Lectured By Dr. H.K. Yadav
Deptt. of Mathematics, Maruden College, DBU.
B.Sc-part-I(H), paper-I, Date- 20-05-2020.
Algebra.

Q.1. State and prove Lagrange's theorem.

Soln: Statement: → The order of a sub-group H of a finite group G is a divisor of the order of G.

Proof: Let the order of the finite group G be n and the order of its sub-group H be m.

Let m members of H be

$h_1, h_2, h_3 \ldots h_m$

and let $a \in G$ but $\notin H$.

Then, $h_1a, h_2a, h_3a, \ldots h_ma$ are m elements of Ha.

It is clear that these elements are all different, for

$$h_ia = h_ja \Rightarrow h_iaa^{-1} = h_jaa^{-1}$$
$$\Rightarrow h_i = h_j$$
$$\therefore h_ia \neq h_ja$$

Since, G is finite, therefore, the number of such cosets is also finite.

Let K be the number of disjoint right cosets.

$\therefore G = H \cup Ha_1 \cup Ha_2 \ldots \cup Ha_K$.

∴ the total number of elements of G = number of elements in the K cosets

i.e. $n = mK$, as each coset contains m elements.

i.e. order of G = (order of H).K.

Hence, the order of a sub-group is a divisor of the order of the group.

Ajanta Oxford

B.Sc-part-I(H), paper-I. 29-05-2020.

Q.2. Show that the set E of even integers is a subgroup of the group Z of integers under ordinary addition.

Soln: It is given that $(Z, +)$ is a group of integers under ordinary addition.

Here, the set E = the set of even integers

$= \{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$

Then obviously $E \subseteq Z$.

Now, we shall prove that E forms a group under ordinary addition.

Let us apply the postulates of group to E.

(I) We find that $2+4=6$, $6+8=14$, ... That is, the sum of any two even integers is an even integer.

Hence, the set of even integers is closed with respect to addition. [by closure property]

II obviously $2+(4+6)=(2+4)+6$.

$12+(14+20)=(12+14)+20$. etc.

That is, the addition of even integers is associative. [Associative property]

(III) The number 0 is even. Also we have

$0+2=2=2+0$, $0+8=8=8+0$, etc.

The identity element is zero. [Identity property]

(IV) We find that $(-2)-2=0=2+(-2)$;

$(-6)+6=0=6+(-6)$. etc.

The inverse of every even integer exists and it belongs to the set E. [Inverse property]

Since, all the postulates of group are satisfied by E, therefore, the set E forms a group with respect to addition.

Q.3. Show that $(Z, +)$ is an infinite cyclic group, where Z is the set of integers.

Soln: The group of integers under addition can be generated by the single elementic set {1}. For example, 8 can be expressed as $8(1)$ - 17 can be expressed as $(-17)(1)$, etc.

Again, the group $(Z, +)$ can be generated by (-1). obviously $(Z, +)$ is an infinite cyclic group.

Q.4. State and prove Fermat's Theorem:

Soln: Statement: → If a is any integer and p is prime, then $a^p = a \pmod p$.

proof: If $a = 0$, then theorem is obviously true.

If $a \neq 0$. Let G be the multiplicative group of residue classes modulo p, then G contains $(p-1)$ distinct elements namely

$$[1], [2], \ldots, [p-1]$$

$\Rightarrow o(G) = p-1$ and $[e] = 1$, by this theorem, we have,

$$[a^{p-1}] = [1] \Rightarrow a^{p-1} \equiv 1 \pmod p$$

Now, since p is prime. Hence

$$a^{p-1} \cdot a \equiv 1 \cdot a \pmod p \Rightarrow a^p \equiv a \pmod p$$

Proved.

Q.5. State and prove Euler's Theorem.

Soln: Statement: → If n is a positive integer and a is any integer relatively prime to n, the

$$a^{\phi(n)} \equiv 1 \pmod n$$

proof: Let us suppose $[x]$ denote the residue class of the set of integer mod n, for any integer-n.

Now, we have, the residue classes G is a group of order $\phi(n)$ with identity element, residue class $[1]$.

Now, we have

$$[a] \in G \Rightarrow [a]^{o(G)} = [1] \Rightarrow [a]^{\phi(n)} = [1].$$
$$\Rightarrow [a][a] \ldots \text{upto } \phi(n) \text{ times} = [1]$$
$$\Rightarrow [a \cdot a \ldots \text{upto } \phi(n) \text{ times}] = [1].$$
$$\Rightarrow [a^{\phi(n)}] = [1]$$
$$\Rightarrow a^{\phi(n)} = 1 \pmod n.$$

Q.6. Define Homomorphism and Isomorphism with example.

Soln: Homomorphism: → Let (G, o) and $(G', *)$ be two groups. Then a mapping $f: G \to G'$ is called a homomorphism if

$$f(x \circ y) = f(x) * f(y) \quad \forall\ x, y \in G.$$

Here, we say that f preserves compositions in G and G'.

Rest part of Q. 6. B.Sc. Part-I(H), Paper-I, 20-5-2020

Isomorphism: → Let (G, o) and $(G', *)$ be any two groups.

"A one-one onto map $f: G \to G'$ is called an isomorphism iff

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

Here, we say that G is ~~isomorphic~~ isomorphic to G' and can be written as

$G \cong G'$.

We also say that G is isomorphically mapped onto G' and G and G' are isomorphic groups.

For example: If R is the additive group of real numbers and R^+ is the multiplicative group of positive real numbers then the mapping

$f: R \to R^+$ defined by $f(x) = e^x$, $\forall x \in R$ is an isomorphism.

Q.7: If f is a homomorphism of a group G into a group G' then

(I) $f(e) = e'$ where e is the identity of G and e' is the identity of G'. (II) $f(x^{-1}) = [f(x)]^{-1}$, $\forall x \in G$

(III) If the order of element $x \in G$ is finite, then the order of $f(x)$ is a divisor of the order of x.

Proof: (I) Let $x \in G \Rightarrow f(x) \in G'$

Let us consider $f(x)e' = f(x)$ [$\because$ e' is the identity of G']

$= f(x)e$ [$\because$ e is the identity of G]

$= f(x) \cdot f(e)$ [By structure preserving property of f]

$\Rightarrow f(x)e' = f(x)f(e)$

$\Rightarrow e' = f(e)$ [By left cancellation law in G']

(II) Let $x \in G \Rightarrow x^{-1} \in G$, we have

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

Thus, $f(x) f(x^{-1}) = e'$, where e' is the identity of G' which implies $[f(x)]^{-1} = f(x^{-1})$.

(III) Let $x \in G$ and $o(x) = m$ so that $x^m = e$. Then

$f(x^m) = f(e) \Rightarrow f(x x x \ldots m \text{ times}) = e'$

$\Rightarrow f(x) f(x) \ldots m \text{ times} = e'$

$\Rightarrow [f(x)]^m = e'$

$\Rightarrow o(f(x)) \mid m$ [$\because x^m = e \Rightarrow o(x) \mid m$]

$\Rightarrow o(f(x)) \mid o(x)$

Thus, the order of $f(x)$ is a divisor of the order of x.

Proved.