Group Theory 14

04 November 2023 10:58

Q) G is a group. $H \leq G$, $[G:H] = 2$. K be a subgroup of G with at least one element $g \notin H$. Then $G = HK$

gH, H $\quad g \notin H \quad$ $K \ni e$

$HK = He \cup Hg = G$

<u>Definitions:-</u> If p is a prime then a p-group is a group in which every element has an order of p.

<u>Lemma:-</u> If G is a finite abelian group whose order is divisible by a prime p, then G contains an element of order p.

<u>Proof:-</u> $|G| = np$, $k \neq 0$

$n = 1 \Rightarrow |G| = p$ so cyclic so $\exists a \in G$ s.t. $\mathrm{Ord}(a) = 1$

<u>Induction:-</u> Assume for $n = 1$ to $k-1$ it is true

If $p|d$ then, $d = \mathrm{Ord}(a)$, $a^{d/p}$ has order p when $p|d$.

$a \in G$ such that

Suppose $p \nmid \mathrm{Ord}(a) = d$

We know that G is abelian, so, $\langle a \rangle$ is a normal subgroup of G. $\Rightarrow G/\langle a \rangle$ is an abelian group.

$|G/\langle a \rangle| = kp/d$. Now $p \nmid d \Rightarrow k/d < k \in \mathbb{Z}$

$|G/\langle a \rangle| < kp$ so it is true by induction

So G contains a such that $\mathrm{Ord}(a) = p$.

<u>Theorem:-</u> If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

<u>Proof:-</u> If $x \in G$ then $[G : C_G(x)]$ = the number of conjugates of x

Proof:- If $x \in G$ then $[G : C_G(x)]$ = the number of conjugates of x

If $x \notin Z(G)$ then $|C_G(x)| < |G|$

If $p \mid |C_G(x)|$ for any non-central x, then done.

But if $p \nmid |C_G(x)|$, then, $|G| = [G : C_G(x)]\,|C_G(x)|$

If $p \mid |G : C_G(x)|$,

$$|G| = \sum_i [G : C_G(x_i)] + Z(G)$$

for $x_i \in$ conjugacy class and ~~no~~ $x_i, x_j \in$ same conjugacy class

$$\Rightarrow Z(G) = |G| - \sum_i [G : C_G(x_i)]$$

Now $p \mid |G : C_G(x_i)|$ and $p \mid |G| \Rightarrow p \mid Z(G)$

and $Z(G)$ is abelian so $a \in G$ such that $\mathrm{Ord}(a) = p$

- A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof:- $|G| = p^m$ then $H \leq G \Rightarrow |H| = p^k$, $k \leq m$ so G is a p-group.

Conversely,

Suppose $|G| \neq p^m \Rightarrow q \mid |G|$ where $q \neq p$ and q is a prime

So $\exists\, a \in G$ such that $\mathrm{Ord}(a) = q \Rightarrow \Leftarrow$ Contradiction.

Thus $|G| = p^m$

Theorem:- If $G \neq 1$ is a finite p-group, then $Z(G) \neq 1$

Proof:-

$$|G| = Z(G) + \sum [G : C_G(x_i)]$$

$x_i \notin Z(G)$.

$|G| = p^m$ so $p \mid [G : C_G(x_i)] \Rightarrow p \mid |Z(G)|$

$\Rightarrow Z(G) \neq 1$

- If p is a prime then every group G of order p^2 is abelian

Theorem:- Let G be a finite p-group, then,

(a) If H is proper subgroup of G then $H < N_G(H)$

(b) Every maximal subgroup of G is normal and has index p.

Proof:- a) $H < G$, if $H \trianglelefteq G$, then $N_G(H) = G$ so done.

If not, let C be the set of all conjugate of H,

$|C| = [G : N_G(H)] \neq 1$

Orbit of x consists of all points that be reached using the group action $G \cdot x = \{ g \cdot x \mid g \in G \}$

Every orbit of C is a power of p.

Orbit of $\{H\}$ will be size 1.

we will get $p-1$ orbits of size 1

So except e we will get $\{gHg^{-1}\}$ has orbit size 1.

$gHg^{-1} \neq H$ where $\{gHg^{-1}\}$ has orbit size 1.

For $a \in H$ $g^{-1}ag \in N_G(H)$ $\forall a \in H$ and we also get,

$gag^{-1} \notin H$ for some $a \in H$

$\Rightarrow H < N_G(H)$

b) If $H < N_G(H) \Rightarrow N_G(H) = G$ if H is maximal $H \trianglelefteq G$.

$\Rightarrow [G : H] = p$

Lemma:- If G is a finite p-group and r_1 is the number of subgroups of G having order p then $r_1 \equiv 1 \pmod p$

Proof:- $Z(G)$ is abelian. H is formed by $Z(G)$ and 1

$H < G \Rightarrow |H| = p^m$

No. of central elements will be $|H| - 1 \equiv p^m - 1 \pmod p$

$\equiv -1 \pmod p$

If $x \in G$ of order p and not central,

x^G contains elements of order p.

$|G| = p^n$

... of order $p = p^n - 1 \pmod p \equiv -1 \pmod p$

$|G| = p^n$

No. of elements in G of order $p = p^n - 1 \pmod p \equiv -1 \pmod p$

No. of subgroups of G is r_1 of order p.

No. of element in each such subgroup of order p is $p-1$

So we get $r_1(p-1) = (-1) \bmod p$ from distinct subgroups

$\Rightarrow r_1 \equiv 1 \pmod p$