Group Action & Sylow's Thm.

Lecture 12

09/02/2022

Recall:

A gp action of a gp G on a set A is a map
$$G \times A \longrightarrow A$$
$$(g, s) \longmapsto g \cdot s$$
satisfying

(1) $g_1 (g_2 s) = (g_1 g_2) s$

(2) $1 \cdot s = s$ $\quad \forall s \in A.$

This gp action can be represented in a different way also

For each fixed $g \in G$ we get a map σ_g defined by
$$\sigma_g : A \longrightarrow A \quad \text{by}$$
$$\sigma_g (s) = g \cdot s.$$

and it has the following properties:

(1) For each fixed $g \in G$, σ_g is a permutation of A

(2) The map $\varphi : G \longrightarrow S_A$ defined by $\varphi(g) = \sigma_g$ is a homo.

$$\varphi(g_1 g_2) = \sigma_{g_1 g_2}$$

WTS $\sigma_{g_1 g_2} = \sigma_{g_1} \cdot \sigma_{g_2}$

$$\sigma_{g_1 g_2}(s) = (g_1 g_2)(s) = g_1 (g_2 s)$$
$$= \sigma_{g_1} \sigma_{g_2}(s)$$

The above homo φ is called the permutation representation associate to a grp action.

$$O(s) = \{ g\cdot s \mid g \in G \}.$$

$$G_s = \mathrm{stb}(s) = \{ g \in G \mid gs = s \} \leq G.$$

Note $\boxed{|O(s)| = [G : G_s].}$

Defn. A gp action of G on a set A is called transitive if there is only one orbit i.e given any two elts $x, y \in A$, $\exists\, g \in G$ s.t $x = gy$.

Thm (Cauchy): Let G be a finite gp and p be a prime number s.t $p \mid |G|$. