Pdf-05, (1) Algebra Dr Satish kr Gupta

(1) Cauchy's theorem for abelian groups

Suppose G be a finite abelian group. Let $p \mid o(G)$ i.e p is a divisor of $o(G)$ where p is prime then there is an element $a \in G$ different from identity element such that $a^p = e$, e is identity in G.

(2) State and prove Cauchy theorem.

2012 Statement. Suppose G is a finite group and $p \mid o(G)$ where p is prime. Then there is an element $a \in G$ such that $o(a) = p$.

Proof. Let G be a finite group such that $p \mid o(G)$, p is prime

Let $a \in G$ then

To prove $o(a) = p$.

We shall prove the theorem by induction on $o(G)$.

Suppose the theorem is true for all groups whose order is less than $o(G)$, we shall prove it also true for G.

If $o(G) = 1$, we are nothing to prove i.e theorem is true

If $o(G) \geq 2$.

Let H be any subgroup of G such that $o(H) < o(G)$.

Now two cases arise

(1) $p \mid o(H)$ (2) p is not a divisor of $o(H)$

(1) If $p \mid o(H)$ then by our supposition $\exists$ $a \in H$ such that $a^p = e$, e is identity element in H.

(2) If $p \nmid o(H)$, Let z be the centre of G then class equation of G is

$$o(G) = o(z) + \sum_{a \notin z} \frac{o(G)}{o(N(a))} \quad \text{--- (1)}$$

, $N(a)$ is a normalizer of a, $a \in G$.

Pdf-05, ② Algebra, Dr Satish Kr Gupta

If $a \notin Z \Rightarrow N(a) \neq G$ [i.e $N(a)$ is a proper subgroup of G]

$\Rightarrow p$ does not divide $o(N(a))$

But p divides $o(G)$ $\left[o(G) = o(N(a)) \cdot \frac{o(G)}{o[N(a)]} \right]$

$\Rightarrow p \mid \frac{o(G)}{o(N(a))}$, if $a \notin Z$

$\therefore p \mid \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$

$\Rightarrow p \mid \left[o(G) - \sum_{a \notin Z} \frac{o(G)}{o[N(a)]} \right]$

$\Rightarrow p \mid o(Z)$ $\left[\because o(Z) = o(G) - \sum_{a \notin Z} \frac{o(G)}{o[N(a)]} \right]$

~~which is a contradiction~~ p can divide $o(Z)$ only when $Z = G$.

$\Rightarrow Z$ must be equal to G

If $Z = G$ then G must be abelian

$\Rightarrow \exists\, a \in G$ such that $a^p = e$. proved.

Q. Show that if p is a prime number $o(G) = 2p$ then there exists a normal subgroup of order p.

Sol Given $o(G) = 2p$, where G is a finite group

To prove if H is a subgroup of order p then H will be normal

Now, $\frac{o(G)}{o(H)} = \frac{2p}{2} = 2$

$\Rightarrow o\left(\frac{G}{H}\right) =$ index of H in G $= 2$

$\Rightarrow$ H is a normal subgroup of G.

Note. Here $p \mid o(G) \Rightarrow \exists\, a \in G$ such that $a^p = e$.

. Let $H = (a) = \{a, a^2, a^3, \ldots, a^p = e\}$

$\Rightarrow o(H) = p$ Now $\frac{o(G)}{o(H)} = \frac{2p}{p} = 2 \Rightarrow H \triangle G$.

Pdf-05 ③ Algebra , Dr. Satish Kr Gupta

Q. Define p-Sylow subgroup of a group G, p is prime

Ans. Suppose G be a finite group and $o(G) = p^m \cdot n$ where p is prime and $p \nmid n$. Then a subgroup H of G is said to be p-Sylow subgroup of G iff $o(H) = p^m$.

e.g. Let $o(G) = 24 = 2^3 \cdot 3$ Here $p = 2$, $m = 3$, $n = 3$

Here $p \nmid n$ i.e $2 \nmid 3$.

so H is any subgroup of G is called 2-Sylow such group of G whose order will be 2^3.

Theorem. State and prove Sylow's theorem.

Statement. Suppose G be a finite group. If $p^m \mid o(G)$ and p^{m+1} is not a divisor of $o(G)$, p is prime then G has a subgroup of order p^m.

