Department of Mathematics

SEM - 6

Course - BMH6DSE33

Group Theory - II

Notes given by Rima Dutta.

Now, $C(a) \subsetneq G$.

So, $|C(a)| < |G| = n$

Hence by induction hypothesis, $C(a)$ has an element of order p and hence G has an element of order p.

Definition (p-group) :— A group G is said to be p-group if the order of each element of G is some power of p where p is prime.

A subgroup H of G is called p-subgroup if H is a p-group.

Example :— Consider the group $(\mathbb{Z}_4, +)$.

Now, $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

Note that, $o(\bar{0}) = 1$, $o(\bar{1}) = 4 = 2^2$, $o(\bar{2}) = 2 = 2^1$,

$o(\bar{3}) = 4 = 2^2$.

Thus, $(\mathbb{Z}_4, +)$ is a 2-group.

Theorem :— Let G be a non-trivial finite group. Then G is a p-group if and only if $|G| = p^k$ for some positive integer k.

Proof:- Let G be a p-group.

Let $|G| = m$.

Then m can be expressed as a product of prime factors.

Let $m = p_1 p_2 \dots p_k$ where each $p_i (i = 1, 2, \dots, k)$ is prime.

By Cauchy's theorem, G has an element of order p_i for all $i = 1, 2, \dots k$.

Since G is a p-group, so order of each element is p^{r_i} where r_i is a positive integer.

So $p_i = p^{r_i}$ where $r_i > 0$.

Since p and p_i are all primes, so $p = p_i$ for all $i = 1, 2, \dots k$.

Hence $|G| = p \cdot p \cdots p$ (k times)

$= p^k$.

Conversely let $|G| = p^k$ where p is prime.

Then by Lagrange's theorem, the order of each element of G is some power of p.

Hence G is a p-group.

Exercise:- Let G be a finite p-group with $|G| > 1$. Then $Z(G)$, the centre of G, has more than one element ie. $|Z(G)| > 1$.

Solution:- Let G be a p-group of order p^n, for some $n \in \mathbb{N}$.

First we prove that an element $a \in Z(G)$ if and only if $C(a) = G$.

Let $a \in Z(G)$.

Then $ag = ga \quad \forall g \in G$.

Hence $g \in C(a)$.

$\therefore C(a) = G$.

Conversely, if $C(a) = G$, then a commutes with all the elements of G.

ie. $a \in Z(G)$.

We now consider the class equation $|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)]$

where the summation runs over the complete set of distinct conjugacy class representative which does not belong to $Z(G)$.

Let $a \notin Z(G)$.

Then $C(a) \subsetneq G$.

Hence $|C(a)| \mid |G|$

ie. $|C(a)| \mid p^n$

$\therefore |C(a)| = p^r$ where $r < n$ is a positive integer.

$\therefore [G : C(a)] = \dfrac{|G|}{|C(a)|} = p^{n-r}$

Thus, $p \mid [G : C(a)]$ when $a \notin Z(G)$

$\therefore p \mid \sum_{a \notin Z(G)} [G : C(a)]$

Again, $p \mid |G|$.

$\therefore$ From the class equation, we have,

$p \mid |Z(G)|$.

But p is prime. So, $p > 1$.

Hence $|Z(G)| > 1$.

ie. $Z(G)$ contains more than one element.

Theorem:- Let p be a prime integer. Then any group of order p^2 is commutative.

Proof:- Let G be a group of order p^2 where p is prime.

Then G is a p-group.

Then $|Z(G)| > 1$.

Then $|Z(G)| = p$ or p^2.

Let $|Z(G)| = p$.

Then $Z(G) \subsetneq G$.

So $\exists$ an element $a \in G$ such that $a \notin Z(G)$.

For this $a (\in G)$, we have $C(a) \subsetneq G$.

Again since $a \notin Z(G)$, so $Z(G) \subsetneq C(a)$

This implies $|C(a)| > |Z(G)|$.

$\therefore |C(a)| = p^2$

Hence $C(a) = G$.

Thus, $ax = xa \quad \forall\ x \in G$.

$\therefore a \in Z(G)$ — which is a contradiction.

$\therefore |Z(G)| = p^2$.

Thus, $Z(G) = G$.

Hence G is commutative.

Exercise:- Let G be a non-commutative group of order p^3, where p is a prime integer. Prove that, $|Z(G)| = p$.

Solution:- Now, $|G| = p^3$.

Then G is a p-group.

Thus, $|Z(G)| > 1$.

Hence $|Z(G)| = p$ or p^2 or p^3.

If $|Z(G)| = p^3$ then $Z(G) = G$. Hence G is commutative which is a contradiction,

$\therefore |Z(G)| \neq p^3$.

If $|Z(G)| = p^2$. Then $|G/Z(G)| = \frac{|G|}{|Z(G)|} = p$.

Thus, $G/Z(G)$ is cyclic ($\because p$ is prime) and therefore, $G/Z(G)$ is commutative.

Hence G is commutative, which is a contradiction.

$\therefore |Z(G)| = p$. (Proved).

Note:- We know that the converse of Lagrange's theorem may not be true in general.

But, the converse of Lagrange's theorem is true for finite commutative group.

Theorem:- Let G be a commutative group of order n. If m is a positive integer such that $m|n$ then G has a subgroup of order m.

