \Rightarrow xhx^{-1} \in H_2.$$



Thus we see that

$$x \in G, h \in H_1 \cap H_2 \Rightarrow xhx^{-1} \in H_1 \text{ and } xhx^{-1} \in H_2$$

$$\Rightarrow xhx^{-1} \in H_1 \cap H_2$$

$$\therefore \quad H_1 \cap H_2 \lhd G$$

Cor. *The intersection of any finite family of normal subgroups is a normal subgroup.*

Theorem 6.16. ***If H is a subgroup of G and*** $N \triangleleft G$, ***then*** $H \cap N \triangleleft H$.

Proof : Since intersection of two subgroups is also a subgroup,

so $H \cap N$ is also a subgroup of G.

Also $H \cap N \subset H$, therefore $H \cap N$ is also a subgroup of H.

Let $h \in H \cap N$ and $x \in H$,

then $h \in H \cap N \Rightarrow h \in H$ and $h \in N$

Again $h \in H, x \in H \Rightarrow xhx^{-1} \in H$ [$\because H$ is a subgroup]

and $h \in N, x \in H \Rightarrow h \in N, x \in G.$ [$\because H \subset G$]

$\Rightarrow xhx^{-1} \in N.$ [$\because N$ is normal]

Therefore $xhx^{-1} \in H, xhx^{-1} \in N \Rightarrow xhx^{-1} \in H \cap N.$

Thus we see that

$$h \in H \cap N, x \in H \Rightarrow xhx^{-1} \in H \cap N.$$

$$\therefore \quad H \cap N \triangleleft H$$

Theorem 6.17. If H and K are two normal subgroups of a group G, then $HK \triangleleft G$.

§ 6.32. Quotient group : *Definition* :

Let G be a group and $H \triangleleft G$, *then the set G/H of all cosets of H in G together with the binary composition defined by* $HaHb = Hab$ *,where* $Ha \in G/H, Hb \in G/H$ *is a group, and is called the quotient group of G by H.*

Remarks :

1. For the ***existence of the quotient group*** G/H, it is necessary that H is a normal subsgroup of G.
2. The addition $(+)$ composition in G/H is defined as

$$(H+a)+(H+b)=H+(a+b).$$

Order of the Quotient group : *If G is a finite group and* $N \triangleleft G$, *then*

$$O\left(\frac{G}{N}\right) = \frac{O(G)}{O(N)}$$

Properties of Quotient group :

1. Every quotient group of an abelian group is abelian but not conversely.
2. Every quotient group of a cyclic group is cyclic but not conversely.

Illustrative Examples

Ex.1. ***Find the quotient group G/H and also prepare its operation table when :***

$$G=[\{1,-1,i,-i\},\times], H=[\{1,-1\},\times]$$

Sol. Since G is a commutative group, therefore $H \triangleleft G$.

Consequently, G/H exist having the following cosets of H:

$$H.1 = \{1.1,-1.1\}=\{1,-1\} = H$$

$$H(-1) = \{1.(-1),-1.(-1)\}=\{-1,1\} = H.$$

$$H.i. = \{1.i,-1.i\}=\{i,-i\} = Hi$$

$H(-i) = \{1.(-i), -1(-i)\} = \{-i, i\} = Hi$

Thus we see that $G/H = \{H, Hi\}$

The composition table of G/H is as follows :

	H	Hi
H	H	Hi
Hi	Hi	H

Ex. 2. Find the quotient group G/H and also prepare its operation table wh

$$G=(Z,+), H=(4Z,+).$$

Sol. Since $(Z,+)$ is a commutative group, therefore $(4Z,+) \lhd Z$

Hence G/H exists.

