PAGE NO. 11
DATE / /

4. Prove that the set of n^{th} roots of unity form an abelian group under multiplication.

Let $G_1 = \{e^{\frac{i2r\pi}{n}},\ r = 0, 1, 2, \ldots, (n-1)\}$

To proove G_1 is an abelian group, we verify the following group axioms (properties)

(i) Closure Property :-

Let $a = e^{\frac{2r_1\pi i}{n}}$, $b = e^{\frac{2r_2\pi i}{n}}$ where $0 \le r_1 \le n-1$, $0 \le r_2 \le n-1$ be two arbitary elements of G_1

$\therefore ab = e^{\frac{2(r_1+r_2)\pi i}{n}}$ ——— (1)

If $0 \le r_1 + r_2 \le n-1$ then obviously $ab \in G_1$

If $r_1 + r_2 > n-1$

Taking maximum value of r_1 and r_2 as $n-1$

$\therefore r_1 + r_2 = n-1 + n-1 = n+n-2$

From (1)

$$ab = e^{\frac{2(n+n-2)\pi i}{n}}$$

$$= e^{\frac{2n\pi i}{n} + \frac{2(n-2)\pi i}{n}}$$

$$= e^{2\pi i} \cdot e^{\frac{2(n-2)\pi i}{n}}$$

$$= e^{\frac{2(n-2)\pi i}{n}} \in G_1 \quad \{\because e^{2\pi i} = 1\}$$

$\therefore$ Closure Property hold in G_1.

or G_1 is closed under multiplication.

(ii) Since the elements of G_1 are either real or complex so they must obey Associative law.

(iii) Existence of identity element: The identity element is $e^{\frac{2n\pi i}{n}} = 1$

[Since $e^{\frac{2r\pi i}{n}} \times 1 = 1 \times e^{\frac{2r\pi i}{n}} = e^{\frac{2r\pi i}{n}}$]

(iv) Existence of inverse' → The inverse of $e^{\frac{2r\pi i}{n}} \in G_1$ is $e^{\frac{2(n-r)\pi i}{n}} \in G_1$

Since $e^{\frac{2r\pi i}{n}} \cdot e^{\frac{2(n-r)\pi i}{n}} = e^{\frac{2n\pi i}{n}} = e^{2\pi i} = 1$

and $e^{\frac{2(n-r)\pi i}{n}} \cdot e^{\frac{2r\pi i}{n}} = 1$

from (i) and (iv), it follows that G_1 is a group under multiplication.

G_1 is also abelian, since the elements of G_1 are either real or complex so they must obey the commutative law.

—×—

Q: If a and b be two elements of a group G then Prove that $(ab)^2 = a^2b^2$ iff G is commute (abelian).

Ans: Let G_1 be abelian group.

To prove $(ab)^2 = a^2b^2$

$\therefore (ab)^2 = (ab)(ab)$

$= a\{b(ab)\}$ [by Associative law]

$= a[(ba)b\}$ [" " "]

$= a[(ab)b]$ [$\because G_1$ is abelian]

$= a[a(bb)]$ [by Associative law]

$= (aa)(bb)$

$= a^2b^2$

Converse:—

Let $(ab)^2 = a^2b^2$

To prove G is abelian

$\because (ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a\{b(ab)\} = a\{a(bb)\}$ [by associative law]

$\Rightarrow b(ab) = a(bb)$ [by left cancellation law]

$\Rightarrow (ba)b = (ab)b$ [by Ass. law]

$\Rightarrow ba = ab$ [by right cancellation law]

$\Rightarrow$ G is abelian.

Q: If G is a group such that $(ab)^m = a^m b^m$ for three consecutive integers m and for all ($\forall$) $a, b \in G$ show that G is abelian.

Ans → Suppose G is a group and $a, b \in G$ are arbitary such that

$(ab)^m = a^m b^m$ for three consecutive integers.

To prove G is abelian.