Proof:- If $n = 1$ then $m = n = 1$. and the results follows trivially.

So we assume that $n > 1$.

If $m = 1$, then $\{e\}$ is the required subgroup of order m.

Thus, we assume that $m > 1$.

We prove the theorem by mathematical induction on n.

If $n = 2$ then $m = n = 2$. and in this case G is itself the required subgroup of G. of order m.

Now, we assume that the theorem is true for all finite commutative groups of order K, $2 \leq K < n$.

Let G be a commutative group of order n.

Also let m be a positive integer such that $m|n$.

If m is prime, then by Cauchy's theorem, G has an element of order m and hence a subgroup of order m.

So let m be not prime.

Then m is composite.

So m has a prime factor (say) p.

Let $m = pm_1$ where m_1 is a positive integer greater than 1.

Again since $m \mid n$ so, $n = mm_2$ for some positive integer m_2.

$\therefore n = pm_1m_2$.

This implies, $p \mid n = |G|$.

Since p is prime and G is finite commutative group, so by Cauchy's theorem, G has an element of order p. and hence a subgroup H of order p.

Since G is commutative, so H is normal in G.

$\therefore G/H$ exists.

Now, $|G/H| = \frac{|G|}{|H|} = m_1m_2 < n$.

Since G is commutative, so G/H is commutative.

$\therefore |G/H| < n$ and $m_1 \mid |G/H|$.

so by induction hypothesis, G/H has a subgroup K/H (say) of order m_1., where K is a subgroup of G containing H.

Now, $|K| = \frac{|K|}{|H|} \cdot |H| . = |K/H| \cdot |H| = m_1p = m$.

Hence K is a subgroup of G of order m.

Thus, G has a subgroup of order m where $m \mid |G|$.

Lemma 1. :-

Exercise :- Let G be a finite group of order p^n (where p is prime and $n \geq 1$). Suppose S is a finite G-set.

If $S_0 = \{a \in S : ga = a \ \forall \ g \in G\}$. then $|S| \equiv |S_0| \pmod{p}$

Proof :- We first show that, $a \in S_0$ if and only if $[a] = \{a\}$.

Let $a \in S_0$.

Then for any $b \in [a]$, we have

$b = ga$ for some $g \in G$.

Again since $a \in S_0$, so $ga = a$.

Hence $b = a$.

$\therefore [a] = \{a\}$.

Conversely let, $[a] = \{a\}$

Let $g \in G$.

Then $ga \in [a] = \{a\}$.

Thus, $ga = a. \ \forall \ g \in G$.

$\therefore a \in S_0$.

Thus, $a \in S_0$ if and only if $[a] = \{a\}$.

Now, $S = S_0 \cup [a_1] \cup [a_2] \cup \ldots \cup [a_K]$ where $a_1, a_2, \ldots, a_K \notin S_0$

$\therefore |S| = |S_0| + |[a_1]| + |[a_2]| + \ldots + |[a_K]|$.

$= |S_0| + [G : G_{a_1}] + [G : G_{a_2}] + \ldots + [G : G_{a_K}]$.

Now for any a_i $(i=1,2,\ldots,k)$, we have $G_{a_i} \subsetneq G$.

$\therefore |G_{a_i}| < |G|$

Hence $|G_{a_i}| = p^r$ where $r < n$.

Thus, $[G : G_{a_i}] = p^{n-r}$.

$\therefore p \mid [G : G_{a_i}] = p^{n-r}$ for all $i=1,2,\ldots,k$

$\therefore p \mid \sum_{i=1}^{k} [G : G_{a_i}]$

ie. $p \mid (|S| - |S_0|)$

ie. $|S| \equiv |S_0| \pmod{p}$.

Lemma 2 :- Let G be a finite group and H be a subgroup of G such that $|H| = p^n$, where p is prime and $n \geq 1$. Then $[G:H] \equiv [N(H) : H] \pmod{p}$.

Proof :- $N(H)$ = Normalizer of H.

$$= \{g \in G : gHg^{-1} = H\}.$$

Let $S = \{gH : g \in G\}$.

Since G is finite, so S is finite.

Now, we define group action of H on S by

$$a \cdot gH = (ag)H \quad \forall\, a \in H, \forall\, gH \in S.$$

Under this action, S is a H-set.

Also let $S_0 = \{ gH \in S : a \cdot gH = gH \ \forall \ a \in H \}$.

Then by previous lemma, we must have,

$$|S| \equiv |S_0| \pmod{p}. \quad \text{---} (1)$$

Now, $|S| = [G : H]$.

Moreover, $gH \in S_0$ if and only if $a \cdot (gH) = gH \ \forall \ a \in H$.

ie. if and only if $g^{-1}ag \in H \ \forall \ a \in H$.

ie. if and only if $g^{-1}Hg \subseteq H$.

Also, $|g^{-1}Hg| = |H|$.

$\therefore gHg^{-1} = H$.

ie. $g \in N(H)$ of H

This, gH is a left coset in $N(H)$.

$\therefore |S_0| = [N(H) : H]$.

Hence from (1), we have,

$$|S| \equiv [N(H) : H] \pmod{p}.$$

ie. $[G : H] \equiv [N(H) : H] \pmod{p}$.

Exercise :- Let G be a finite group of order p^n where p is prime and $n \geq 1$. Prove that any subgroup of G of order p^{n-1} is a normal subgroup.