UNIT - I

Group :-

Def :

A non-empty set G together with a binary operation $* : G \times G \to G$ is called a group if the following conditions are satisfied

(i) $*$ is associative (i.e) $a*(b*c) = (a*b)*c$ for all $a, b, c \in G$

(ii) There exists an element $e \in G$ such that $a*e = e*a = a$ for all $a \in G$

e is called the identity element of G.

(iii) For any element a in G there exists an element $a' \in G$ such that $a*a' = a'*a = e$

a' is called the inverse of a.

Examples :-

1. The set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$ is a group under matrix addition.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity element and

$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Scanned by CamScanner

2. The set of 2×2 non-singular matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$ is a group under matrix multiplication.

We know that matrix multiplication is associative $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element.

The inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{|A|}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

where $|A| = ad - bc \neq 0$ (i)

$A^{-1} = \frac{1}{|A|}\,adj\,A$

$|A| \neq 0$ (ii)

A is non singular.

---

3. N is not a group under usual addition since there is no element $e \in N$ such that $x + e = x$.

$N = \{1, 2, 3, \ldots\}$

N is not a group.

---

4. The set E of all even integers under usual addition is a group. For $a, b \in E \Rightarrow a + b \in E$

Therefore usual addition is a binary operation in E

$0 \in E$ is the identity element

---

5. Q^* and R^* under usual multiplication are groups. 1 is the identity element and the inverse of a is $1/a$

Scanned by CamScanner

Q^* is a non zero Rational number.

R^* is a non zero Real number.

---

6. Q^+ is a group under usual multiplication. for $a, b \in Q^+ \Rightarrow ab \in Q^+$. therefore usual multiplication is a binary operation in Q^+

$1 \in Q^+$ is the identity element

If $a \in Q^+$, $(1/a) \in Q^+$ is the inverse of a

---

7. Z(integer) under the usual multiplication is not a groups. $1 \in Z$ is the identity element. However any element other than 1 and -1 does not have an inverse $Z = \{0, \pm 1, \pm 2 - - - - \}$

---

8. Let $G_1 = \{1, -1\}$. G_1 is a group under usual multiplication. 1 is the identity element. The inverse of each element is itself. The Layley table for the group is

*	1	-1
1	1	-1
-1	-1	1

Scanned by CamScanner

9. Let $G = \{1, i, -1, -i\}$. G is a group under usual multiplication. The identity element is 1. The inverse of $1, i, -1$ and $-i$ are $1, -i, -1$ and i respectively. The cayley table for this group is given by

$*$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

10. Let $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

G is a group under matrix multiplication (construct the cayley table for this group)

Scanned by CamScanner

11. C^* is a group under usual multiplication given by $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$

Proof :-

Let $x, y \in C^*$. Then $x = a+ib$ where, a and b are not simultaneously zero and any $y = c+id$ where c and d are not simultaneously zero.

Now,

$$xy = (a+ib)(c+id)$$
$$= (ac-bd) + i(ad+bc)$$

we shall first prove that $ac-bd$ and $ad+bc$ are not simultaneously zero

Suppose, $ac-bd = 0 \longrightarrow (1)$

and, $ad+bc = 0 \longrightarrow (2)$

multiplying (1) by d and (2) by c and subtracting

$(1) \times \Rightarrow ac - bd = 0$

$(2) \times \Rightarrow ad + bc = 0$

$$adc - bd^2 = 0$$
$$adc + bc^2 = 0$$
$$-bd^2 - bc^2 = -0$$
$$-(bd^2 + bc^2) = -0$$
$$\therefore b(d^2+c^2) = 0$$

Scanned by CamScanner

Either, $b=0$ (or) $d^2+c^2=0$

$b=0$ (or) ($d=0$ and $c=0$)

Similarly

③ $\times \Rightarrow ac^2 - bcd = 0$

④ $\times \Rightarrow ad^2 + bcd = 0$

$ac^2 + ad^2 = 0$

$a(c^2+d^2) = 0$

Either, $a=0$ (or) $c^2+d^2=0$

$a=0$ (or) ($c=0$ and $d=0$)

Thus ($a=0$ and $b=0$) (or) ($c=0$ and $d=0$)

$\therefore x=0$ (or) $y=0$ which is a contradiction

Hence $xy \in C^*$

Now, let $x = a+ib$, $y = c+id$ $z = e+if$

Then, $x(yz)$

$= (a+ib)[(c+id)(e+if)]$

$= (a+ib)[(ce-df) + i(cf+de)]$

$= (ace - adf - bde - bcf) + i(bce - bdf + acf + ade)$

Similarly

$(xy)z = [(a+ib)(c+id)](e+if)$

Scanned by CamScanner

$$= [(ac-bd)+i(ad+bc)](e+if)$$

$$= (ace - bde - fad - bcf) + i(ade + bce + acf - bdf)$$

Hence, $x(yz) = (xy)z$

$1+i0$ is the identity element

Also, $\frac{1}{x} = \frac{1}{a+ib} \times \frac{a-ib}{a-ib}$

$$= \frac{a-ib}{(a+ib)(a-ib)}$$

$$= \frac{a-ib}{a^2+b^2}$$

$$= \left(\frac{a}{a^2+b^2}\right) - i\left(\frac{b}{a^2+b^2}\right)$$

$i^2 = -1$

$a^2 - i^2 b^2$

$a^2 - (-1) b^2$

$a^2 + b^2$

Since $a^2+b^2 \neq 0$. $\frac{1}{x} \in C^*$ and is the inverse of x.

Hence C^* is a group under usual multiplication.

---

12. Let $G = \{z/z \in C \text{ and } |z| = 1\}$. G is a group under usual multiplication.

Proof:

Let $z_1, z_2 \in G$

Then $|z_1| = |z_2| = 1$.

$\therefore |z_1 z_2| = |z_1||z_2| = 1$ and hence $z_1 z_2 \in G$

we know that usual multiplication of complex number is associative.

Scanned by CamScanner

Also, $1 = 1+i0 \in G_1$ and is the identity element.

now, let $z \in G_1$. Then $|z| = 1$

Hence $|1/z| = 1/|z| = 1/1 = 1$

$\therefore 1/z \in G_1$ and is the inverse of z.

Hence G_1 is a group.

---

13. The set of all n^{th} roots of unity with usual multiplication is a group.

Proof:

$$\sqrt[n]{1} = (1)^{1/n}$$

$\cos 2\pi = 1$

$\sin 2\pi = 0$

let $(\cos\theta + i\sin\theta)^{2\pi/n} = \omega$

$$\left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)$$

let, $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$

Then the n^{th} roots of unity are given by,

$$1, \omega, \omega^2, \ldots \omega^{n-1}$$

let $G_1 = \{1, \omega, \omega^2, \ldots \omega^{n-1}\}$

we know that $\omega^n = 1$, $\omega^{n+1} = \omega$ etc.

let, $\omega^r \cdot \omega^s \in G_1$

Scanned by CamScanner

Let $r+s = qn+t$ where $0 \le t < n$.

$$\omega^r \cdot \omega^s = \omega^{r+s} = \omega^{qn+t}$$

$$= (\omega^n)^q \, \omega^t = \omega^t \in G_1$$

we know that usual multiplication of complex number is associative.

$1 \in G_1$ is the identity element. $(\omega = (1)^{1/n})$

Inverse of ω^r

$$= \frac{\omega^n}{\omega^r} = \omega^n \cdot \omega^{-r} = \omega^{n-r}$$

Inverse of ω^r is ω^{n-r}

Hence G_1 is a group.

---

14. Let $G_1 = \{a+b\sqrt{2} \mid a, b \in Z\}$. Then G_1 is a group under usual addition.

Proof:

Let $a+b\sqrt{2}$ and $c+d\sqrt{2} \in G_1$

Then, $(a+b\sqrt{2}) + (c+d\sqrt{2})$

$= (a+c) + (b+d)\sqrt{2} \in G_1$

we know that usual addition is associative

$0 = 0+0\sqrt{2} \in G_1$ is the identity element

$-a-b\sqrt{2}$ is the inverse of $a+b\sqrt{2}$

Hence G_1 is a group

Scanned by CamScanner

15. Let G be the set of all real numbers except -1. Define $*$ on G by $a*b = a+b+ab$. Then $(G, *)$ is a group.

Proof:

Let $a, b \in G$

Then $a \neq -1$ and $b \neq -1$, we claim that $a*b \neq -1$

Suppose $a*b = -1$

Then, $a+b+ab = -1$

$a+b+ab+1 = 0$

$a(1+b) + (b+1) = 0$

$(a+b)\cdot(b+1) = 0$ so that either $a = -1$ or $b = -1$ which is a contradiction. Hence $a*b \neq -1$ and thus $*$ is a binary operation on G. $*$ is associative for $a*(b*c)$

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

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

Also $(a*b)*c = (a+b+ab)*c$

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

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

0 is the identity for $a*0 = a+0+0a = a$

and $0*a = 0+a+0a = a$

Scanned by CamScanner

Now, let a' be such that $a * a' = 0$

Hence $a * a' = 0$

$$a + a' + aa' = 0$$

$$a'(1+a) + a = 0$$

$$a'(1+a) = -a$$

$$a' = \frac{-a}{1+a}$$

Since $a \neq -1$, we have $a' \in R - \{-1\}$

Also, $a' * a = \frac{-a}{1+a} * a$

$$= \frac{-a}{1+a} + a - \frac{a^2}{1+a}$$

$$= \frac{-a}{1+a} + \frac{a(1+a)}{(1+a)} - \frac{a^2}{1+a}$$

$$= \frac{-a - a^2 + a(1+a)}{1+a}$$

$$= \frac{a - a^2 + a + a^2}{1+a} = 0$$

Hence a' is the inverse of a

Thus G is a group.

---

16 In R^* we define $a * b = (1/2)ab$. Then $(R^*, *)$ is a group.

Proof Obviously $*$ is a binary operation in R^*.

Scanned by CamScanner

Let $a, b, c \in R^*$

Then $(a*b)*c = \frac{1}{2}ab*c$

$$= \frac{\frac{1}{2}abc}{\frac{1}{2}}$$

$$= \frac{abc}{4}$$

$$= \left(\frac{1}{4}\right)abc$$

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

$$= \frac{\frac{1}{2}abc}{\frac{1}{2}}$$

$$= \frac{abc}{4}$$

$$= \left(\frac{1}{4}\right)abc$$

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

Hence $*$ is associative

Let $e \in R^*$ be such that $a*e = a$

$$a*e = \frac{1}{2}ae$$

$$a = \frac{1}{2}ae$$

$$e = 2$$

$2*a = a*2 = a$. Hence 2 is the identity

Let $a \in R^*$. Let $b \in R^*$ be such that $a*b = 2$

Then $\left(\frac{1}{2}\right)ab = 2$

$$ab = 2 \times 2$$

$$b = \frac{4}{a}$$

Scanned by CamScanner

$\therefore a * (1/a) = 1/2\,(1/a)\,a = 2$

$(1/a)$ is the inverse of a

Thus $(R^*, *)$ is a group.

---

17. Let $f_a : R \to R$ be the function defined by $f_a(x) = x + a$

Then $G = \{f_a / a \in R\}$ is a group under composition of functions.