The cosets of H in G are as follows :

$$0+H = H+0=\{\ldots,-8,-4,0,4,8,\ldots\} = H$$
$$1+H = H+1=\{\ldots,-7,-3,1,5,9,\ldots\}$$
$$2+H = H+2=\{\ldots,-6,-2,2,6,10,\ldots\}$$
$$3+H = H+3=\{\ldots,-5,-1,3,7,11,\ldots\}$$

We further observe that

$$H = H+4 = H+8 = H+12 = \ldots = H+(-4) = H+(-8) = \cdots$$
$$H+1 = H+5 = H+9 = H+13 = \ldots = H+(-3) = H+(-7) = \cdots$$
$$H+2 = H+6 = H+10 = H+14 = \ldots = H+(-2) = H+(-6) = \cdots$$
$$H+3 = H+7 = H+11 = H+15 = \ldots = H+(-1) = H+(-5) = \cdots$$

Thus H has four distinct cosets and so

$$G/H = \{H, H+1, H+2, H+3\}$$

The composition table of G/H is as shown below :

+	H	$H+1$	$H+2$	$H+3$
H	H	$H+1$	$H+2$	$H+3$
$H+1$	$H+1$	$H+2$	$H+3$	H
$H+2$	$H+2$	$H+3$	H	$H+1$
$H+3$	$H+3$	H	$H+1$	$H+2$

§6.33. Homomorphism. ***Definition :***

A mapping f from a group $(G,*)$ to a group (G',o) is called

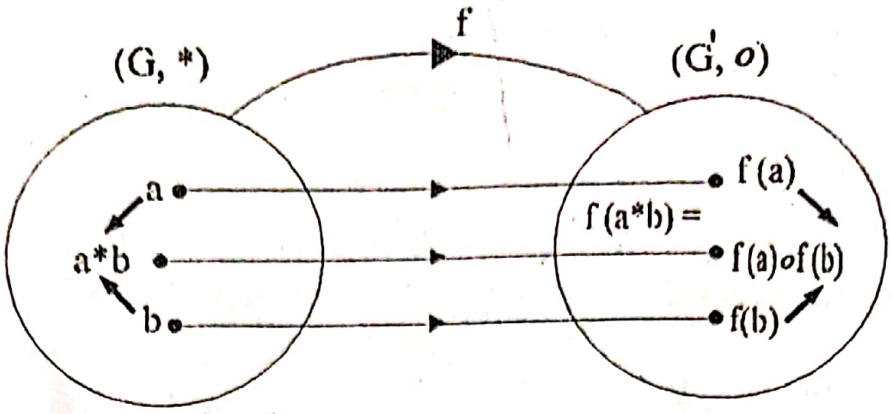
homomorphism (or group morphism) from G to G' if

$$f(a*b) = f(a) o f(b), \quad \forall\ a,b \in G.$$

Thus, if f is a morphism from G to G', then it preserves the composition in both t

G and G' *i.e.*,

Image of the composite = Composite of images



Example. Let $(R,+)$ be the additive group of real numbers and $(R_0,\times)$ be the multiplicative group of non zero real numbers.

The mapping $f:(R,+)\to(R_0,\times); f(x)=2^x, \quad \forall\ x\in R$

is a homomorphism of R into R_0 because for any $x_1,x_2\in R$

$$f(x_1+x_2)=2^{x_1+x_2}=2^{x_1}.2^{x_2}=f(x_1)f(x_2)$$

§ 6.34. Various Morphisms :

A morphism f of a group G into G' is called

(*i*) Monomorphism, *if f is injection (one one).*

(*ii*) Epimorphism, *if f is surjection (onto).*

Here G' is called the *homomorphic image* of the group G.

(*iii*) Isomorphism, *if f is bijection (one one onto).*

(*iv*) Endomorphism, if $G'=G$ *i.e. f is a homomorphism from G to itself.*

(*v*) Automorphism, *if $G'=G$ and f is bijection.*

Theorem 6.16. ***If f is a homomorphism from a group G to G' and if e and e' be their respective identities, then :***

(a) $f(e)=e'$ **[Raj. BE III (CS), 04]**

(b) $f(a^{-1})=[f(a)]^{-1}, \quad \forall\ a\in G$ **[Raj. BE III (CS), 04]**

Proof (a) : Let $a\in G$, then $ae=a=ea$

$\Rightarrow f(ae)=f(a)=f(ea)$

$\Rightarrow f(a)f(e)=f(a)=f(e)f(a)$ [$\because$ f is homomorphism]

$\Rightarrow f(e)$ is the identity in $G' \Rightarrow f(e)=e'$

Therefore the image of the identity of G under the group morphism f is the identity of G'

(b) Let a^{-1} be the inverse of $a\in G$, then

$aa^{-1}=e=a^{-1}a \Rightarrow f(aa^{-1})=f(e)=f(a^{-1}a)$

$\Rightarrow f(a)f(a^{-1})=e'=f(a^{-1})f(a) \Rightarrow f(a^{-1})=[f(a)]^{-1}$

therefore, the f-image of the inverse of any element of G under f is the inverse of the f-image of a in G'.