Let $(ab)^m = a^m b^m$ ——①

$(ab)^{m+1} = a^{m+1} b^{m+1}$ ——②

and $(ab)^{m+2} = a^{m+2} b^{m+2}$ ——③

From ③,

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

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

$\Rightarrow a^{m+1} b^{m+1} ab = a^{m+1}(ab^{m+1})b$ [by ②]

$\Rightarrow a^{m+1}(b^{m+1}a)b = a^{m+1}(ab^{m+1})b$ [By ass. law]

$\Rightarrow b^{m+1}a = ab^{m+1}$ [by left and right cancellation law]

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

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

$\Rightarrow (a^m b^m)(ba) = (a^m a)(b^m b)$

$\Rightarrow (ab)^m (ba) = a^{m+1} b^{m+1} = (ab)^{m+1}$ {using ① + ②}

$\Rightarrow (ab)^m (ba) = (ab)^m ab$

$\Rightarrow ba = ab$ [by left cancellation law]

$\Rightarrow G_1$ is abelian.

Order of a group → The number of elements of a group is called its order. If a group containing finite number of elements then group is called of finite order and of a group contains infinite numbes of elements then order of group is infinite.

Order of an element :- If G_1 be a group and $a \in G_1$, then order of a is said to be n if n is the least (+ve) integer such that $a^n = e$, where e is the identity element of the group.

Ex- (i) $G_1 = \{1, \omega, \omega^2\}$ is a group under multiplication

order of $\omega = 3$

order of $\omega^2 = 3$

(ii) $G_1 = \{1, -1, i, -i\}$ is a group.

order of $-1 = 2$

order of $i = 4$

order of $-i = 4$

Note (i) Order of $a = O(a)$
(ii) Order of $G_1 = O(G_1)$
(iii) Order of $e = 1$

Idempotent element - If G_1 be a group and $a \in G_1$, Then a is said to be idempotent element of G_1
if $O(a) = 2$ i.e $a^2 = e$

Idempotent group - The group G_1 said to be idempotent if $O(a) = 1$ (or $a^2 = e$) $\forall a \in G_1$

Q Theorem - If a group G is such that each element except identity element of order two, then Prove that G must be abelian

or,

If G be a group and $a^2 = e \ \forall a \in G$ then Prove that G is abelian

or

P.T. idempotent Group is a abelian group.

Ans → Let a and b be any two elements of a group G whose identity element is e.
To prove G_1 is abelian.
$\because \ a, b \in G$
$\Rightarrow \ ab \in G$ [by closure Property]
$\Rightarrow \ a, b, ab \in G_1$
$\therefore a^2 = e, \ b^2 = e, \ (ab)^2 = e$
$\therefore \ a^2 = e$
$\Rightarrow \ aa = e$
$\Rightarrow \ a^{-1}(aa) = a^{-1}e$, where a^{-1} is inverse of a
$\Rightarrow \ (a^{-1}a)a = a^{-1}$

$\Rightarrow ea = a^{-1}$

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

Similarly,

$b = b^{-1}$

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

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

$\Rightarrow ab = ba$

$\Rightarrow G$ is abelian. //

Q. Find the order of every element in the multiplicative group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$ the identity element of the given group is e.

Sol: The identity element of the given group is

$a^6 = e$

$\because a^6 = e \Rightarrow O(a) = 6$

$\because (a^2)^3 = a^6 = e \Rightarrow O(a^2) = 3$

$\because (a^3)^2 = a^6 = e \Rightarrow O(a^3) = 2$

$\because (a^4)^3 = a^{12} = e^2 = e \Rightarrow O(a^4) = 3$

$\because (a^5)^6 = (a^6)^5 = e^5 = e \Rightarrow O(a^5) = 6$

~~and $(a^5)^n \neq e$ for any $n < 6$~~

$(a^6)^1 = a^6 = e \Rightarrow O(a^6) = 1$

Thus the orders of elements $a\ a^2\ a^3\ a^4\ a^5\ a^6$ are $6, 3, 2, 3, 6,$ resp.

Note: (1) $m = nq + r$, where $n > r$

where q is integers
r = reminder and $0 \leq r < n$

(2) $a^0 = e$