Proof

Let $f_a, f_b \in G$

Then, $(f_a \circ f_b)(x) = (f_a(f_b(x)))$

$= (f_a(x+b))$

$= f_a(x+b)$

$= x + b + a$

$= f_{b+a}(x)$

Hence $f_a \circ f_b = f_{b+a} \in G$

$(f \circ g)(x) = f(g(x))$

$= (f_a \circ f_b)(x)$

$= f_a(f_b(x))$

$= f_a(x+b)$

$= x + b + a$

$= f_{b+a}(x)$

we know that composition of mapping is associative

Also, $f_a \circ f_0 = f_{a+0} = f_a = f_0 \circ f_a$

Hence f_0 is the identity

Also, $f_a \circ f_{-a} = f_0 = f_{-a} \circ f_a$

Hence f_{-a} is the inverse of f_a

Hence G is group

Scanned by CamScanner

Def:

Let $Z_n = \{0, 1, 2, \ldots (n-1)\}$

Let $a, b \in Z_n$. Let $a+b = q_n + r$ where $0 \le r < n$

we define $a \oplus b = r$

Let $ab = q'n + s$ where $0 \le s < n$

we define $a \odot b = s$

The binary operations $\oplus$ and $\odot$ are called addition modulo n and multiplication modulo respectively.

---

8. $(Z_n, \oplus)$ is a group.

Proof

Clearly $\oplus$ is a binary operation in Z_n.

Let $a, b, c \in Z_n$

Let

$a+b = q_1 n + r_1$ where $0 \le r_1 < n \longrightarrow (1)$

$b+c = q_2 n + r_2$ where $0 \le r_2 < n \longrightarrow (2)$

$r_1 + c = q_3 n + r_3$ where $0 \le r_3 < n \longrightarrow (3)$

using (1) and (3)

$a+b+r_1+c = q_1 n + r_1 + q_3 n + r_3$

$a+b+c = (q_1 + q_3) n + r_3 + r_1 - r_1$

$a+b+c = (q_1 + q_3) n + r_3$

Scanned by CamScanner

$$a + q_2 n + r_2 = (q_1 + q_3) n + r_3 \quad \text{(by 2)}$$

$$a + r_2 = (q_1 - q_2 + q_3) n + r_3$$

$$a + r_2 = q_4 n + r_3 \longrightarrow (4)$$

where $q_4 = q_1 - q_2 + q_3$

$a \oplus b = q_1 n + r_1$

$a \oplus b = r_1$

$b \oplus c = q_2 + r_2$

$b \oplus c = r_2$

$r_1 \oplus c = q_3 + r_3$

$r_1 \oplus c = r_3$

$a \oplus r_2 = q_4 n + r_3$

$a + r_2 = r_3$

now $(a \oplus b) \oplus c = r_1 \oplus c$

$= r_3$

Also $a \oplus (b \oplus c) = a \oplus r_2$

$= r_3$

Hence $\oplus$ is associative

clearly the identity element is 0

and the inverse of $a \in Z_n$ is $n-a$.

Hence $(Z_n, \oplus)$ is a group.

Note :1 $(Z_n, \oplus)$ is called the group of Integers modulon.

---

note :2. This example shows that for any positive integer n there exists a group with n elements.

---

19 19. Let n be a Prime. Then $Z_n - \{0\}$ is a group under multiplication modulon.

Proof

Scanned by CamScanner

Proof

Let $a, b \in Z_n - \{0\}$

Then $a \neq 0$ and $b \neq 0$

Now, by definition $a \odot b \in Z_n$. We claim that $a \odot b \neq 0$

Suppose $a \odot b = 0$

Then $n \mid ab = \frac{ab}{n}$ $\quad n/a = q/n$

Since n is prime n/a or n/b $\quad n/b = b/n$

$\therefore a = 0$ (or) $b = 0$ which is contradiction

Hence $a \odot b \in Z_n - \{0\}$

Now, let $a, b, c \in Z_n - \{0\}$

Let,

$ab = q_1 n + r_1$ where $0 \leq r_1 < n \longrightarrow (1)$

$bc = q_2 n + r_2$ where $0 \leq r_2 < n \longrightarrow (2)$

$r_1 c = q_3 n + r_3$ where $0 \leq r_3 < n \longrightarrow (3)$

Eqn (1) multiplies c

$abc = q_1 nc + r_1 c$

$a(q_2 n + r_2) = q_1 cn + q_3 n + r_3$

$aq_2 n + ar_2 = q_1 cn + q_3 n + r_3$

$ar_2 = q_1 cn + q_3 n + r_3 - aq_2 n$

$ar_2 = (q_1 c + q_3 - aq_2) n + r_3$

Scanned by CamScanner

$$ar_2 = q_4 n + r_3 \longrightarrow (4)$$

where $q_4 = q_1 c + q_3 - a q_2$.

now $(a \odot b) \odot c = r_1 \odot c$

$(a \odot b) \odot c = r_3$

Also $a \odot (b \odot c) = a \odot r_2$

$= r_3$

$(a \odot b) \odot c = a \odot (b \odot c)$

Hence $\odot$ is associative

$1 \in Z_n - \{0\}$ is the identity element.

Let $a \in Z_n - \{0\}$

Since n is prime $(a, n) = 1$ (coprime)

Hence the linear congruence

$ax = 1 \pmod n$ has a unique sol^n, say

$b \in Z_n - \{0\}$

clearly $a \odot b = b \odot a = 1$

Thus b is the inverse of a

Hence $Z_n - \{0\}$ is a group.

Scanned by CamScanner

2020. The set of all positive integers less than n and prime to it is a group under multiplication modulo n.

Proof: Let $G = \{m / m < n \text{ and } (m, n) = 1\}$.

Let $p, q \in G$ obviously $pq \neq n$ and $(pq, n) = 1$

Now, let $pq = sn + r$, $0 < r < n$

Hence $p \odot q = r$ (by definition)

we claim that $(r, n) = 1$.

Suppose, $(r, n) = a > 1$, then a/r and a/n

Hence $a/(r + sn)$ ie a/pq. Also a/n.

Hence $(pq, n) \neq 1$ which is a contradiction.

Hence $r \in G$. Hence G is closed under $\odot$ we know that multiplication modulon is associative $1 \in G$ is the identity element. Let $a \in G$. Then $(a, n) = 1$.

Hence the linear congruence $ax \equiv 1 \pmod{n}$ has a unique solution for x. Say b.

$\therefore ab \equiv 1 \pmod{n}$. Hence $a \odot b = 1$

Now, we have to prove that $b \in G$. Suppose $(b, n) = c$

Since $ab = 1 \pmod{n}$. $ab = qn + 1$

Now c/b and $c/n \Rightarrow a/(ab - qn) \Rightarrow c/1$

$\Rightarrow c = 1$ Thus $(b, n) = 1$

Hence $b \in G$ and is the inverse of a.

Thus G is a group

Scanned by CamScanner

21. Let G denote the set of all matrices of the form $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ where $x \in R^*$. Then G is a group under matrix multiplication.

Proof:- Let $A, B \in G$. Let $A = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

and $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix}$

Then, $AB = \begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix}$

$$AB = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G$$

we know that matrix multiplication is associative

Let $E = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$ be such that

$$AE = A$$

$$\therefore \begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$$\therefore \begin{pmatrix} 2xe & 2xe \\ 2xe & 2xe \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$$2xe = x$$

$$e = 1/2$$

$E = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ is the identity element of G.

Let $\begin{pmatrix} y & y \\ y & y \end{pmatrix}$ be the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$

Then, $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

$$\begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

Scanned by CamScanner

$2xy = 1/2$.

Inverse of $\begin{pmatrix} x & xy \\ x & x \end{pmatrix}$

Hence G_1 is a group.

---

22. In N we define $a * b = a$. Then $(N, *)$ is not a group.

Proof:

clearly $*$ is an associative binary operation on N. However, there is no element $e \in N$ such that $e * a = a$ for all $a \in N$

Hence there is no identity element in $(N, *)$

Hence $(N, *)$ is not a group.

Def.

A group G is said to be abelian if $ab = ba$ for all $a, b \in G$. A group which is not abelian is called a non-abelian group

---

Elementary properties of a Group

1. Let G be a group then,

(i) identity element of G is unique

(ii) for any $a \in G$ the inverse of a is unique

Scanned by CamScanner

Proof:

(i) Let e and e' be two identity elements of G.

Then $ee' = e'$ (since e is an identity)

$ee' = e$ (since e' is an identity)

left side equal = right side equal

Hence $e = e'$

(ii) Let a' and a'' be two inverse of a.

$aa' = a'a = e$ and

$aa'' = a''a = e$

$\therefore a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$

$a' = a''$

---

2. In a group the left and right cancellation laws hold (ie) $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$

Proof

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

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

$\Rightarrow eb = ec$

$\Rightarrow b = c$

Similarly,

$ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$

$\Rightarrow be = ce$

$\Rightarrow b = c$

Hence the proved.

Scanned by CamScanner

3. Let G be a group and $a, b \in G$. Then the equations $ax = b$ and $ya = b$ have unique solution for x and y in G.

Proof:-

Consider $a^{-1}b \in G$.

$$a(a^{-1}b) = (aa^{-1})b$$
$$= eb$$
$$= b$$

Hence $a^{-1}b$ is a solution of $ax = b$

Now, to prove the uniqueness

Let x_1 and x_2 be two solution of $ax = b$

Then, $ax_1 = b$ and

$ax_2 = b$

$ax_1 = ax_2$ which implies

$x_1 = x_2$

$x = a^{-1}b$ is the unique solution for

$ax = b$

Similarly,

$ba^{-1} \in G$

$$(ba^{-1})a = b(a^{-1}a)$$
$$= be$$
$$= b$$

Hence ba^{-1} is a solution of $ya = b$

Now, to prove the $y = ba^{-1}$ is the unique

Let y_1 and y_2 be two solutions of $ya = b$

$y_1 a = b$ and

$y_2 a = b$

Scanned by CamScanner

$y_1 = y_2$

$y = ba^{-1}$ is the unique solution for

$ya = b$

Hence the proved.

---

4. Let G be a group. Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$

Proof :-

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$$
$$= aea^{-1}$$
$$= (ae)a^{-1}$$
$$= aa^{-1}$$
$$= e$$

Similarly.

$$(b^{-1}a^{-1})(ab) = e$$
$$b^{-1}a^{-1} = \frac{e}{ab}$$
$$b^{-1}a^{-1} = e(ab)^{-1}$$

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

Defination :-

Let G be a group and $a \in G$. For any positive integer n. we define $a^n = aa \cdots a$ (a written n times)

clearly,

$$(a^n)^{-1} = (aa \cdots a)^{-1}$$

Scanned by CamScanner

$= (a^{-1}\, a^{-1} \cdots\cdots a^{-1})$

$= (a^{-1})^n$

we now define $a^{-n} = (a^{-1})^n$

$= (a^n)^{-1}$

Finally we define $a^0 = e$

Thus a^n is defined for all integers n.

---

5. (i) $a^m a^n = a^{m+n}$, $m, n \in Z$

(ii) $(a^m)^n = a^{mn}$, $m, n \in Z$

Proof:-

(i) when $n = 0$ the result follows directly from the definition. now let $n > 0$.

we prove the result by induction on n.

when $m \geq 0$. $a^{m+1} = a^m a^1$ (by def)

$m = -1$; $a^{m+1} = a^0 = e$

$a^m\, a^1 = a^1 a = e$.