Theorem 6.17. *If f is a homomorphism of a group G to a group G',*

(a) H is a subgroup of $G \Rightarrow f(H)$ is a subgroup of G'.

(b) H' is a subgroup of $G' \Rightarrow f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ is a subgroup of G

Proof : (a) Clearly $f(H) \subset G'$ and $f(H) \neq \phi$, because

$e \in H \Rightarrow f(e) = e' \in f(H)$ where e' is identity in G'

If $a', b' \in f(H)$, then

$a', b' \in f(H) \Rightarrow$ there exist a, b in H such that

$$f(a) = a' \text{ and } f(b) = b'$$

$$\Rightarrow a'(b')^{-1} = f(a)[f(b)]^{-1}$$

$$= f(a) f\left(b^{-1}\right) \qquad [\because [f(b)]^{-1} = f\left(b^{-1}\right)]$$

$$= f\left(ab^{-1}\right) \qquad [\because f \text{ is homomorphism}]$$

But $a \in H, b \in H \Rightarrow ab^{-1} \in H$

$$\Rightarrow f(ab^{-1}) \in f(H)$$

Thus $a', b' \in f(H) \Rightarrow f\left(ab^{-1}\right) = a'(b')^{-1} \in f(H)$

$\therefore f(H)$ is a sub group of G'

(b) Obviously $f^{-1}(H') \subset G$

and $f^{-1}(H') \neq \phi$ because atleast $e \in f^{-1}(H')$

If $a, b \in f^{-1}(H')$, then

$a, b \in f^{-1}(H') \Rightarrow f(a) \in H'$ and $f(b) \in H'$

$$\Rightarrow f(a)[f(b)]^{-1} \in H' \qquad [\because H \text{ is a subgroup}]$$

$$\Rightarrow f(a) f\left(b^{-1}\right) \in H'$$

$$\Rightarrow f\left(ab^{-1}\right) \in H' \qquad [\because f \text{ is homomorphism}]$$

$$\Rightarrow ab^{-1} \in f^{-1}(H')$$

Thus $a, b \in f^{-1}(H') \Rightarrow ab^{-1} \in f^{-1}(H')$

$\therefore f^{-1}(H')$ is a subgroup of G

Cor. ***If f is a homomorphism from a group G to G', then $f(G)$ is a subgroup of G'.***
This can be easily proved by taking $H = G$ in part (a) of the above theorem.

§6.35. Kernel of Homomorphism : ***Definition :***

Let f be a homomorphism of a group G into G', then the set K of all those elements of G which are mapped to the identity e' of G' is called the kernel of the homomorphism f.

It is denoted by Ker f or Ker (f)

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}$$

§6.36. Isomorphism : *Definition :*

A morphism f of a group $(G,*)$ to a group (G', o) is an isomorphism if

(*i*) f is *one-one* i.e., $f(a)=f(b) \Rightarrow a=b, \quad \forall\ a,b \in G$

(*ii*) f is *onto* i.e., $f(G)=G'$

and (*iii*) f is a *morphism* i.e, $f(a*b)=f(a)\,o\,f(b), \quad \forall\ a,b \in G$

From the above definition, it is clear that a group morphism is an isomorphism if f is a *bijection.*

Isomorphic Groups : *Definition :*

A group G is said to be isomorphic to a group G', if there exists an isomorphism of G onto G'.

Symbolically, we write it as $G \cong G'$.

