Lagrange's Theorem

06 October 2020 09:39

Corollary

Groups of prime order are cyclic

Proof: Let G be a group and $|G| = p$ (prime)

Now, let $a \in G$ and $a \neq e$.

Then $\langle a \rangle$ is a subgroup of G.

$\Rightarrow |\langle a \rangle|$ divides $|G|$

$\Rightarrow |\langle a \rangle|$ divides p

$\Rightarrow |\langle a \rangle| = 1$ or p

$\Rightarrow |\langle a \rangle| = p \quad (\because a \neq e)$

$\Rightarrow |\langle a \rangle| = |G|$

$\Rightarrow |a| = |G| \Rightarrow G$ is cyclic.

Note: (1) A group G of order n is cyclic if and only if G has an element of order n.

i.e. if $\exists\, a \in G$ s.t.

i.e. if $\exists\, a \in G$ s.t.

$|G| = |a| = n$, then G is cyclic and $G = \langle a \rangle$.

② A finite set G is a group iff it is closed and associative.

<u>Corollary:</u>

Let G be a finite group and let $a \in G$. Then $a^{|G|} = e$.

<u>Proof:</u> $\because a \in G$

$\Rightarrow \langle a \rangle$ is a subgroup of G

$\Rightarrow |\langle a \rangle|$ divides $|G|$

$\Rightarrow |a|$ divides $|G|$

$\Rightarrow |G| = k|a|$ where $k \in \mathbb{N}$.

$\therefore a^{|G|} = a^{k|a|} = \{a^{|a|}\}^k = e^k = e.$

<u>Corollary:</u> <u>Fermat's Little Theorem:</u>

For Every integer a and every prime p,

$$a^p \equiv a \pmod{p}.$$

Proof: Case-I $\gcd(a, p) \neq 1$, i.e. $\gcd(a, p) = p$

In, this case, $p \mid a$. $\Rightarrow p \mid a^p$

Now, $p \mid a^p$ & $p \mid a$

$\Rightarrow p \mid (a^p - a) \Rightarrow a^p \equiv a \pmod{p}$

Case-II: $\gcd(a, p) = 1$.

In this case $p \nmid a$.

By the division algorithm.

$a = pm + r$, where $r = 1, 2, \ldots, p-1$. —— (1)

i.e. $r \in U(p)$

Now, we know that $U(p)$ is a group under multiplication modulo p

.

and $r \in U(p) \Rightarrow r^{|U(p)|} \equiv 1 \pmod{p}$ (using previous corollary)

$$\Rightarrow r^{p-1} \equiv 1 \pmod{p} \quad \text{--- (2)}$$

Now from eq^n (1), $a = pm + r$

$$\Rightarrow a \equiv r \pmod{p}$$

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

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \quad \text{(using eq}^n\text{ (2))}$$

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

$$\Rightarrow a^p \equiv a \pmod{p}$$

Second statement of Fermat's little thm

Let a be any integer and $p \nmid a$, then

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

When we divide a^{p-1} by p, then remainder is 1.

Q. Show that Converse of Lagrange theorem is False.

Soln

Thm If H is a subgroup of G, then |H| divides |G|.

Converse. If |H| divides |G|, then H is the subgroup of G.

Example is A_4 → Alternating group of degree 4.

$$|A_4| = \frac{4!}{2} = \frac{24}{2} = 12 \qquad \Big| \qquad |A_n| = \frac{n!}{2}$$

Cayley table of A_4:

A_4 has eight elements of order 3.

Now we will show that $6 \mid 12$ but A_4 has no subgroup of order 6.

Index of a subgroup:

The index of a subgroup H in a group G is the number of distinct left (or right) cosets of H in G.

It is denoted by $|G:H|$ or $[G:H]$

If G is finite, then $|G:H| = \frac{|G|}{|H|}$.

Suppose that H is a subgroup of A_4 and $|H| = 6$.

Let a be any element of order 3 in A_4.

The left cosets of H are H, aH and a^2H.

Now, $|G:H| = \frac{|G|}{|H|} = 12/6 = 2$.

$\because$ H has index 2 in A_4,

$\therefore$ atmost two of the cosets H, aH and a^2H are distinct.

If $aH = H \Rightarrow a \in H$

If $aH = a^2H \Rightarrow H = aH \Rightarrow a \in H$

If $H = a^2H \Rightarrow aH = a^3H \Rightarrow aH = H \Rightarrow a \in H$.

$\because$ a is an arbitrary element of order 3 in A_4.

and there are eight elements of order 3 in A_4.

Thus, a subgroup of order 6 would have to contain eight elements of order 3 which is a contradiction.

$\therefore$ A_4 has no subgroup of order 6.

Q. find last digit of 9^{81} and 7^{72}.

$x = 9$
$y =$

Sol

$9^{81} \equiv x \pmod{10}$ & $7^{72} \equiv y \pmod{10}$
find x & y.