Hence $a^{m+1} = a^m a^1$

when, $m \leq -2$ let $m = -p$ where $p \geq 2$

$\therefore (a^m)\, a = (a^{-p})\, a = (a^{-1})^p a$

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

$= (a^{-1})^{p-1}$

$= a^{-p+1}$

$= a^{m+1}$

Scanned by CamScanner

Hence $a^{m+1} = a^m a^1$ for all $m \in Z$

Hence the result is true for $n=1$. suppose now that the theorem is valid for $n=k>1$.

$$a^m a^k = a^{m+k}$$

$$\therefore a^m a^{k+1} = a^m (a^k a)$$

$$= (a^m a^k) a$$

$$= a^{m+k} a \quad \text{(hypothesis)}$$

$$= a^{m+k+1} \quad \text{(by def.)}$$

Thus it follows that the theorem is valid for $n = k+1$.

Hence by induction the theorem holds forall positive integers n.

Finaly if $n<0$. we can prove the result by induction on $-n$.

Proof of (ii) is left to the reader.

Solved problems

1. Show that in a group G. $x^2 = x$ if and only if $x = e$

Sol $\quad e^2 = ee = e$

conversly let $x^2 = x$

Then $\quad x\,x = x\,e$

Hence by cancellation law $x = e$

Scanned by CamScanner

Note:

An element $a \in G$ is called idempotent if $a^2 = a$. Thus we have shown that in a groaph G. The identity element is the only idempotent element.

2. In an abelian group $(ab)^2 = a^2b^2$

Sol

$$(ab)^2 = (ab)(ab)$$
$$= a(ba)b$$
$$= a(ab)b$$
$$= (aa)(bb)$$
$$= a^2b^2$$

3. Let G be groaph such that $a^2 = e$ for all $a \in G$ Then G is abelian.

Sol

$$a^2 = e \Rightarrow aa = e \Rightarrow a = a^{-1}$$

now,

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

Hence G is abelian.

4. Let G be a group in which $(ab)^m = a^m b^m$ for three consecutive integers and for all $ab \in G$. Then G is abelian.

Sol

Let $a, b \in G$

Let $(ab)^m = a^m b^m$; $(ab)^{m+1} = a^{m+1}b^{m+1}$ and

$$(ab)^{m+2} = a^{m+2}b^{m+2}$$

Scanned by CamScanner

$(ab)^{m+1} = a^{m+1} b^{m+1}$

$(ab)^m (ab)^1 = a^m a^1 b^m b^1$

$b^m a = a b^m$ (by cancellation) → ①

Similarly,

$(ab)^{m+2} = a^{m+2} b^{m+2}$

$(b)^{m+1} a^1 = a \cdot b^{m+1}$

$b^m b^1 a^1 = a \cdot b^m b^1$

$b^m ba = a b^m b$

$\Rightarrow ba = abc$ (by cancellation law)

$\therefore$ a is abelian.

---

5. Let $(H, \cdot)$ and $(K, *)$ be groups. We define a binary operation $\square$ on $H \times K$ by $(h_1, k_1) \square (h_2, k_2) = (h_1 h_2, k_1 * k_2)$ Then $H \times K$ is a group.

$H \times K$ is called the direct product of H and K

First we shall prove that $\square$ is associative.

Let $(h_1, k_1) \cdot (h_2, k_2) \cdot (h_3, k_3) \in H \times K$

$[(h_1 \cdot k_1) \square (h_2 \cdot k_2)] \square (h_3 \cdot k_3)$

$= (h_1 h_2, k_1 * k_2) \square (h_3 \cdot k_3)$

$= ((h_1 h_2) h_3 \cdot (k_1 * k_2) * k_3)$

Scanned by CamScanner

$= (h_1(h_2 h_3), k_1 * (k_2 * k_3))$

$= (h_1, k_1) \square (h_2 h_3 , k_2 * k_3)$

$= (h_1, k_1) \square [(h_2 , k_2) \square (h_3 , k_3)]$

Let e, e_1 be the identities of the groups H and K respectively. clearly (e, e_1) is the identity element in $H \times K$. Also (h^{-1}, k^{-1}) is the inverse of (h, k)

Hence $H \times K$ is a group.

Equivalent Definitions of a Group.

Def:

Let $*$ be a binary operation defined on G.

An element $e \in G$ is called a left identity if $e * a = a$ for all $a \in G$.

e is called a right identity if $a * e = a$ for all $a \in G$.

Def:

Let $*$ be a binary operation defined on G.

Let $e \in G$ be the identity element. Let $a \in G$.

An element $a' \in G$ is called a left inverse of a. if $a' * a = e$ a' is called a right inverse of a if $a * a' = e$

Scanned by CamScanner

1. Let G be a non-empty set with an associative binary operation defined on it such that there exists a left identity e in G and each element $a \in G$ has a left inverse a' with respect to then G is a group.

Proof:

$$a^{-1} * a = e$$

a' is a left inverse of a so that $a'a = e$

Let a'' be a left inverse of a' so that $a''a' = e$

Then $aa' = e(aa')$ (Since e is left identity)

$= (a''a')(aa')$

$= a''(a'a)a'$ (associatively)

$= a''(ea')$

$= a''a'$ (since e is left identity

$= e.$

Hence a' is also a right inverse of a.

Also, $a = ea = (aa')a$

$= a(a'a)$

$= ae = a$

Hence e is also a right identity

Thus, $ea = a = ae$

and

$a'a = aa' = e$ and forall $a \in G$,

Hence G is a Grouph.

Scanned by CamScanner

2. Let G be a non-empty set with an associative binary operation defined on it such that equations $ax = b$ and $ya = b$ have unique solu for x and y in G. Then G is a gro

Proof: Let $a \in G$

Then there exists a unique $e \in G$ such that

$$ea = a.$$

Now, let b be any other element in G. Then there exists a unique x in G such that $ax = b$.

$$\begin{aligned} eb &= e(ax) \\ &= (ea)x. \\ &= ax \\ &= b \end{aligned}$$

$eb = b$ for all $b \in G$ so that e is a identity. Let $a \in G$. Then $ya = a$ has a unique solu a'.

$a'a = e$ so that a' is the left invers of a.

Hence (by theorem 3.6) let G be a non-emp set with an associative binary operations defined on it such that there exists a left identity e in G and each element $a \in G$ has a left inverse a' with respect to e.

Then G is a group.

Scanned by CamScanner

UNIT-II

Sub groups :-

Def :-

Let G be a set with a binary operation * defined on it. Let $S \subseteq G$. If for each $a, b \in S$. $a * b$ (Computed in G) is in S. we say that S is <u>closed</u> with respect to the binary operation "*".

Def:

A subset H of group G is called a <u>Sub group</u> of G if H forms a group with respect to the binary operation in G.

Examples :-

1. Let G be any group. Then $\{e\}$ and G are subgroups of G. They are called Improper subgroups of G.

2. $(Q, +)$ is a subgroup of $(R, +)$ and $(R, +)$ is a subgroup of $(C, +)$.

3. In $(Z_8, \oplus)$, let $H_1 = \{0, 4\}$ and $H_2 = \{0, 2, 4, 6\}$

The Cayley tables for H_1 and H_2 are given by

$\oplus$	0	4
0	0	4
4	4	0

Scanned by CamScanner

$\oplus$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

$8/8 = 0$

$12/8 = 4$

It is easily seen that H_1 and H_2 are closed under $\oplus$ and $(H_1, \oplus)$ and $(H_2, \oplus)$ are groups

Hence H_1 and H_2 are subgroups of Z_8.

④ $\{1, -1\}$ is a subgroup of $(R^*, \cdot)$

⑤ $\{1, i, -1, -i\}$ is a subgroup of $(C^*, \cdot)$

2 marks

6. For any integer n we define

$$nZ = \{nx / x \in Z\}$$

Then $(nZ, +)$ is a subgroup of $(Z, +)$

For, let $a, b \in nZ$

Then, $a = nx$

$b = ny$

where $x, y \in Z$

Hence $a + b = n(x+y) \Rightarrow nx + ny \in nZ$;

Hence nZ is closed under $+$

$0 \in nZ$ is the identity element

Scanned by CamScanner

Inverse of nx is $-nx = n(-x) \in nz$.

Hence $(nz, +)$ is a group.

Theorem : 3.15

Let H be a sub group of G_1. Then (a) the identity element of H is the same as that of G_1.

(b) For each $a \in H$ the inverse of a in H is the same as the inverse of a in G_1.

Proof:

(a) Let e and e' be the identities of G_1 and H respectively

$e \in G_1$

$e' \in H$

Let $a \in H$, Now,

$ea = ae = a$

$e'a = ae' = a$

$e'a = a$ (since e' is the identity of H)

$= ea$ (since e is the identity of G_1 and $a \in G_1$)

$e'a = ea$

$e' = e$ (by cancellation law)

(b) Let a' and a'' be the inverse of a in G_1 and H respectively.

$aa' = a'a = e$

$aa'' = a''a = e' = e$

$aa' = a'a = aa'' = a''a = e$

Scanned by CamScanner

$a'a = e = a''a$

$a'a = a''a$

$a' = a''$

Since by (a). G and H have the same identity element e.

$a'a = e = a''a$ (by cancellation law)

$a' = a''$

Theorem : 3.16

A subset H of a group G is a subgroup of G iff.

(i) it is closed under the binary operation in G.

(ii) The identity e of G is in H.

(iii) $a \in H \Rightarrow a^{-1} \in H$.

Proof :

Let H be a subgroup of G. The result follows immediately.

(i) $e \in H$ $e \in G$

(ii) inverse is same

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

Conversly let H be a subset of G satisfying conditions (i), (ii) and (iii). Then, obviously H itself is a group with respect to the binary operation in G.

There fore H is a subgroup of G.

Scanned by CamScanner

Theorem : 3.17

A non-empty subset H of a group G is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$

Proof :-

Let H be a subgroup of G. Then $a, b \in H$

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

$a, b \in G$

$ab \in G$

$a.b \in H$

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

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

$ab^{-1} \in H$

Conversly, let H be a non-empty subset of G such that $a, b \in H$

$ab^{-1} \in H.$

Since, $H \neq \phi$, there exists an element $a \in H$

Hence $aa^{-1} \in H$

Thus $e \in H.$

$e, a \in H$

$ea^{-1} \in H.$

Hence $a^{-1} \in H$

let, $a, b \in H.$ Then $a, b^{-1} \in H$

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

Thus H is closed under the binary operation in G.

Hence by G is a subgroup of G.

Scanned by CamScanner

Note:

If the operation is + then H is a subgroup of G iff $a, b \in H \Rightarrow a-b \in H$

Def:

Let A and B be two subsets of a group G. we define $AB = \{ab / a \in A, b \in B\}$

Theorem: 3.21

Let A and B be two subgroups of a group G. Then AB is a subgroup of G iff $AB = BA$.

Proof:

Let AB be a subgroup of G.

we claim that $AB = BA$

Let $x \in AB$

Since AB is a subgroup of G.

$$x^{-1} \in AB$$

Let $x^{-1} = ab$ where $a \in A$ and $b \in B$

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

Since A and B are subgroups of G.

$a^{-1} \in A$ and $b^{-1} \in B$

$\therefore x \in BA$

Hence $AB \subseteq BA \longrightarrow (1)$

Now, let $x \in BA$

Then $x = ba$ where $b \in B$ and $a \in A$

$\therefore x^{-1} = (ba)^{-1} = a^{-1}b^{-1} \in AB$

Scanned by CamScanner

Now,

Since AB is a subgroup and $x^{-1} \in AB$ we have $x \in AB$.

$$BA \subseteq AB \longrightarrow (2)$$

From (1) and (2) we get

$$AB = BA$$

Conversely,

Let $AB = BA$

we claim that AB is a subgroup of G_1.

Clearly, $e \in AB$ and hence AB is non-empty.

