409 ✱ Existence of Cancellation laws

If $a, b, c \in G$ then

(i) $ab = ac \Rightarrow b = c$ (Left Cancellation law)

(ii) $ba = ca \Rightarrow b = c$ (Right Cancellation law)

Proof → G is a group so $a^{-1} \in G$

Here $ab = ac$

multiplying by a^{-1}

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

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

$\Rightarrow eb = ec$ [existence of inverse element]

$\Rightarrow b = c$ [" " identity element]

(ii) Again multiplying both sides of $ba = ca$ by a^{-1}

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

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$ [by Associative axiom]

$\Rightarrow be = ce$ [existence of inverse element]

$\Rightarrow b = c$ [By identity axiom]

Hence proved

4|0 **Solvability of equations in a group and uniqueness of solutions**

Prove that the equations
(i) $ax = b$ and
(ii) $ya = b$
have unique solutions in the group G, where $a, b, x, y \in G$.

Proof → Here $ax = b$
Put $x = a^{-1}b$
$\Rightarrow a(a^{-1}b) = b$ (Associative axiom)
$\Rightarrow (aa^{-1})b = b$ (existence of inverse elements)
$\Rightarrow eb = b$ (existence of identity element)
$\Rightarrow b = b$
Thus the equation $ax = b$ is satisfied by $x = a^{-1}b$, Also $a^{-1} \in G$,
Since $a^{-1} \in G$ and $b \in G$
Now we have to prove that the solution is unique.
we assume x_1 and x_2 be two solutions of $ax = b$
then $ax_1 = b$ and $ax_2 = b$
$\therefore ax_1 = ax_2$
or $x_1 = x_2$ (By Cancellation law)
Thus we observe that $a^{-1}b$ is a Unique solution of the equation $ax = b$.
Similarly we can show that the equation $ya = b$ has a unique solution ba^{-1}.

#411 order of an element of a group.

The order of an element a of a group (G, o) is the least positive integer n such that $a^n = e$, the identity element of group where $a o a o a o a o a o \ldots \ldots$ upto n times is denoted by a^n.

The order of an element a is denoted by $o(a)$.

If there is no such positive integer n such that $a^n = e$ then the order of the element a is zero (or infinite). order of identity element is 1.

Ex → (1) $G = \{1, -1, i, -i\}$ is a group under multiplication of complex numbers and its identity element = 1

$i^4 = 1$, so the order of i is 4 $\Rightarrow o(i) = 4$

$(-i)^4 = 1$, so the order of $-i$ is 4 $\Rightarrow o(-i) = 4$

$(1)^1 = 1$, so the order of 1 is 1 $\Rightarrow o(1) = 1$

$(-1)^2 = 1$, so the order -1 is 2 $\Rightarrow o(-1) = 2$

Ex→2 In the infinite multiplicative group of non-zero rational numbers, the order of every element except the elements 1 and -1 is infinite.

→ we have $(-1)^1 = -1$, $(-1)^2 = 1$ (identity element)

$\therefore o(-1) = 2$

Now $2^1 = 2$, $2^2 = 4$, $2^3 = 8$ and .....

Thus there exists no positive integer n such that $2^n = 1$ (identity element)

So $o(2)$ is infinite.

412

* Prove that the order of every element of a finite group is finite.

Proof → Let a be an element of finite group G.
Suppose that all positive integral powers of a ∈ G.
i.e. $a, a^2, a^3, \ldots \in G$.
But the group G is finite so the elements $a, a^2, a^3, \ldots$ must be finite.
Hence $a, a^2, a^3, \ldots$ Cannot be all different elements.
Otherwise the group will be infinite.
Now suppose that

$a^m = a^n$, $m > n \Rightarrow m-n > 0$

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

$\Rightarrow a^{m-n} = a^{n-n} = a^0$

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

$\Rightarrow a^p = e$, where $m-n = p > 0$

Again if $a^r = a^s$, $r > s \Rightarrow r-s > 0$

Similarly as above we get

$a^q = e$, where $r-s = q > 0$

. . . . . .

Thus we get $a^p = e$ $a^q = e$ . . . . .

Now the set of positive Integers p, q . . . . must Contain a least positive number, z such that $a^z = e$

It shows that the order of $a \in G$ is finite.

4.13 ✱ Prove that the order of an element of a group is always equal to the order of its inverse.

(or) Prove that $O(a) = O(a^{-1}) \; \forall \; a \in G$.

Proof:

Let G be a group and $a \in G$

Let a^{-1} be the inverse of G and $a^{-1} \in G$

Let $O(a) = r$ and $O(a^{-1}) = s$

then from the definition of order of an element in a group

$$a^r = e$$

& $$(a^{-1})^s = e$$

we know that the order of any power of an element of a group cannot exceed the order of the element.

So $O(a^{-1}) \leq O(a)$

$\Rightarrow s \leq r$

$\because (a^{-1})^s = e$

$\Rightarrow a^{-s} = e$

$\Rightarrow a^{-s} \cdot a = ea$

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

$\Rightarrow a^{(1-s)} = a$ (by identity axiom)

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

This reflects that a is equal to some power of a^{-1}.

$\therefore O(a) \leq O(a^{-1})$

$\Rightarrow r \leq s$

we have shown that $s \leq r$ and $r \leq s$

So we get $r = s$

4|4 * Prove that the orders of ab and ba are equal for all $a, b \in G$

or

$o(ab) = o(ba) \quad \forall\ a, b \in G$.

Proof: we have

$a^{-1}(ab)a = (a^{-1}a)(ba)$ [By associative axiom]

$\Rightarrow a^{-1}(ab)a = e(ba)$ [By inverse axiom]

$= ba$ [By identity axiom]

we know that the order of ab = the order of $a^{-1}(ab)a$

So $o(ab) = o(ba)$

* Prove that a group G is abelian if every element of G (except the identity e) is of order two.

Proof: Let $a, b \in G$, where a and b are of order two.

$\therefore a^2 = e \quad \cdots (1)$

$\therefore b^2 = e \quad \cdots (2)$

Again $a, b \in G$, So, ab must be of order two

$(ab)^2 = e \quad \cdots (3)$

or $(ab)(ab) = e$

or $a(ba)b = e$ [Associative axiom]

or $a[a(ba)b]b = aeb$

or $(aa)(ba)(bb) = ab$ [Associative and identity axiom]

or $a^2(ba)b^2 = ab$

or $e(ba)e = ab$ [from (1) & (2)]

or $ba = ab$ [By identity axiom]

So $ab = ba$

which shows that the group G is abelian