Department of Mathematics

SEM - 6

Course - BMH6DSE33

Group Theory - II

Notes given by Rima Dutta.

Notes by Rima Dutta.

Sylow Theorem

Definition :- Let G be a group and $a, b \in G$. Then b is said to be conjugate to a if $\exists$ an element $x \in G$ s.t. $b = xax^{-1}$.

Note :- Let $a \in G$.

Then $a = eae^{-1}$

Then a is conjugate to a.

Let $a, b \in G$ s.t.

a is conjugate to b.

Then $b = xax^{-1}$ for some $x \in G$.

$\Rightarrow x^{-1}bx = a$

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

$\Rightarrow a$ is conjugate to b.

Also let $a, b, c \in G$ s.t.

b is conjugate to a and c is conjugate to b.

$\Rightarrow b = xax^{-1}$ and $c = yby^{-1}$ for some $x, y \in G$.

$\Rightarrow c = y(xax^{-1})y^{-1}$

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

$\Rightarrow c$ is conjugate to a.

$\therefore$ This is an equivalence relation.

This relation is called conjugacy relation on G.

If $a \in G$, then the equivalence class $[a]$, determined by a under this relation is called conjugacy class of a and it is denoted by $C_l(a)$.

Theorem :- Let G be a group. and $a \in G$. Then

(i) $Z(G) \subseteq C(a)$ [$Z(G) \to$ Centre of G, $C(a) \to$ centralizer of a]

(ii) $|C_l(a)| = [G : C(a)]$

Proof :- (i) Let $g \in Z(G)$.

Then $gx = xg \quad \forall x \in G$.

In particular, $ga = ag$.

$\therefore g \in C(a)$

$\therefore Z(G) \subseteq C(a)$.

(ii) Let $T = \{xC(a) : x \in G\}$.

Now, $C_l(a) = \{b \in G : b = xax^{-1} \text{ for some } x \in G\}$.

Now, we define $f : T \to C_l(a)$ by

$f(xC(a)) = xax^{-1}$ for all $xC(a) \in T$.

Let $xC(a), yC(a) \in T$.

Note that,

~~$xC(a) = yC(a)$~~

$\Rightarrow f(xC(a)) = f(yC(a))$

$\Rightarrow xax^{-1} = yay^{-1}$

$\Rightarrow x^{-1}xax^{-1}y = x^{-1}yay^{-1}xy$

$\Rightarrow ax^{-1}y = x^{-1}ya.$

$\Rightarrow x^{-1}y \in C(a)$

$\Rightarrow xC(a) = yC(a)$

This implies that, '$\Rightarrow$' shows that f is injective and '$\Leftarrow$' shows that f is well defined.

Again let $b \in C_l(a)$.

Then $\exists\ z \in G$ s.t. $b = zaz^{-1}$.

Now, $zC(a) \in T$ such that $f(zC(a)) = zaz^{-1} = b$.

Thus, f is surjective.

Thus, f is bijective.

Hence, $|C_l(a)| = |T| = [G : C(a)]$.

Theorem:- Prove that, $|G| = \sum_{a \in G} [G : C(a)]$, where the summation runs over the complete set of conjugacy class representive.

Proof:- Let G be a group.

We know that conjugacy relation is an equivalence relation on G.

So, the group G can be partitioned into disjoint conjugacy classes.

Hence $G = \bigcup_{a \in G} C_l(a)$, where the union runs over the complete set of disjoint conjugacy class representative

Therefore, $|G| = \sum_{a \in G} |C_l(a)|$, where the summation runs over the complete set of disjoint conjugacy class representative.

Also, we know, $|C_l(a)| = [G : C(a)]$ for all $a \in G$.

Thus, $|G| = \sum_{a \in G} [G : C(a)]$, where the summation runs over the complete set of disjoint conjugacy class representative.

Theorem:- Prove that, $|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)]$, where the summation runs over the complete set of disjoint conjugacy class representative which does not belong to $Z(G)$. [This equation is called class equation of a finite group].

Proof:- We first show that, $a \in Z(G)$ if and only if $C_l(a) = \{a\}$.

For this, let $a \in Z(G)$ and $b \in C_l(a)$.

Then $\exists\ x \in G$ s.t. $b = xax^{-1}$.

Then $b = xax^{-1} = axx^{-1} = a$.

$\therefore C_l(a) = \{a\}$.

Conversely let, $x \in G$.

Then $xax^{-1} \in C_l(a) = \{a\}$.

$\therefore xax^{-1} = a$

$\Rightarrow xa = ax$.

Thus, $a \in Z(G)$.

Thus, $a \in Z(G)$ if and only if $C_l(a) = \{a\}$.