Now, let $x, y \in AB$. Then $x = a_1 b_1$ and $y = a_2 b_2$ where, $a_1, a_2 \in A$ and $b_1, b_2 \in B$

$$\therefore xy^{-1} = (a_1 b_1)(a_2 b_2)^{-1}$$
$$= a_1 b_1 b_2^{-1} a_2^{-1}$$

Now,

$$b_2^{-1} a_2^{-1} \in BA$$

Since,

$$BA = AB.$$

$$b_2^{-1} a_2^{-1} \in AB$$

$$\therefore b_2^{-1} a_2^{-1} = a_3 b_3 \text{ where } a_3 \in A \text{ and}$$

$$b_3 \in B$$

$$xy^{-1} = a_1 b_1 a_3 b_3$$

Now,

$$b_1 a_3 \in BA$$

Scanned by CamScanner

Since $BA = AB$, $b_1 a_3 \in AB$

$\therefore b_1 a_3 = a_4 b_4$ where $a_4 \in A$ and $b_4 \in B$

$$xy^{-1} = a_1 (a_4 b_4) b_3$$

$$= (a_1 a_4)(b_4 b_3) \in AB$$

AB is a sub group of G.

Corollary:

If A and B are subgroups of an abelian group G. Then AB is a sub group of G.

Proof:

Let $x \in AB$.

Then, $x = ab$ where $a \in A$ and $b \in B$

$x \in BA$

$x = ab \quad a \in A \quad b \in B$

$x = ba \quad b \in B \quad a \in A$

$x \in BA$

Hence $AB \subseteq BA$

Similarly

Let $x \in BA$

$x = ba \quad b \in B \quad a \in A$

$x = ab \quad a \in A \quad b \in B$

$x \in AB$

Hence, $BA \subseteq AB$.

$\therefore AB = BA$

Hence AB is a subgroup of G.

Scanned by CamScanner

1. Let $a \in R^*$. Let $H = \{a^n / n \in Z\}$. Then H is a subgroup of R^*.

Sol

clearly,

H is non-empty

now,

let $x, y \in H$

Then, $x = a^s$ and $y = a^t$

where $s, t \in Z$

$\therefore xy^{-1} = a^s (a^t)^{-1}$

$= a^s a^{-t}$

$= a^{s-t} \in H.$

Hence H is a subgroup of R^*

---

3. Let G be the set of all 2x2 matrices with entires from R. Then G is a group under matrix addition.

Let $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in R \right\}$. Then H is a subgroup of G.

Sol: Let $A, B \in H$.

Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and

$B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

now,

$AB = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

$= \begin{pmatrix} a-c & 0 \\ 0 & b-d \end{pmatrix} \in H.$

Hence H is a subgroup of G.

Scanned by CamScanner

4. Let G be a group.

Let $H = \{a / a \in G$ and $ax = xa$ for all $x \in G\}$.

i.e) H is the set of all elements which commute with every other element. Show that H is a subgroup of G.

Sol :-

Clearly, $ex = xe = x$ for all $x \in G$

Hence $e \in H$

So that H is non empty

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

Then, $ax = xa$ and

$bx = xb$ for all $x \in G$

Now, $bx = xb \Rightarrow b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1}$

$\Rightarrow (b^{-1}b)xb^{-1} = b^{-1}x(bb^{-1})$

$\Rightarrow exb^{-1} = b^{-1}xe$

$\Rightarrow xb^{-1} = b^{-1}x \longrightarrow (1)$

$\therefore$ let $(ab^{-1})x = a(b^{-1}x)$

$= a(xb^{-1})$ (by (1))

$= (ax)b^{-1}$

$= (xa)b^{-1}$ (Since $ax = xa$)

$= x(ab^{-1})$

Thus ab^{-1} commutes with every element of G.

$\therefore ab^{-1} \in H$ and hence H is a subgroup of G

Scanned by CamScanner

Note:

The above subgroup of G_1 is called the centre of G and is denoted by $Z(G_1)$

5. Let G_1 be a group and let a be a fixed element of G_1.

Let $H_a = \{x / x \in G_1 \text{ and } ax = xa\}$

i.e) H_a is the set of all elements in G_1 which commute with a.

Show that H_a is a subgroup of G_1.

Sol

clearly, $ea = ae = a$

Hence $e \in H_a$ so that H_a is non-empty

Now, let $x, y \in H_a$

Then, $ax = xa$ and

$ay = ya$

Now,

$$ay = ya \Rightarrow y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$$

$$y^{-1}a(yy^{-1}) = (y^{-1}y)ay^{-1}$$

$$y^{-1}ae = eay^{-1}$$

$$y^{-1}a = ay^{-1} \longrightarrow (1)$$

Hence,

$$a(xy^{-1}) = (ax)y^{-1}$$

$$= x(ay^{-1}) \quad ay = ya$$

$$= x(y^{-1}a)$$

$$= (xy^{-1})a.$$

Hence xy^{-1} commutes with a.

$xy^{-1} \in H_a$ and hence H_a is a subgroup of G_1.

Scanned by CamScanner

Note:

H_a is called the normaliser of a in G.

Cyclic Groups.

Def:

Let G be a group. Let $a \in G$,

then $H = \{a^n / n \in Z\}$ is a subgroup of G (verify)

H is called the cyclic sub group of G generated by a and is denoted by (a).

Ex.

(i) In $(Z, +)$ $\langle 2 \rangle = 2Z$ which is the group of even integers.

(ii) In the group $G = (Z_{12}, \oplus)$, $\langle 3 \rangle = \{0, 3, 6, 9\}$

$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = Z_{12}$

(iii) In the group $G = \{1, i, -1, -i\}$

$\langle i \rangle = \{i, i^2, i^3 \ldots\}$

$= \{i, -1, -i, 1 \ldots\} = G$

Def:

Let G be a group and let $a \in G$, a is called generator of G if $\langle a \rangle = G$.

A group G is cyclic if there exists an element $a \in G$ such that $\langle a \rangle = G$.

Scanned by CamScanner

Note:

If G_1 is a cyclic group generated by an element a, then every element of G_1 is of the form a^n for some $n \in Z$.

Theorem : 3.22

Any cyclic group is abelian.

Proof:

Let $G_1 = \langle a \rangle$ be a cyclic group.

Let $x, y \in G_1$.

Then, $x = a^r$ and

$y = a^s$ for some $r, s \in Z$.

Hence, $xy = a^r a^s$

$= a^{r+s}$

$= a^{s+r}$

$= a^s a^r$

$= yx$

$\therefore G_1$ is abelian.

Theorem : 3.23

A subgroup of cyclic group is cyclic.

Proof:

Let G_1 be a cyclic group generated by a and let H be a subgroup of G_1.

We claim that H is cyclic.

Clearly, every element of H is of the form a^n for some integer n.

Scanned by CamScanner

Let m be the smallest positive integer such that $a^m \in H$.

We claim that a^m is a generator of H.

Let $b \in H$. Then $b = a^n$ for some $n \in \mathbb{Z}$.

Let $n = mq + r$ where $0 \leq r < m$.

Then, $b = a^n = a^{mq+r} = a^{mq} a^r$

$$b = (a^m)^q a^r \Rightarrow a^r = \frac{b}{(a^m)^q}$$

$$\therefore a^r = (a^m)^{-q} b \longrightarrow (1)$$

Now,

$a^m \in H$

Since H is a subgroup.

$(a^m)^{-q} \in H$.

Also, $b \in H$

By (1) $a^r \in H$ and $0 \leq r < m$.

But m is the least positive integer such that $a^n \in H$.

$\therefore r = 0$

Hence $b = a^n$

$= a^{qm}$

$= (a^m)^q$

$\therefore$ Every element of H is a power of a^m.

$\therefore H = \langle a^m \rangle$ and Hence H is cyclic.

Scanned by CamScanner

Order of an Element.

Def:- Let G be a group and let $a \in G$. The least positive integer n (if it exists) such that $a^n = e$ is called the order of a. If there is no positive integer n such that $a^n = e$. then the order of a is said to be infinite.

Theorem : 3.24.

Let G be a group and $a \in G$. Then the order of a is the same as the order of the cyclic group generated by a.

Proof: Let a be a group and $a \in G$. Then $a^n = e$

we claim that $e, a, a^2 \ldots a^{n-1}$ are all distinct

Suppose $a^r = a^s$ where $0 < r < s < n$.

Then, $a^{s-r} = e$ and $s - r < n$ which contradicts the definition of the order of a. Hence $e, a, a^2 \ldots a^{n-1}$ are n distinct elements and $\langle a \rangle = \{e, a, a^2 \ldots a^{n-1}\}$ which is of order n.

If a is of infinite order, the sequence of element $a, a^2 \ldots a^n \ldots$ are all distinct and are in $\langle a \rangle$. Hence (a) is an infinite group.

Scanned by CamScanner

Theorem 3.25

In a finite group every element is a finite order.

Proof: Let $a \in G$.

If a is of infinite order, then $\langle a \rangle$ is an infinite subgroup of G, which is a contradiction since G is finite. Hence the order of a is finite.

Theorem : 3.26.

Let G be a group and a be an element of order n in G. Then $a^m = e$ iff n divides m.

proof:

Suppose n/m.

$n/m = \frac{m}{n}$

Then $\frac{m}{n} = q$

$m = nq$

where $q \in Z$

$a^m = a^{nq}$

$= (a^n)^q$

$= e^q$

$= e$.

conversely let $a^m = e$

let $m = nq + r$ where $0 \leq r < n$.

$\therefore a^m = a^{nq+r}$

$= a^{nq} a^r$

$= e a^r$

$= a^r$

Scanned by CamScanner

$\therefore a^r = e$ and $0 \leq r < n$

Now,

Since n is the smallest positive integer such that $a^n = e$. we have $r = 0$

Hence $m = nq$.

Therefore n/m.

Theorem : 3.27

Let G be a group and $a, b \in G$.

Then, (i) order of a = order of a^{-1}

(ii) order of a = order of $b^{-1}ab$

(iii) order of ab = order of ba.

Proof :

(i) Let a be an element of order n.

Then $a^n = e$.

$$(a^{-1})^n = (a^n)^{-1}$$
$$= e^{-1}$$
$$= e$$

Now,

If Posible, let $0 < m < n$ and $(a^{-1})^m = e$

$\therefore (a^m)^{-1} = e$.

Hence $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(a^{-1})^n = e$

$\therefore$ The order of a^{-1} is n.

Scanned by CamScanner

(ii) we shall first prove that for any positive integer r.

$$(b^{-1}ab)^r = b^{-1}a^r b \longrightarrow (1)$$

(1) is trivialy true if $r=1$.

Now, Suppose that (1) is true for $r=k$ so that $(b^{-1}ab)^k = b^{-1}a^k b$.

Then $(b^{-1}ab)^{k+1} = (b^{-1}ab)^k (b^{-1}ab)$

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

$= b^{-1}a^{k+1}b.$

Hence by induction (1) is true for all positive integers.

Now, let a be an element of order n.

Then $a^n = e$.

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

$= b^{-1}eb$

$= e$

Now,

If possible, let $0 < m < n$ and $(b^{-1}ab)^m = e$

$\therefore b^{-1}a^m b = e.$

Hence $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(b^{-1}ab)^n = e$

Scanned by CamScanner

$\therefore$ The order of $b^{-1}ab$ is n.

(iii) The order of ab = the order of $a^{-1}(ab)a$

= The order of ba. (by (i) & (ii))

Theorem: 3.28

Let G be a group and let a be an elements of order n in G. Then the order of a^s, where $0 < s < n$, is n/d where d is the g.c.d of n and s.