Example. The map $f:(Z,+)\to(2Z,+), f(x)=2x, \forall\ x \in Z,$

is an isomorphism from Z onto $2Z$, because for any $x_1, x_2 \in Z$

(*i*) $f(x_1+x_2)=2(x_1+x_2)=2x_1+2x_2=f(x_1)+f(x_2)$

$\therefore f$ is a group ***morphism.***

(*ii*) $f(x_1)=f(x_2) \Rightarrow 2x_1=2x_2 \Rightarrow x_1=x_2$

$\therefore f$ is ***one-one.***

(*iii*) $f(Z)=2Z$, $\therefore f$ is ***onto.***

Hence $Z \cong 2Z.$

Algebraic Structures with two Binary Compositions

§ 6.45. Now here we propose to introduce and study another algebraic structure equipped with *TWO binary compositions*. The simplest algebraic structure with two binary compositions is *Ring* which has a great contribution in *Discrete Mathematics* and many other branches of mathematics.

The study of the following *special type of Rings* is also very useful:

1. Integral Domain
2. Division Ring
3. Field
4. Ideal etc.

§ 6.46. Ring. ***Definition :***

[Raj. B.Sc., 17; Hons. 16; Ajmer B.Sc. 15, Udaipur 17; Jodhpur, 16]

The structure $(R, +, \times)$ *consisting of a non void set* R *and two binary compositions, denoted by* $+$ *and* $\times$ *or* $\cdot$ *is said to be a ring, if the following axioms are satisfied :*

$[R_1]$ $(R, +)$ ***is an abelian group.***

$[R_2]$ $(R, \times \text{ or } \cdot)$ ***is a semi-group.***

$[R_3]$ $\forall\ a, b, c \in R$

$$a \times (b+c) = a \times b + a \times c \qquad \text{[Left distributive law]}$$

and $$(a+b) \times c = a \times c + b \times c \qquad \text{[Right distributive law]}$$

Thus we see that the ring $(R, +, \times)$ satisfies the following properties:

$$\forall\ a, b, c \in R,$$

R_{11}. $(a+b)+c = a+(b+c)$, [Associativity]

R_{12}. There exists an element 0 in R called *additive identity*

such that $a+0 = a = 0+a$

R_{13}. For every a in R there exists $-a$ in R called *additive inverse*

such that $a+(-a) = 0 = -a+a$

R_{14}. $a+b = b+a$, (commutativity for $+$)

R_{21}. $(a \times b) \times c = a \times (b \times c)$, (associativity for $\times$)

R_{31}. $a \times (b+c) = a \times b + a \times c$, (Left distributive law)

R_{32}. $(a+b) \times c = a \times c + b \times c$ (Right distributive law)

denoted by a^{-1} or $\frac{1}{a}$.

§ 6.47. Types of Rings :

[Raj. B.Sc., 16]

1. Ring with unity : ***Definition :***

A ring $(R, +, \times)$ is said to be a ring with unity if its multiplicative identity exists i.e. if $\exists$ $e \in R$ such that :

$[R_{22}]$ $\qquad ea = a = ae, \quad \forall \quad a \in R$

[Udaipur B.Sc., 14]

2. Commutative ring . ***Definition :***

A ring $(R, +, \times)$ is said to be a commutative ring if its multiplicative composition is also commutative i.e. if :

$[R_{23}]$ $\qquad a \times b = b \times a, \quad \forall \quad a, b \in R$

Examples of Rings :

Ex. 1. The set R consisting of a single element 0 with two compositions (+) and ($\times$) defined as $0 + 0 = 0$ and $0 \times 0 = 0$

is a ring called the ***Zero ring*** or ***Null ring or Trivial Ring.***

Ex. 2. The set of integers Z for addition and multiplication of integers $(Z, +, \times)$ is a ring. It is a commutative ring with unity because multiplication of integers is commutative and 1 is the unity element in Z.

Similarly the following structures of numbers are commutative rings:

$$(Q, +, \times), (R, +, \times), (C, +, \times), (mZ, +, \times)$$

Ex. 3. The set $R = \{a, b\}$ with addition (+) and multiplication ($\times$) defined by the following table :

+	a	b
a	a	b
b	b	a

$\times$	a	b
a	a	a
b	a	b

is a commutative ring with unity , a is its zero element and b is its unit element.

