19/2/18

B.C. Sir Class

Proposition-① Let G be a group & $a \in G$. Then a^{-1} is unique

Let a' and a'' be two inverses of a.

$\therefore a * a' = e = a' * a$

and $a * a'' = e = a'' * a$.

Now

$a' = a' * e$ → identity element

$= a' * (a * a'')$

$= (a' * a) * a''$ (by associative law)

$= e * a''$

$= a''$

Hence proved

Proposition: Let, G be a group & $a, b \in G$
Then $(a*b)^{-1} = (b^{-1} * a^{-1})$

Proof: Now $(a*b) * (b^{-1} * a^{-1})$

$= a * (b * b^{-1}) * a^{-1}$ (by Associativity)

$= (a * e) * a^{-1}$ ('e' is the identity element in G under $*$)

$= a * a^{-1}$

$= e$.

Again $(b^{-1} * a^{-1}) * (a * b)$

$= b^{-1} * (a^{-1} * a) * b$

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

$= (b^{-1} * e) * b$

$= b^{-1} * b$

$= e$

$\therefore (a*b)^{-1} = (b^{-1} * a^{-1})$

—x—

Proposition: Let G be a group & $a, b \in G$
Then $a*x = b$ or $y*a = b$ has unique solution in G for the unknowns x & y

P.T.P.: (1) There exists a solution in the Group
(2) The solution is Unique.

Proof: Let us consider $a * x = b$
Since $a \in G$, a^{-1} exists uniquely in G.

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

$\Rightarrow (a^{-1} * a) * x = a^{-1} * b$ (by Associativity)

$\Rightarrow e * x = a^{-1} * b$

$\Rightarrow x = (a^{-1} * b)$ (by Closure property)

$\therefore a$ is a B.O. & a^{-1} is unique, b is given

$\therefore (a^{-1} * b)$ is also unique

$\therefore x$ is unique.

—x—

Proposition: Let G be a group and $a, b, c \in G$

Then (i) $a * b = a * c \Rightarrow b = c$ (Left Cancellation Law)

(ii) $b * a = c * a \Rightarrow b = c$ (Right Cancellation Law)

For Cancellation → $*$ should be associative & the inverse should exist

Since $a \in G$, a^{-1} exists.

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

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

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$.

—×—

Proposition: Let G be a group & $a \in G$

Then $a * G = G$ where $aG = \{a * g : g \in G\}$

↓

Means (a) is operated with all elements in (G)

∴ (a) will be operated with itself also.

R.T.P. $aG = G$ → Equality of 2 sets.

To prove 2 sets are equal: prove each set is a subset of the other.

Let, $p \in aG$. Then $p = ag$ for some $g \in G$

Since $a, g \in G$, $ag \in G$ (by closure property)

(Doesn't mean product. Means (a) operated with an element in (G))

$\therefore p \in G$.

This implies that $aG \subseteq G$ → (1)

Now let $q \in G$. Then there exists a unique x in G, s.t. $q = ax \in aG$

↓ Proved earlier today

This implies that $G \subseteq aG$ → (2)

From (1) & (2)

$aG = G$

aG → ~~aaa~~ doesn't mean product of (a) & (G)

→ Means (a) is operated with all elements in (G)

—×—

Finite Group → Speciality: For some (m, k)
Identity element $a^m = a^k$
$a^{m-k} = e$

Let, G be a group & $a \in G$ Then 'a' is said to be of finite order if $\exists$ at least one integer (n) such that $a^n = e$.
The smallest positive of all such (n) is called the order of (a).

Eg: $\{1, -1, i, -i\}$ is my structure

$i^4 = 1$, $i^8 = 1$, $i^{16} = 1$
$i^{-4} = 1$

∴ Order of $i = 4$ → denoted by $O(a)$

Order of $1 = 1$
Order of $-1 = 2$ $[\because (-1)^2 = 1]$
Order of $-i = 4$.

If G is finite then the group G^* is a finite group & the no. of elements in G is called the Order of G.

Proposition

Theorem: Let G be a group and $a \in G$ Then
i) $O(a) = O(a^{-1})$
ii) if $O(a) = u$ and $a^m = e$
then (u) is a divisor of m.
iii) if $O(a) = u$, then $a, a^2, a^3, \ldots a^u (= e)$ are all distinct
iv) if $O(a) = u$, then $O(a^p) = u$, iff 'p' is prime to u.

Eg. in $\{Z_8, +\}$ → Order of $3 =$ Order of $5 = 8$
Order of $2 =$ Order of $6 = 4$.

2 is inverse of 6.
∴ $2 * 6 = 2 + 6 = 8$; $8 \bmod 8 = 0$ identity element

$O(1) = 8$, $O(7) = 8$ ← 1 & 7 are inverse of each other

v) if $O(a)$ is infinite and p is +ve integer then $O(a^p)$ is infinite.

iv) $O(3) = 8$.
$O(5) = 8$.

$O(3^7) = 5$ ∵ 7 is prime to 8

Proof (i) Let, $o(a) = m$.

$\therefore a^m = e$ → identity element

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

$\Rightarrow (a^{-1})^m = e \rightarrow (1)$

~~This does.~~ $o(a)$ means smallest positive integer.

So (1) doesn't guarantee (m) is smallest

Let $(n \in N)$ & $n < m$, s.t. $a^n = e$

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

~~From (1)~~ $a^{+m} = e$.

$a^m \cdot a^{-n} = e \cdot e$

$\Rightarrow \boxed{a^{m-n} = e} \rightarrow (2)$

Now $(m-n) > 0$ $\because n < m$ (assumed)

We had assumed $a^m = e$

But $m - n < m$

$\therefore o(a)$ can't be m

So there cannot be any positive integer less than (m) which can be order of a

$\therefore$ (2) Contradicts our assumption.

Proof (ii): By division algorithm

$m = qu + r$

for some $q, r \in Z$ and $0 \leq r < (u-1)$

take $a = 2$

$u = 8$

$e = 0$

$m = 8$

$2^u = 8$

$a^m = a^{qu+r}$

$\Rightarrow e = (a^u)^q \cdot a^r$

$= e^q \cdot a^r$

$\boxed{e = a^r}$

There are 2 possibilities: $r = 0$ or $r = 1, \ldots (u-1)$

'r' can't be any one of $\{1, 2, \ldots (u-1)\}$

(u) is order of (a)

$\therefore$ 'r' can't be less than (u)

r is positive

$\therefore (r = 0)$ → only possibility.

$\therefore m = qu$

$\therefore$ 'u' divides 'm'.

Proof (iii) $O(a) = n$.

Let us assume (p, q) both being least $\leq n$ such that $a^p = a^q$

$\therefore a^{p-q} = e$

Now if $p > q$ $\therefore p - q > 0$ & $p - q < n$

We assumed $p \& q < n$

$\therefore$ [illegible] $\therefore a^{p-q} = e$.

it contradicts

$\therefore a, a^2, a^3, \ldots a^n$ are all distinct

—X—

21/2/18