Proof:

Let $(n/d) = k$ and $(s/d) = l$ so that k and l are relatively prime,

Now, $(a^s)^k = a^{sk} = a^{ld \cdot k} = a^{ln} = (a^n)^l = e$

Further if m is any positive integer such that $(a^s)^m = e$ then $a^{sm} = e$

Since order of a is n, we have n/sm

$\therefore kd/ldm$

Hence k/lm

But k and l are relatively prime

Hence k/m so that $m \geq k$.

Thus k is the least positive integer such that $(a^s)^k = e$

$\therefore$ order of $a^s = k = n/d$.

Scanned by CamScanner

1. If G is a finite group with even number of elements then G contains at least one element of order 2.

Sol:

a is an element of order $2 \Leftrightarrow a^2 = e$

$\Leftrightarrow a^{-1} = a$.

Hence it is enough if we prove that there exists an element different from e in G whose inverse is itself.

Let $S = \{a \in G, a \neq a^{-1}\}$

Hence

clearly $a \in S \Rightarrow a^{-1} \in S$ and $a \neq a^{-1}$

Hence S contains an even number of elements

Also $e \notin S$.

Hence $S \cup \{e\}$ contains an odd number of elements, since the order of the group is even. there exists at least one element $a \notin S \cup \{e\}$.

clearly $a = a^{-1}$

---

2. The order of a permutation P is the l.c.m. of the lengths if its disjoint cycles.

Sol:

Let $P = C_1 C_2 \ldots C_r$ where the C_i s are are mutually disjoint cycles of lengths l_i

now, let $p^m = e$

Scanned by CamScanner

Since product of disjoint cycles is commutative

$$e = p^m = (c_1, c_2 \cdots c_r)^m$$

$$= c_1^m c_2^m \cdots c_r^m.$$

Now,

Since the elements moved by one cycle are left fixed by all the other cycles.

$$c_1^m = c_2^m = \cdots c_r^m = e$$

Now, $c_1^m = e \Rightarrow l_1 / m$.

Since the order of $c_1 = l_1$

Similarly $l_2, l_3 \cdots l_r$ divide m.

Thus m is a common multiple of $l_1, l_2 \cdots l_r$.

∴ The order of p is the least such m which is obviously the L.C.M of $l_1, l_2 \cdots l_r$.

---

3. If a is a generator of the cyclic group G and if there exists two unequal integers m and n such that $a^m = a^n$. Prove that G is a finite group.

Sol

Since m and n are unequal we may assume that $m > n$.

Hence $m-n$ is a positive integer.

Also, $a^m = a^n \Rightarrow a^{m-n} = e$

∴ Order of a is finite.

∴ $G = \langle a \rangle$ is a finite group.

Scanned by CamScanner

Cosets and Lagrange's Theorem.

Def:- Let H be a subgroup of a group G. Let $a \in G$. Then the set $aH = \{ah / h \in H\}$ is called the left coset of H defined by a in G.

Similarly $Ha = \{ha / h \in H\}$ is called the right coset of H defined by a.

Ex.

(i) Consider $(Z_{12}, \oplus)$. Then $H = \{0, 4, 8\}$ is a subgroup of G.

The left cosets of H are given by

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

we notice that

$$4 + H = \{4, 8, 0\} = H \text{ and}$$
$$5 + H = \{5, 9, 1\} = 1 + H \text{ etc.}$$

Theorem 3.29.

Let G be a group and H be a subgroup of G. Then.

(i) $a \in H \Leftrightarrow aH = H$

(ii) $aH = bH \Leftrightarrow a^{-1}b \in H$

(iii) $a \in bH \Leftrightarrow a^{-1} \in Hb^{-1}$

(iv) $a \in bH \Leftrightarrow aH = bH$

Scanned by CamScanner

Proof:

(i) Let $a \in H$

we claim that $aH = H$

$x \in aH \qquad a \in H$

$x = ah \qquad h \in H$

(Since H is a subgroup)

$h \in H \Rightarrow ah \leq H$

Hence $aH \subseteq H$

Let $x \in H$

$x = ex$

$= (aa^{-1})x$

$= a(a^{-1}x) \in aH$

Hence $H \subseteq aH$. Thus $H = aH$

conversly.

Let $aH = H$

Now, $a = ae \in aH$

$\therefore a = H$

(ii) Let $aH = bH$

$a \in H \Leftrightarrow aH = b$

$a^{-1}b \in H \Leftrightarrow a^{-1}bH = H$

$a^{-1}aH = a^{-1}bH$

$eH = a^{-1}bH$

$H = a^{-1}bH$

$a^{-1}b \in H$

$a^{-1}bH = H$

$(aa^{-1})bH = aH$

Scanned by CamScanner

$ebH = aH$

Hence $bH = aH$

(iii) let $a \in bH \Rightarrow a = bh$

$a^{-1} \in Hb^{-1}$

$a^{-1} = b^{-1}h^{-1}$

$= h^{-1}b^{-1} \in Hb^{-1}$

$a^{-1} \in Hb^{-1}$

iv) let $a \in bH$

$x = aH$

$a = bh_2 \cdot x = ah_1$

$x = (bh_2)h_1$

$x = b(h_2h_1) \in bH$

$\therefore aH \subseteq bH$

Now, let $x \in bH$

Then $x = bh_3$ for some $h_3 \in H$.

Also from (i)

$b = ah_2^{-1} \Rightarrow x = bh_3$

$\therefore x = ah_2^{-1}h_3 \in aH$

$\therefore bH \subseteq aH.$

Hence $aH = bH$

Conversly, let $aH = bH$

Then $a = ae \in aH$

$\therefore a \in bH$

Scanned by CamScanner

UNIT-III

Normal Subgroups and Quotient Groups.

Definition:-

A Subgroup H of G is called a normal Subgroup of G. if $aH = Ha$ all $a \in G$.

ex:-

i) For any group G, $\{e\}$ and G are normal Subgroups

ii) In S_3, the subgroup $\{e, P_1, P_2\}$ is normal

iii) In S_3, the subgroup $\{e, P_3\}$ is not a normal Subgroup.

Scanned by CamScanner

Theorem 3.39.

Every subgroup of an abelian group is a normal subgroup.

Proof:

Let G be an abelian group and let H be a subgroup of G. Let $a \in G$.

We claim that $aH = Ha$.

Let $x \in aH$. Then

$x = ah$ for some $h \in H$

$= ha$

$x \in H$. Hence $aH \subseteq Ha$.

Similarly $x = ha$

$= aH$

$aH = Ha$ and hence H is a normal subgroup.

Theorem 3.40:

~~Let H be a subgroup of index 2 in a group G. Then the following are equivalent.~~

Let H be a subgroup of index 2 in a group G. Then H is a normal subgroup of G.

If $a \in H$ Then $H = aH = Ha$.

If $a \notin H$, then aH is a left coset different from H.

Hence $H \cap aH = \phi$

Further, since index of H in G is 2. $H \cup aH = G$.

Hence $aH = G - H$

Similarly $Ha = G - H$ so that $aH = Ha$

Hence H is a normal subgroup of G.

Scanned by CamScanner

Theorem 3.41.

Let N be a subgroup of G. Then the following are equivalent.

(i) N is a normal subgroup of G.

(ii) $aNa^{-1} = N$ for all $a \in G$.

(iii) $aNa^{-1} \subseteq N$ for all $a \in G$.

(iv) $ana^{-1} \in N$ for all $n \in N$ and $a \in G$.

Proof:-

(i) $\Rightarrow$ (ii)

Suppose N is a normal subgroup of G.

$\therefore aN = Na$ for all $a \in G$.

$aNa^{-1} = Naa^{-1} = Ne = N$

(ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (iv) are obvious (iv) $\Rightarrow$ (i)

Suppose that $ana^{-1} \in N$ for all $n \in N$ and $a \in G$.

We claim that $aN = Na$.

Let $x \in aN$.

$x = an$ for some $n \in N$.

$x = (ana^{-1})a \in Na$

$aN \subseteq Na$ ——————→ (1)

Now, let $x \in Na$.

$x = na$ for some $n \in N$.

$x = a(a^{-1}na) = a(a^{-1}n(a^{-1})^{-1}) \in aN$.

$Na \subseteq aN$ ——————→ (2)

From (1) and (2) we get $Na = aN$

Hence N is normal subgroup of G.

Problem :1.

Prove that the intersection of two normal subgroups of a group G is a normal subgroup of G.

Let H and K be two normal subgroups of G. Then $H \cap K$ is a subgroup of G.

Scanned by CamScanner

Now, let $a \in G$ and $x \in H \cap K$. Then $x \in H$ and $x \in K$.

Since H and K are normal $axa^{-1} \in H$ and $axa^{-1} \in K$.

Hence $axa^{-1} \in H \cap K$. Thus $H \cap K$ is a normal subgroup of G.

Problem 2:

The centre H of a group G is a normal subgroup of G.

Sol: The centre H of G is given by

$H = \{x / a \in G \; ax = xa \text{ for all } x \in G\}$

Now, let $x \in H$ and $a \in G$. Hence $ax = xa$.

$x = axa^{-1} \in H$.

Hence H is a normal subgroup of G.

Problem 3:

Let H be a subgroup of G, let $a \in G$. Then aHa^{-1} is a subgroup of G.

Sol: $e = aea^{-1} \in aHa^{-1}$ and hence $aHa^{-1} \neq \phi$

Now, let $x, y \in aHa^{-1}$

Then $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$ where $h_1, h_2 \in H$.

Now, $xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1}$

$= (ah_1a^{-1})(ah_2^{-1}a^{-1})$

$= a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$

aHa^{-1} is a subgroup of G.

Problem 4:

Show that if a group G has exactly one subgroup H of given order, then H is a normal subgroup of G.

Sol: Let the order of H be m.

Let $a \in G$. Then by solved problem 3, aHa^{-1} is also a subgroup of G.

Scanned by CamScanner

we claim that $|H| = |aHa^{-1}| = m$.

Now, consider $f : H \to aHa^{-1}$ defined by $f(h) = aha^{-1}$

f is 1-1, for.

$$f(h_1) = f(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1}$$

$$\Rightarrow h_1 = h_2.$$

f is onto, for let $x = aha^{-1} \in aHa^{-1}$

Then $f(h) = x$. Thus f is a bijection.

$|H| = |aHa^{-1}| = m$.

But H is the only subgroup of G of order m.

$aHa^{-1} = H$. Hence $aH = Ha$.

H is a normal subgroup of G.

Problem 5.

Show that if H and N are subgroups of a group G and N is normal in G. then $H \cap N$ is normal in H. Show that by an example that $H \cap N$ need not be normal in G.

Sol. let $x \in H \cap N$ and $a \in H$

we claim that $axa^{-1} \in H \cap N$.

Now, $x \in N$ and $a \in H \Rightarrow axa^{-1} \in N$.

Also, $x \in H$ and $a \in H \Rightarrow axa^{-1} \in H$.

Hence $axa^{-1} \in H \cap N$

$H \cap N$ is a normal subgroup of H.

The following example shows that $H \cap N$ need not be normal in G.

let $G = S_3$. Take $N = G$ and $H = \{e, (12)\}$

Now $H \cap N = H$ which is not normal in G.

Scanned by CamScanner

Problem :6:

If H is a subgroup of G and N is a normal subgroup of G then HN is a subgroup of G.

Sol To prove that HN is a subgroup of G. It is enough if we prove that $HN = NH$

Let $x \in HN$. Then $x = hn$ where $h \in H$ and $n \in N$.

$x \in hN$.