Theorem 4.25. *A ring R is without zero divisors iff the cancellation law holds in R.*

§ 6.52. INTEGRAL DOMAIN: *Definition :*

[Ajmer B.Sc., 16, Raj. B.Sc. 15; (Hons.) 17]

A ring D is said to be an Integral Domain, if it is a commutative ring with unity and without zero divisors i.e. a ring R is :

(*i*) commutative $[R_{23}]$

(*ii*) with unity $[R_{22}]$

(*iii*) without zero divisors.

Remark. In an integral domain, atleast two elements are required, because there must be *atleast one non zero element.*

Thus a set $(D, +, \times)$ is called an integral domain if it satisfies the following axioms for the two defined binary compositions '+' and '$\times$':

$[ID_1]$. $(D,+)$ ***is an abelian group i.e.,*** $(\forall\ a, b, c \in D)$

$[I_{11}]$ $a+(b+c)=(a+b)+c$ [Associativity]

$[I_{12}]$ $\exists\, 0 \in D$ *s.t.* $a+0=a$, [Additive Identity]

$[I_{13}]$ $\forall\ a \in D,\ a+(-a)=(-a)+a=0$ [Additive Inverse]

$[I_{14}]$ $a+b=b+a$ [Commutativity]

$[ID_2]$. $(D, \times)$ ***is semi abelian group with unity i.e.,***

$[I_{21}]$ $a \times (b \times c) = (a \times b) \times c$

$[I_{22}]$ $\exists\, 1 \in D$ *s.t.* $a \times 1 = 1 \times a = a$,

I_{23} $a \times b = b \times a$

$[ID_3]$. **Distributivity :**

I_{31} $a \times (b + c) = a \times b + a \times c$ [Left]

I_{32} $(b + c) \times a = b \times a + c \times a$ [Right]

§6.53. FIELD. *Definition* :

[Raj. B.Sc., 15; Ajmer B.Sc. 13, (Hons.) 14; Jodhpur B.Sc., 17; Udaipur B.Sc., 16]

A ring F is called a field, if it is :

$[F_1]$ *Commutative*

$[F_2]$ *with unity*

and $[F_3]$ *its every non zero element is invertible*

i.e. has multiplicative inverse.

Thus a structure $(F, +, \times)$ containing atleast two elements is a field if it satisfies the following axioms :

$[F_1]$. $(F, +)$ ***is an abelian group i.e.,*** $\forall \ a, b, c \in F$,

$[F_{11}]$ $(a + b) + c = a + (b + c)$,

$[F_{12}]$ $\exists\, 0 \in F$ *s.t.* $a + 0 = a$, $\qquad a + 0 = a$,

$[F_{13}]$ $\forall \ a \in F, \exists -a \in F$ *s.t.* $\qquad a + (-a) = (-a) + a = 0$

$[F_{14}]$ $a + b = b + a$

$[F_2]$. $(F_0, \times)$ ***is an abelian group***

(F_0, F is the set of allnon zero elements of F)

$[F_{21}]$ $(a \times b) \times c = a \times (b \times c)$

$[F_{22}]$ $\exists\, 1\ (\neq 0) \in F$ *s.t.* $a \times 1 = a$, $\qquad a \times 1 = a$,

$[F_{23}]$ $\forall \ a\ (\neq 0) \in F \ \exists\, a^{-1} \in F$ *s.t.* $\qquad a \times a^{-1} = 1$ (Unity)

$[F_{24}]$ $a \times b = b \times a$

$[F_3]$. **Distributivity :**

$[F_{31}]$ $a \times (b + c) = a \times b + a \times c$ [Left]

$[F_{32}]$ $(a + b) \times c = a \times c + b \times c$ [Right]

Remark. It may be observed that in a field $(F, +, \times)$, each equation of the form

$$a + x = b, x + a = b, ax = b (a \neq 0) \text{ or } xa = b (a \neq 0).$$

has a unique solution in F for all a, b in F.

Example 1. The following rings of numbers

$$(Q, +, \times), (R, +, \times), (C, +, \times).$$

are field because each is a commutative ring with unity and multiplicative inverse $1/a$ of every nonzero element a of ring exists.

nonzero elements in a ring with unity : *Definition:* *than any*