Proof. Suppose G be a finite group such that $o(G) = p^m \cdot n$, where p is prime and $p \nmid n$.

Let p^{m+1} is not a divisor of $o(G)$.

We shall prove the Theorem by induction method on $o(G)$.

Suppose that the theorem is true for all groups of order less than $o(G)$. We shall ~~true~~ prove it is also true for G.

If $o(G) = 1$, then theorem is true obviously

Let $o(G) = p^m \cdot n$ where $p \nmid n$.

If ~~p~~ $m = 0$, the theorem is obviously true

If $m = 1$, Then theorem is true by Cauchy theorem.

So let $m > 1$

$\Rightarrow G$ be a group of ~~or~~ composite order

So G must possesses a subgroup H such that $H \neq G$.

Now cases arise

(1) $p \nmid \frac{O(G)}{O(H)}$ (2) $p \mid \frac{O(G)}{O(H)}$, H is any proper subgroup of G

(1) If $p \nmid \frac{O(G)}{O(H)} \Rightarrow p^m \nmid \frac{O(G)}{O(H)}$

$\Rightarrow p^m \mid O(H)$ $\left[\because O(G) = O(H) \cdot \frac{O(G)}{O(H)} \text{ and } p \mid O(G), O(G) = p^m \cdot n \right]$

Also p^{m+1} cannot be a divisor of $O(H)$ [If so, $p^{m+1} \mid O(G)$] which will be a contradiction

Also $O(H) < O(G)$

So by hypothesis H has a subgroup of ~~of~~ order p^m and this will be a subgroup of G.

(2) If $p \mid \frac{O(G)}{O(H)}$ then consider class equ of G

$$O(G) = O(Z) + \sum_{a \notin Z} \frac{O(G)}{O[N(a)]}$$, Z is centre of G, $N(a)$ is normalizer of a, $a \in G$.

Since $a \notin Z \Rightarrow O(G) \neq O[N(a)]$

$\Rightarrow O[N(a)] < O[G]$

$\Rightarrow p \mid \frac{O(G)}{O[N(a)]}$ [$\because N(a)$ is a proper subgroup of G]

$\Rightarrow p \mid \sum_{a \notin Z} \frac{O(G)}{O[N(a)]}$

Also $p \mid O(G)$

$\Rightarrow p \mid \left[O(G) - \sum_{a \notin Z} \frac{O(G)}{O[N(a)]} \right] \Rightarrow$

$\Rightarrow p \mid O(Z)$ $\left[\because O(Z) = O(G) - \sum_{a \notin Z} \frac{O(G)}{O[N(a)]} \right]$

By cauchy theorem $\exists$ an element $b \in Z$ such that $b^p = e$, e is identity element of Z.

Pdf-05, (5) Algebra, Dr Satish Kr Gupta.

Let $N = (b)$ be a cyclic subgroup of Z

where b is generator of N

$\Rightarrow O(N) = p$ [Any group G is called cyclic if $o(a) = O(G), a \in G$]

Here N is a subgroup of Z

and $Z \Delta G$

$\Rightarrow N \Delta G$ [$xnx^{-1} \in N$ as $N \subseteq Z$, $Z \Delta G$]

$\Rightarrow \frac{G}{N}$ is a quotient group.

Let $G' = \frac{G}{N}$

$\Rightarrow o(G') = \frac{o(G)}{o(N)} = \frac{p^m \cdot n}{p} = p^{m-1} \cdot n$

$\Rightarrow o(G') < o(G)$ also $p^{m-1} \mid o(G')$

but $p^m \nmid o(G')$ so by induction

G' has a subgroup say s' whose order is p^{m-1}.

Now To prove the theorem is true for G

We know $\phi : G \longrightarrow \frac{G}{N}$

such that

$\phi(x) = Nx$, $\forall x \in G$

is a homomorphism mapping with kernel N

Also we know

If $S = \{x \in G \mid \phi(x) \in s'\}$ then

$\frac{S}{\text{Kernel of } \phi} \cong s' \Rightarrow \frac{S}{N} = s'$

$\Rightarrow \frac{O(S)}{O(N)} = o(s') \Rightarrow O(S) = O(N) \cdot O(s')$

$= p \cdot p^{m-1}$

$= p^m$

$O(S) = p^m$

Thus S is a subgroup of order p^m.

Hence proved