But, $hN = Nh$

$x \in Nh$

$x \in NH$ Hence $HN \subseteq NH$

Similarly, $NH \subseteq HN$

$HN = NH$.

Hence HN is a subgroup of G.

Problem :7.

M and N are normal subgroups of a group G such that $M \cap N = \{e\}$. Show that every element of M commutes with every element of N.

Sol Let $a \in M$ and $b \in N$

we claim that $ab = ba$.

Consider the element $aba^{-1}b^{-1}$

Since $a^{-1} \in M$ and M is normal $ba^{-1}b^{-1} \in M$

Also $a \in M$, So that $aba^{-1}b^{-1} \in M$

Again since $b \in N$ and N is normal, $aba^{-1} \in N$

Also $b^{-1} \in N$, So that $aba^{-1} \in N$

$aba^{-1}b^{-1} \in M \cap N = \{e\}$

$aba^{-1}b^{-1} = e$ So that $ab = ba$.

Scanned by CamScanner

Theorem 3.42.

A subgroup N of G is normal iff the product of two right cosets of N is again a right coset of N.

Proof: Suppose N is a normal subgroup of G.

Then,

$$NaNb = N(aN)b$$
$$= N(Na)b$$
$$= NNab$$
$$= Nab.$$

Conversely, Suppose that the product of any two right cosets of N is again a right coset of N. Then $NaNb$ is a right coset of N.

Further, $ab = (ea)(eb) \in NaNb$.

Hence $NaNb$ is the right coset containing ab.

$$NaNb = Nab.$$

Now, we prove that N is a normal subgroup of G.

Let $a \in G$ and $n \in N$. Then

$$ana^{-1} = ena a^{-1} \in NaNa^{-1} = Naa^{-1} = N$$
$$ana^{-1} \in N.$$

Hence N is a normal subgroup of G.

Theorem 3.43.

Let N be a normal subgroup of a group G. Then G/N is a group under the operation defined by $NaNb = Nab$.

Proof:

By theorem 3.42. the operation given by $NaNb = Nab$ is a well defined binary operation in G/N.

Now, let $Na, Nb, Nc \in G/N$

Then
$$Na(NbNc) = Na(Nbc)$$
$$= Na(bc)$$
$$= N(ab)c$$
$$= (NaNb)Nc$$

Scanned by CamScanner

The binary operation is associative

$Na \cdot Ne = Nae = Na = NeNa$

Ne is the identity element.

Also, $NaNa^{-1} = Naa^{-1} = Ne = Na^{-1}Na$

$\therefore Na^{-1}$ is the inverse of Na

$\therefore G/N$ is a group.

Definition:

Let N be a normal subgroup of G. Then the group G/N is called the quotient group of G modulo

---

ISOMORPHISM:

Definition:

Let G and G' be two groups. A map $f: G \to G'$ is called an isomorphism if.

(i) f is a bijection.

(ii) $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Two groups G and G' are said to be isomorphic if there exists an isomorphism $f: G \to G'$. If two groups G and G' are isomorphic we write $G \cong G'$.

Theorem 3.2.4.

Isomorphism is an equivalance relation among groups.

Proof:

For any group G. $i_G : G \to G$ is clearly an isomorphism.

Hence $G \cong G$. Therefore the relation is reflexive.

Now, let $G \cong G'$ and let $f: G \to G'$ be an isomorphism

Then f is a bijection

$\therefore f^{-1} : G' \to G$ is also a bijection

Scanned by CamScanner

Now, let $x', y' \in G'$

Let $f^{-1}(x') = x$ and $f^{-1}(y') = y$

Then, $f(x) = x'$ and $f(y) = y'$

$$f(xy) = f(x)f(y) = x'y'$$

$$f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$$

Hence f^{-1} is an isomorphism.

Thus $G' \cong G$ and hence the relation is symmetric

Now, let $G \cong G'$ and $G' \cong G''$.

Then there exist isomorphisms $f: G \to G'$ and $g: G' \to G''$

Since f and g are bijections. $g \circ f: G \to G''$ is also a bijection

Now, let $x, y \in G$. Then.

$$(g \circ f)(xy) = g[f(xy)]$$

$$= g[f(x)f(y)]$$

$$= g[f(x)]\, g[f(y)]$$

$$= (g \circ f)(x)\,(g \circ f)(y)$$

Hence $g \circ f$ is an isomorphism.

Thus $G \cong G''$ and hence the relation is transitive.

∴ Isomorphism is an equivalence relation on groups.

---

5. $(Z_n, \oplus)$ is a group.

Let G denote the set of all n^{th} roots of unity. G is a group under usual multiplication.

We claim that $(Z_n, \oplus) \cong G$.

Consider $f: Z_n \to G$ given by $f(m) = \omega^m$

where $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$

Clearly f is a bijection

Let $a, b \in Z_n$. Let $a+b = qn + r$ where $0 \le r \le n$.

Then, $a \oplus b = r$.

$$f(a \oplus b) = \omega^r \longrightarrow (1)$$

Scanned by CamScanner

Also $f(a)f(b) = \omega^a \omega^b = \omega^{a+b} = \omega^{2n+r}$

$= \omega^{2n}\omega^r = 1\omega^r = \omega^r \longrightarrow (2)$

From (1) and (2) we get.

$f(a \oplus b) = f(a)\, f(b)$

Hence f is an isomorphism.

Theorem 3.45.

Let $f: G \to G'$ be an isomorphism. Then,

(i) $f(e) = e'$ where e and e' are the identity elements of G and G' respectively. (ie) In an isomorphism identity is mapped onto identity.

(ii) $f(a^{-1}) = [f(a)]^{-1}$

Proof

(i) To prove that $f(e) = e'$ it is enough if we prove that $a'f(e) = f(e)a' = a'$ for all $a' \in G'$

Let $a' \in G'$. Since $f: G \to G'$ is a bijection. there exist such that $a \in G$ such that $f(a) = a'$

$a'f(e) = f(a)\, f(e) = f(ae) = f(a) = a'$

similarly.

$f(e)a' = f(e)\, f(a) = f(ea) = f(a) = a'$

$f(e) = e'$

(ii) It is enough to prove that

$f(a)\, f(a^{-1}) = f(a^{-1})\, f(a) = e'$

Now, $f(a)\, f(a^{-1}) = f(aa^{-1}) = f(e) = e'$

Also, $f(a^{-1})\, f(a) = f(a^{-1}a) = f(e) = e'$.

$\therefore f(a)f(a^{-1}) = f(a^{-1})f(a) = e'$

$[f(a)]^{-1} = f(a^{-1})$

Scanned by CamScanner

Theorem 3.46.

Let $f: G \to G'$ be an isomorphism. If G is abelian, then G' is also abelian.

Proof Let $a', b' \in G'$. Then there exists $a, b \in G$ such that $f(a) = a'$ and $f(b) = b'$

Now, $a'b' = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b'a'$

Hence G' is abelian.

Theorem 3.47.

Let $f: G \to G'$ be an isomorphism. Let $a \in G$. Then the order of a is equal to the order of $f(a)$. (ie) Isomorphism preserves the order of each element in a group.

Proof Suppose the order of a is n. Then n is the least positive integer such that $a^n = e$

Now,

$$[f(a)]^n = f(a) \cdot \cdots \cdot f(a)$$
$$= f(a^n) \quad [\text{since } f \text{ is an isomorphism}]$$
$$= f(e) = e'$$

Now, if possible let m be a positive integer such that $0 < m < n$ and $[f(a)]^m = e'$

Then $f(a^m) = [f(a)]^m = e'$

But $f(e) = e'$, since f is 1-1 we have $a^m = e$ which contradicts the definition of the order of a.

n is the least positive integer such that $[f(a)]^n = e'$

The order of $f(a)$ is n.

Theorem 3.48.

Let $f: G \to G'$ be an isomorphism. If G is cyclic then G' is also cyclic.

Scanned by CamScanner

Proof:

Let a be a generator of the group G. We shall prove that $f(a)$ is a generator of the group G'.

Let $x' \in G'$. Since f is a bijection, there exists $x \in G$ such that $f(x) = x'$.

Now, since $G = \langle a \rangle$, $x = a^n$ for some integer n.

Hence $x' = f(x) = f(a^n) = [f(a)]^n$

Since $x' \in G'$ is arbitrary every element of G' is of the form $[f(a)]^n$ so that $G' = \langle f(a) \rangle$

Hence G' is cyclic.

Problem 3.

If G is a group and G' is a set with a binary operation and there exist a one-one mapping f from G onto G' such that $f(ab) = f(a)f(b)$ for all $a, b \in G$. then show that G' is also a group.

Sol Let $a', b', c' \in G'$

Since $f: G \to G'$ is a bijection, there exists $a, b, c \in G$ such that.

$$f(a) = a', \quad f(b) = b', \quad f(c) = c'$$

Since G is a group, $(ab)c = a(bc)$

$$f[(ab)c] = f[a(bc)]$$

$$f(ab)f(c) = f(a)f(bc)$$

$$[f(a)f(b)]f(c) = f(a)[f(b)f(c)]$$

$$[a'b']c' = a'(b'c')$$

The binary operation in G' is associative

Scanned by CamScanner

Now let $e \in G$ be the identity element.
Let $a' \in G'$. Since $f: G \to G'$ is a bijection, there exists $a \in G$ such that $f(a) = a'$

Now, $ae = ea = a$

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

$f(a)f(e) = f(e)f(a) = f(a)$

$a'f(e) = f(e)a' = a'$

$f(e)$ is the identity in G'.

Let $a' \in G'$. Since $f: G \to G'$ is a bijection, there exists $a \in G$ such that $f(a) = a'$

Now, $aa^{-1} = a^{-1}a = e$

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

$a'f(a^{-1}) = f(a^{-1})a' = f(e)$

$f(a^{-1})$ is the inverse of a' in G'.

Hence G' is a group.

Problem 4:

Let C be any group. Show that $f: G \to G$ give by $f(x) = x^{-1}$ is an isomorphism $\Leftrightarrow G$ is abelian

Let $f: G \to G$ given by $f(x) = x^{-1}$ be an isomorphism.

We claim that G is abelian

Let $x, y \in G$.

Then $f(x^{-1}y^{-1}) = f(x^{-1})f(y^{-1})$

$(x^{-1}y^{-1}) = f(x^{-1})^{-1}(y^{-1})^{-1}$

$(y^{-1})^{-1}(x^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$

$yx = xy$

Hence G is abelian.

Scanned by CamScanner

conversely, suppose G is abelian.

clearly $f: G \to G$ given by $f(x) = x^{-1}$ is a bijection.

now, $f(xy) = (xy)^{-1}$

$= y^{-1}x^{-1}$

$= x^{-1}y^{-1}$

$= f(x)f(y)$

f is an isomorphism.

Theorem 3.49. Any infinite cyclic group G is isomorphic to $(\mathbb{Z}, +)$

Proof let G be an infinite cyclic group with the generator a. Then $G = \{a^n / n \in \mathbb{Z}\}$

Define $f: \mathbb{Z} \to G$. by $f(n) = a^n$

since G is infinite $n \neq m \Rightarrow a^n \neq a^m$

Hence f is 1-1, obviously f is onto.

now, $f(n+m) = a^{n+m} = a^n a^m = f(n) f(m)$

Hence f is an isomorphism.