Now, we know that, $G = \bigcup_{a \in G} C_l(a)$, where the union runs over the complete set of disjoint conjugacy class representative.

Therefore, $G = \left(\bigcup_{a \in Z(G)} C_l(a) \right) \cup \left(\bigcup_{a \notin Z(G)} C_l(a) \right)$

$$= \bigcup_{a \in Z(G)} \{a\} \cup \left(\bigcup_{a \notin Z(G)} C_l(a) \right)$$

Hence, $|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)]$, where the summation runs over the complete set of disjoint conjugacy classes representative which does not belong to $Z(G)$.

Theorem:- Let G be a finite commutative group. If p is a prime integer such that p divides $|G|$, then G has an element of order p.

Proof:- We prove the theorem by using mathematical induction on $|G|$.

Let $|G| = 2$.

Then $G = \{e, a\}$ where $a^2 = e$, e being the identity element of G.

Hence G has an element of order 2.

So the statement is true for $|G| = 2$.

Let us assume that the statement is true for all finite commutative group G such that $2 \leq |G| < n$.

Let us consider a finite commutative group G of order n.

Let p be a prime integer such that $p \mid |G| = n$.

Let $a \in G$ with $a \neq e$ and $o(a) = m$

Then either $p \mid m$ or $p \nmid m$.

If $p \mid m$, then $\exists$ an integer k such that, $m = pk$.

Now, $a^m = e$

$\Rightarrow a^{pk} = e$

$\Rightarrow (a^k)^p = e$

Since $o(a) = m$ and $k < m$, so we have $a^k \neq e$.

Hence $(a^k)^p = e$ implies a^k is an element of G of order p.

Hence G has an element a^k of order p.

Again let $p \nmid m$.

Let $H = \langle a \rangle$.

Since $o(a) = m$, so $|H| = m$.

Since G is commutative, so H is normal subgroup of order m and hence G/H exists.

Now, $2 \leq |G/H| < n$.

Again, $p \mid |G|$. but $p \nmid m = |H|$.

$\therefore p \mid \frac{|G|}{|H|}$ ie. $p \mid |G/H| < n$.

Thus, by induction hypothesis, G/H has an element bH (say), of order p.

Hence $(bH)^p = H$.

ie. $b^p H = H$

ie. $b^p \in H$.

Again $|H| = m$ and $b^p \in H$

$\Rightarrow (bH)^m \neq H$ $\therefore (b^p)^m = e$

$\Rightarrow (b^m)^p = e$.

Now, we show that $b^m \neq e$.

If $b^m = e$ then $b^m H = H$.

ie. $(bH)^m = H$.

Now, $o(bH) = p$ and $(bH)^m = H$ implies $p \mid m$, which is a contradiction.

$\therefore b^m \neq e$.

Thus, $o(b^m) = p$.

Thus, b^m is an element of G of order p.

Theorem :- (Cauchy's Theorem) :-

Let G be a finite group. If p is a prime integer such that p divides $|G|$, then G has an element of order p.

Proof :- We shall prove the theorem by using mathematical induction on $|G|$.

Let $|G| = 2$.

Then $G = \{e, a\}$, where $a^2 = e$, e being the identity element of G.

Hence G has an element of order 2.

So the theorem is true for $|G| = 2$.

Let us assume that the theorem is true for all finite group G such that $2 \leq |G| < n$.

Let us consider a finite group G of order n and p be an prime integer such that $p \mid |G| = n$.

Now we consider the class equation,

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)],$$ where the summation runs over the complete set of disjoint conjugacy class representative.

Case 1:- Suppose $p \mid |Z(G)|$.

Since $Z(G)$ is a commutative group and $p \mid |Z(G)|$ we have $Z(G)$ have an element of order p and hence G has an element of order p.

Case 2:- Let $p \nmid |Z(G)|$.

Then $Z(G) \neq G$. [since, if $Z(G) = G$ then $|Z(G)| = |G|$ and since $p \mid |G|$, so $p \mid |Z(G)|$, which is a contradiction].

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

We claim that, $p \mid |C(a)|$ for atleast one $a \notin Z(G)$.

If not, then $p \nmid |C(a)|$ for all $a \notin Z(G)$.

Now, $p \mid |G|$ implies $p \mid \frac{|G|}{|C(a)|}$ for all $a \notin Z(G)$.

Thus, $p \mid \frac{|G|}{|C(a)|}$ implies $p \mid \sum_{a \notin Z(G)} \frac{|G|}{|C(a)|}$

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

So from the class equation, it follows that $p \mid |Z(G)|$, which is a contradiction.

Hence there is atleast one $a \notin Z(G)$ such that $p \mid |C(a)|$.

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.