$9 \equiv -1 \pmod{10}$

$9^2 \equiv 1 \pmod{10}$

$9^{80} \equiv 1 \pmod{10}$

$\Rightarrow 9^{81} \equiv 9 \pmod{10}$

2×9

$\Rightarrow 9 \equiv 1 \pmod 2$

$\Rightarrow 9^{81} \equiv 1 \pmod 2$. — (1)

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

If $p \nmid a$

$\Rightarrow 9^{81} \equiv 9 \pmod{10}$

$5 \nmid 9$ $\boxed{\text{If } p \nmid a \text{ then } a^{p-1} \equiv 1 \pmod{p}}$

$\Rightarrow 9^{5-1} \equiv 1 \pmod 5 \Rightarrow 9^4 \equiv 1 \pmod 5$

$\Rightarrow (9^4)^{20} \equiv 1^{20} \pmod 5 \Rightarrow 9^{80} \equiv 1 \pmod 5$

$\Rightarrow 9^{81} \equiv 9 \pmod 5$ —— (2)

$\because \gcd(2,5) = 1$

$$\Rightarrow 9^{81} \equiv (1)(9) \pmod{(2)(5)}$$

$$\Rightarrow 9^{81} \equiv 9 \pmod{10}$$

last digit of 9^{81} is 9.

Theorem:

For any two finite subgroups H and K of group G.

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

where $HK = \{hk \mid h \in H, k \in K\}$

Proof:

Chapter-3:

Q. 51

Given $|a| = n$.

$$|a^d| = n/d$$

$$(a^d)^{n/d} = a^n = e.$$

$$\Rightarrow |a| \leq n/d.$$

$$|a| = t < n/d.$$

$\longrightarrow\leftarrow$.

Chapter-4

Q. 20 Suppose that G is an Abelian group of order 35 and every element of G satisfies the equation ~~x35 5 e~~. Prove that G is cyclic. Does your argument work if 35 is replaced with 33?

$\rightarrow x^{35} = e.$

$$x^{35} = e \quad \forall x \in G, \quad (\because |G| = 35)$$

To Prove: G has an element of order 35. $\left(a^{|G|} = e\right)$

$\because |G| = 35$ & $a \neq e$ & $a \in G$

$|a|$ can be 5 or 7 or 35. $\left(\because a^{35} = e\right)$

$\boxed{\because |a| \text{ divides } |G| \Rightarrow \text{Corollary}}$

Now, assume that G has no element of order 35.

In a finite group, the number of elements of order d is a multiple ~~of f(d).~~ of $\phi(d)$

no. of elements of order 5 is a multiple of $\phi(5) = 4$.

$\because 4 \nmid 34 \Rightarrow$ all nonidentity elements of G are not of order 5.

$\because 6 \nmid 34 \Rightarrow$ all nonidentity elements of G are not of order 7.

Now, G has elements of orders 5 and 7.

let $a \in G$ & $|a| = 5$.
and $b \in G$ & $|b| = 7$.

then $ab \in G$ (closure property)

& $|ab| = 35$. $\boxed{(ab)^5 \neq e \quad (ab)^7 \neq e}$

$\therefore$ G has an element of order 35.

$\Rightarrow$ G is cyclic.

Q. (24) For any element a in any group G, prove that $\langle a \rangle$ is a subgroup of C(a) (the centralizer of a).

$\langle a \rangle \subseteq C(a)$.

$a, b \in \langle a \rangle \Rightarrow ab^{-1} \in \langle a \rangle$.

Q (25) If d is a positive integer, $d \neq 2$, and d divides n, show that the number of elements of order d in Dn is $\phi(d)$. How many elements of order 2 does Dn have?

Soln. $|D_n| = 2n$.

In D_n, there are n rotations and n reflections

$\therefore$ Each reflection is of order 2.

Rotation R_{180} is the only rotation that have order 2.

But R_{180} is the element of D_n, if $R_{180} \in D_n$.

$\therefore$ Rotations of D_n form a cyclic group.

$\therefore$ no. of rotations of order d is $\phi(d)$.

no. of reflections of order d is 0. $(d \neq 2)$

$\Rightarrow$ no. of elements of order d in D_n is $\phi(d)$.

Let R_n denote the set of Rotations of D_n.

$|R_n| = n$. & R_n is cyclic.

If $2 | n$ i.e. n is even, then no. of elements of order 2 is $\phi(2) = 1$, namely R_{180}

If $2 \nmid n$, i.e. n is odd, then no. of elements of order 2 in R_n is 0.

$\therefore$ the no. of elements in D_n is $= \begin{cases} n, & \text{if } n \text{ is odd} \\ n+1, & \text{if } n \text{ is even} \end{cases}$