---

corollary: Any two infinite cyclic groups ~~by Theorem 3.49.~~ are morphic to each other.

let G and G' be two infinite cyclic group ~~of order A is isomorphic to $(\mathbb{Z}_n, +)$~~

$G \cong (\mathbb{Z}, +)$ and $(\mathbb{Z}, +) \cong G'$

Thus $G \cong G'$

Scanned by CamScanner

Theorem: 3.50

Any finite cyclic group of order n with is ~~generator~~ isomorphic to $(Z_n, \oplus)$

Proof Let G be a cyclic group of order n with generator a. Then $G = \{e, a, a^2, \ldots, a^{n-1}\}$

Define $f: Z_n \to G$ by $f(r) = a^r$

Clearly f is a bijection

Now, let $r, s \in Z_n$. Let $r \oplus s = t$.

Then $r+s = qn+t$, where $0 \le t < n$

$$f(r \oplus s) = a^{r \oplus s} = a^t \longrightarrow (1)$$

Also,

$$f(r)f(s) = a^r a^s = a^{r+s} = a^{qn+t} = a^{qn} a^t$$

$$= (a^n)^q a^t = e a^t = a^t \longrightarrow (2)$$

From (1) and (2) we get

$$f(r \oplus s) = f(r) f(s)$$

Hence f is an isomorphism.

Theorem 3.51 (Cayley's theorem)

Any finite group is isomorphic to a group of permutation

Proof

Step: 1

Let G be a finite group of order n. Let $a \in G$.

Define $f_a: G \to G$ by $f_a(x) = ax$.

Now, f_a is 1-1, since $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$.

f_a is onto.

$f_a(a^{-1}y) = a(a^{-1}y) = y$.

Thus f_a is a bijection.

Since G has n elements, f_a is just a permutation on n symbols.

Scanned by CamScanner

Let $G' = \{ f_a / a \in G \}$

Step-2. We prove G' is a group. Let $f_a, f_b \in G'$

$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx)$

$= (ab)x = f_{ab}(x)$.

Hence $f_a \circ f_b = f_{ab}$. Hence G_1 is closed under composition of mappings. $f_e \in G'$ is the identity element.

The inverse of f_a in G' is f_a^{-1}.

Step:3. We prove that $G \cong G'$

Define $\phi : G \to G'$ by $\phi(a) = f_a$

$\phi(a) = \phi(b) \Rightarrow f_{ab} = f_a \circ f_b \Rightarrow f_a(x) = f_b(x)$

$\Rightarrow ax = bx \Rightarrow a = b$

Hence ϕ is 1-1. Obviously ϕ is onto.

Also $\phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$

Hence ϕ is an isomorphism.

Definition:

An isomorphism of a group G to itself is called an automorphism of G.

Definition:

The automorphism $\phi_a : G \to G$ defined in example 4 is called an inner automorphism of the group G.

Theorem 3.52. For any group G.

(i) Aut G is a group under composition of functions.

(ii) $I(G)$ is a normal subgroup of Aut G.

Proof (i) Let $f \circ g \in \text{Aut } G$

$\therefore f$ and g are isomorphisms of G to itself

$\therefore f \circ g$ is an isomorphism of G to itself

Scanned by CamScanner

$fog \in Aut\ G_1$.

$f \in Aut\ G_1 \Rightarrow f^{-1} \in Aut\ G_1$.

clearly composition of functions is associative

Hence $Aut\ G_1$ is a group.

(ii) Let $\phi_a, \phi_b \in I(G_1)$. Then

$$(\phi_a \phi_b)(x) = \phi_a(bxb^{-1})$$
$$= a(bxb^{-1})a^{-1}$$
$$= (ab)x(ab)^{-1}$$
$$= \phi_{ab}(x).$$

Hence $\phi_a \phi_b = \phi_{ab} \in I(G_1)$

ϕ_e is the identity element of $I(G_1)$ and the inverse of ϕ_a is $\phi_{a^{-1}}$.

$\therefore I(G_1)$ is a subgroup of $Aut\ G_1$.

We now prove that $I(G_1)$ is a normal subgroup of $Aut\ G$.

Theorem 3.53.

Let G_1 be a cyclic group generated by a. Let $f: G_1 \to G_1$ be a mapping such that $f(xy) = f(x)f(y)$. Then f is an automorphism of G_1 iff $f(a)$ is a generator of G_1.

Proof:

Let f be an automorphism of G_1. We shall prove that $f(a)$ is a generator of G_1.

Case (i) Let G_1 be a finite cyclic group of order n. Then order of a is n. By Theorem, 3.46. $f(a)$ is also an element of order n and hence $f(a)$ is a generator of G_1.

Case (ii) Let G_1 be infinite. Suppose $f(a)$ is not a generator of G_1. Let $H = \langle f(a) \rangle$. Then H is a proper subgroup of G_1.

We claim that $f(G_1) = H$

Let $x' \in f(G_1)$. Then $x' = f(x)$ for some $x \in G_1$.

Now, $x = a^n$ for some n since $G_1 = \langle a \rangle$

Scanned by CamScanner

$x = f(a^n) = [f(a)]^n \in H$

$f(G) \subseteq H$

now let $x \in H$. Then $x = [f(a)^n]$ for some n.

$x = f(a^n)$. Hence $x \in f(G)$

$H \subseteq f(G)$, Hence $f(G) = H$

Since H is a proper subgroup of G. f is not onto which is a contradiction. Hence $f(a)$ is a generator of G.

Conversly let $f: G \to G$ be a mapping such that $f(xy) = f(x) f(y)$ and let $f(a)$ be a generator of G. we shall prove that f is an automorphism.

It is enough if we prove that f is 1-1 and onto

Let $x \in G$. Since $f(a)$ is a generator of G. $x = [f(a)^n]$ for some n.

clearly $f(a^n) = [f(a)]^n = x$. Thus x has a preimage a^n under f. Hence f is onto.

now to prove f is 1-1.

Case (i) G is finite

Since any function from a finite set onto itself is necessarily 1-1 (verify) f is 1-1

case (ii) G is infinite

Let $x, y \in G$ and let $x = a^n$, $y = a^m$ and $n \geq m$.

now, $f(x) = f(y) \Rightarrow f(a^n) = f(a^m)$

$\Rightarrow [f(a)]^n = [f(a)]^m$

$\Rightarrow [f(a)]^{n-m} = e$

$\Rightarrow n - m = 0$

Scanned by CamScanner

Since $f(a)$ is an element of finite order,

$\Rightarrow n = m$

$\Rightarrow a^n = a^m$

$\Rightarrow x = y$.

Hence f is 1-1. Thus f is an automorphism.

Theorem 3.54:
The number of automorphisms of a cyclic group of order n is $\phi(n)$.

Sol Let G be a cyclic group of order of n. Let $a \in G$ be a generator. If $f : G \to G$ is an automorphism then f is completely determined by specifying the image of a. The only possible images of a are any one of the generators of G. Hence the number of automorphisms is equal to the number of generators of G. But the number of generators of a cyclic group of order n is $\phi(n)$. Hence the number of automorphisms of a cyclic grp of order n is $\phi(n)$.

Problem 1.
Construct the group of automorphisms of $(Z_4, \oplus)$

Sol 1 and 3 are the only 2 generators of Z_4. Hence there are only 2 automorphism of Z_4, say f and g. They are given by $f(1) = 1$ and $g(1) = 3$.

Hence Aut $G_1 = \{f, g\} \cong Z_2$.

Problem 2.
Construct the group of automorphisms of $(Z, +)$.

Sol 1 and -1 are the only 2 generators of Z. Hence there are only 2 automorphisms of Z say f and g. They are given by $f(1) = 1$ and $g(1) = -1$. $f(1) = 1$ gives the identity automorphism. $g(1) = -1$ determines the automorphism given by $g(x) = -x$.

Hence Aut $Z = \{f, g\} \cong Z_2$.

Scanned by CamScanner

Problem 2

Let be a finite abelian group of order n and let m be a positive integer relatively prime to n. Then $f : G \to$ defined by $f(x) = x^m$ is an automorphism of G.

Sol Since m and n are relatively prime, there exist integers u and v such that $mu + nv = 1$

Now, let $x \in G$.

Then, $x = x^{mu+nv} = x^{mu} x^{nv} = x^{mu} e = x^{mu}$

Hence, $x = x^{mu}$

Now, $f(x) = f(y) \Rightarrow x^m = y^m$

$\Rightarrow x^{mu} = y^{mu}$

$\Rightarrow x = y$

Hence f is 1-1.

Also $f(x^u) = x^{mu} = x$

Every element x has pre-image x^u under f.

Hence f is onto.

$f(xy) = (xy)^m$

$= x^m y^m$

$= f(x) f(y)$

Hence f is an isomorphism

Problem 4.

Show that $\text{Aut } Z_8 \cong V_4$.

Sol The generators of Z_8 are 1, 3, 5, 7. The four different automorphisms of Z_8 are f_1, f_2, f_3, f_4 given by $f_1(1) = 1$; $f_2(1) = 3$; $f_3(1) = 5$; $f_4(1) = 7$.

We shall now compute $f_2 \circ f_3$

Scanned by CamScanner

Unit - IV

Define : (Rings) :-

A nonempty set R together with binary operations denoted by "+" and "." and called addition and multiplication which satisfy the following axioms is called a ring.

Notation :-

The unique identity of the addition group $(R, +)$ is denoted by 0 and called the "zero elements" of the ring. and the unique additive inverse of a is denoted by $-a$.

Ring of Gaussian Integers :-

Let $R = \{a + ib / a, b \in Z\}$. Then R is a Ring under usual addition & multiplication. This is called the ring of Gaussian Integers.

Null Rings :-

$\{0\}$ with binary operations "+" and "." defined as $0 + 0 = 0$ and $0.0 = 0$ is a ring.

This is called a null ring.

Example :-

The set R of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in R$ is ring under matrix addition and matrix multiplication.

proof :-

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in R$

Then,

$$A+B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R$$

$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+ac) & ac-bd \end{pmatrix} \in R$$

clearly matrix addition is commutative & associative.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ is the zero element

$\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$ is the inverse of the matrix

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

Further matrix multiplication is associative and the distribute laws are valid for 2x2 matrices.

Hence R is ring.

Elementry properties of Rings :-

Theorem 4.1 :-

Let R be a ring and $a, b \in R$. Then.

i) $0a = a0 = 0$ ii) $a(-b) = (-a)b = -(ab)$

iii) $(-a)(-b) = ab$, iv) $a(b-c) = ab - ac$

proof :-

i) $a0 = a(0+0) = a0 + a0$

$\therefore a0 = 0$ (by cancellation law in $(R, +)$)

Similarly $0a = 0$.

(ii) $a(-b) + ab = a(-b+b) = a0 = 0$

$\therefore a(-b) = -(ab)$

Similarly $(-a)b = -(ab)$

(iii) By (ii) $(-a)(-b) = -[a(-b)] = -(-ab) = ab$

(iv) $a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$

problems:

1. If R is a ring such that $a^2 = a$ for all $a \in R$, prove that i) $a+a=0$ ii) $a+b=0 \Rightarrow a=b$ iii) $ab=ba$

proof:

i) $a+a = (a+a)(a+a)$

$= a(a+a) + a(a+a)$

$= aa + aa + aa + aa$

$= (a+a) + (a+a)$ ~~$+(a+a)$~~ (Since $a^2 = a$)

Hence $a+a=0$

ii) Let $a+b=0$

By (i) $a+a=0$

$\therefore a+b = a+a$ so that $a=b$

iii) $a+b = (a+b)(a+b)$

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

$= aa + ab + ba + bb$

$= a + ab + ba + b$

Hence $ab+ba=0$ so that by (ii) $ab = ba$

problem 2:

complete the cayley table for the ring $R = \{a, b, c, d\}$

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			a
d	a	b	c	

Sol:

First we shall compute cb

$cb = (b+d)b$ (from addition table)

$= bb + db$

$= b + b$ (from multiplication table)

$= a$ (from addition table).

Now,

$cc = c(b+d) = cb + cd = a + a = a$

$bc = (b+d)c = cc + dc = a + c = c$

$bd = b(b+c) = bb + bc = b + c = d$

$dd = (b+c)d = bd + cd = d + a = d$

Hence completed table for multiplication

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

Isomorphism:

Def:-

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two rings. A bijection $f: R \to R'$ is called an isomorphism if

i) $f(a+b) = f(a) + f(b)$ and

ii) $f(ab) = f(a) f(b)$ for all $a, b \in R$.

Example:

Let C be the ring of complex number. Let S be the set of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in R$. Then S is a ring under matrix addition. Now the mapping $f: C \to S$ defined by $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an isomorphism

∵ Clearly f is a bijection. Now let $x = a+ib$ and $y = c+id$.

$$f(x+y) = f[(a+c) + i(b+d)]$$

$$= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

$$f(x) + f(y) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

$$= f(x) + f(y)$$

Now $f(xy) = f(x) f(y)$ (verify)

Types of rings

Definition:-

A ring R is said to be commutative if $ab = ba$ for all $a, b \in R$.

Definition :-

Let R be a ring we say that R is a ring with identity if there exists an elements $1 \in R$ such $a1 = 1a = a$ for all $a \in R$.

Theorem :-

In a ring with identity the identity element is unique.

proof :-

Let 1, 1' be multiplicative identities

Then $1.1' = 1'$ (considering 1' as identity)

and $1.1 = 1'$ (considering as identity)

$\therefore 1 = 1'$. Hence the identity element is unique.

Definition :-

Let R be a ring with identity An element $u \in R$ is called a unit in R if it has a multiplication inverse in R. the multiplicative inverse in R. The multiplicative inverse of u is denoted by u^{-1}.

For example in $(Z, +, .)$, 1 and -1 are unit In $M_2(R)$, all the non-singular matrix are units.

In Q, R and every non-zero element is a unit.

Theorem :-

Let R be a ring with identity, the set of all unit in R is a group under multiplication.

Proof :-

Let U denote the set of all units in R.

Clearly $1 \in U$. Let $a, b \in U$,

Here $a^{-1}b^{-1}$ exists in R.

Now, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$

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

Hence $ab \in U$.

Also, $(a^{-1})^{-1} = a$ and hence $a \in U \Rightarrow a^{-1} \in U$.

Hence U is a group under multiplication.

Def :-

Let R be a ring with identity element R is called a skew field or a divisioning is every non-zero element in R is a unit.

Def :-

A commutative skew field is called a field.

In other words a field is a system $(F, +, \cdot)$ satisfying the following conditions.

i) $(F, +)$ is an abelin group.

ii) $(F - \{0\}, \cdot)$ is a an abelian group.

iii) $a.(b+c) = a.b + a.c$ for all $a, b, c \in F$.

Example :-

Let M be the set of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b, c \in M$. Then M is a skew field under matrix addition and matrix multiplication.

Proof:-

Let $A, B \in M$.

Let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$ then

$$A + B = \begin{pmatrix} a+b & b+d \\ -\bar{b}-\bar{d} & \bar{a}+\bar{c} \end{pmatrix}$$

$$= \begin{pmatrix} a+b & b+d \\ \overline{-(b+d)} & \overline{a+c} \end{pmatrix} \in M.$$

Hence M is closed under Matrix addition.

Obviously matrix addition is associative and commutative.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element inverse of

$\begin{pmatrix} -a & -b \\ \bar{b} & -\bar{a} \end{pmatrix}$ is the additive inverse of

$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$.

Hence M is an ~~abtana~~ abelian group under matrix addition.

Now, $AB = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$

$$= \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - a\bar{d} & -bd + \bar{a}c \end{pmatrix}$$

which is of form $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$

Hence M is closed under multiplication.

Further matrix multiplication is associative. and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ is the multiplicative identity.

Now, let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ be a non-zero matrix in M.

Then, either $a \neq 0$ or $b \neq 0$ so that either $|a| > 0$ or $|b| > 0$.

Hence $|A| = a\bar{a} + b\bar{b} = |a|^2 + |b|^2 > 0$.

Thus A is non-singular matrix and hence has a inverse and $A^{-1} \in M$. Thus M is a skew field. Also since matrix multiplication is not commutative M is not a field.

Theorem 4.4

In a skew field R,

i) $ax = ay$. $a \neq 0 \Rightarrow x = y$ } (cancelation laws in rings)

ii) $xa = ya$. $a \neq 0 \Rightarrow x = y$ }

iii) $ax = 0 \Leftrightarrow a = 0$ or $x = 0$.

Proof:-

i) Let $ax = ay$ and $a \neq 0$ since R is a skew field there exists $a^{-1} \in R$.

such that,

$$a a^{-1} = a^{-1} a = 1$$

Hence,

$$ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay)$$
$$\Rightarrow x = y$$

ii) can be proved by

$x = 0$ then clearly $ax = 0$,

Conversely,

Let $ax = 0$ and $a \neq 0$

$\therefore ax = a0$

$\therefore x = 0$ (by (i))

Def:

Let R be a ring. A non-zero element $a \in R$ is said to be a zero divisor if there exists a non-zero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Theorem 4.5:

A ring R has a non-zero divisors iff Cancellation law is valid in R.

Proof:

Let R be a ring without zero divisors.

Let $ax = ay$ and $a \neq 0$.

$\therefore ax - ay = 0$. Hence $a(x-y) = 0$

and $a \neq 0$

$x - y = 0$ (since R has no zero divisors)

$x = y$. Thus cancellation law is valid in

Conversely,

Let the cancellation law be valid in R.

Let $ab = 0$ and $a \neq 0$

Then,

$ab = 0 = a0$

Hence by cancellation law $b = 0$.

Hence R has no zero divises.

Th. 4.6

Any unit in R cannot be a zero divisors.

proof:-

Let $a \in k$ be a unit.

Then,

$ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow b = 0$.

Ily $ba = 0 \Rightarrow b = 0$

Hence a cannot be a zero divisors.

Def:-

A commutative ring with identity having no zero-divisors is called a integral domain.

Thus in a integral domain $ab = 0$

$\Rightarrow$ ~~their~~ either $a = 0$ or $b = 0$.

or equivalently $ab = 0$ and $a \neq 0$.

$\Rightarrow b = 0$; or $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Theorem 4.7

Statement

Z_n is an integral domain iff n is prime.

proof:-

We claim that n is prime

Suppose n is not a prime

then $n = pq$ where $1 < p < n$ & $1 < q < n$

clearly $p \odot q = 0$

Hence p & q are zero divisors.

$\therefore Z_n$ is not an integral domain which is a contradiction

Hence n is prime

Conversely,

Suppose n is prime, Let $a, b \in Z_n$

$\Rightarrow n / ab$

$\Rightarrow n / a$ or n / b (since n is prime)

$\rightarrow a = 0, b = 0$

$\therefore Z_n$ has no zero divisors also Z_n is a commutative ring with identity.

Hence Z_n is an integral domain.

Theorem 4.8 :-

Any field F is an integral domain.

proof :-

It is enough if we P.T F has non-zero divisors.

Let $a, b \in F$, $ab = 0$ & $a \neq 0$.

Since F is a field a^{-1} exists Now $ab = 0 = a0$

$\Rightarrow b = 0$

$\therefore$ F has no zero divisors.

Hence F is an integral domain.

Note :-

The converse of the above theorem is not true (ie) an integral domain need not be a field.

For example :-

Z is an integral domain but not a field.

Theorem :-

Let R be a commutative ring with identity 1. Then R is a integral domain iff the set of non-zero elements in R is closed under multiplication.

Proof :-

Let R be a integral domain

Let $a, b \in R - \{0\}$

Since R has no zero divisors $ab \neq 0$ so that $R - \{0\}$ is closed under multiplication.

conversly,

Suppose, $R-\{0\}$ is closed under multiplication Then the product of any two non-zero elements is a non-zero elements.

Hence R has no zero divisors.

So that R is an integral domain

Theorem:-

Any finite integral domain is field.

Proof:-

Let R be a finite integral domain. we need only to prove that every non-zero element in R has a multiplicative inverse.

Let $a \in R$ and $a \neq 0$.

Let $R = \{0, 1, a_1, a_2, \ldots a_n\}$

consider $\{a, aa_1, aa_2 \ldots aa_n\}$

By the above theorem all these elements are non-zero and distinct.

Hence $aa_i = 1 \quad \forall a_i \in R$.

Since R is commutative

$aa_i = a_i a = 1$ so that $a_i = a^{-1}$

Hence R is a field.

Theorem :- (10m).

Z_n is a field iff n is prime.

proof:-

By theorem 4.7, Z_n is a integral domain iff n is prime.

Further Z_n is finite.

Hence the result follows. The theorem.

Theorem:-

A finite commutative ring R without zero-divisors is field.

proof:-

If we prove that R has an identity element then R becomes an integral domain and hence by theorem 4.11. It is a field so we prove the existence of identity.

Let $R = \{0, a_1, \ldots, a_n\}$

Let $a \in R$ and $a \neq 0$,

Then the elements $aa_1, aa_2 \ldots aa_n$, are distinct and non-zero.

$\therefore aa_i = a$ for some i.

Since R is commutative we have $aa_i = a_i a =$

We now prove that a_i is the identity element of R.

Let $b \in R$. Then $b = aa_j$ for some j.

$\therefore a_i b = a_i (aa_j) = (a_i a) = a_j = aa_j = b$.

Thus $a_i b = ba_i = b$.

Since $b \in R$ is arbitrary, a_i is the identity of R.

Hence the theorem.

Problem:-

1. Prove that the set F of all real numbers of the form $a + b\sqrt{2}$ where $a, b \in Q$ is a field under the usual addition and multiplication of real numbers.

Sol:

Obviously, $(F,+)$ is an abelian group with 0 as the zero element.

Now, let $a+b\sqrt{2}$ and $c+d\sqrt{2} \in F$, then

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in F$

Since the two binary operations are the usual addition and multiplication of real numbers multiplication is associative and commutative and the two distribute laws are true.

$1 = 1+0\sqrt{2} \in F$ and is the multiplicative identity.

Now, let $a+b\sqrt{2} \in F - \{0\}$

Then a and b are not simultaneously 0

Also $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$

We claim that $a^2-2b^2 \neq 0$.

Case(i): $a \neq 0$ and $b \neq 0$. Then $a^2-2b^2 = a^2 \neq 0$

Case(ii): $a = 0$ and $b \neq 0$, then $a^2-2b^2 = -2b^2 \neq 0$.

Case(iii): $a \neq 0$. $b \neq 0$ suppose $a^2-2b^2 = 0$.

Then $a^2 = 2b^2$ so that $\frac{a^2}{b^2} = 2$

Hence $\frac{a}{b} = \pm\sqrt{2}$

Now, $\frac{a}{b} \in \mathbb{Q}$ and $\sqrt{2} \notin \mathbb{Q}$

This is contradiction,

Hence $a^2-2b^2 \neq 0$.

$\therefore \frac{1}{a+b\sqrt{2}} = \left(\frac{a}{a^2-2b^2}\right) - \left(\frac{b}{a^2-2b^2}\right)\sqrt{2} \in F$

and is the inverse of $a+b\sqrt{2}$

Hence F is a field.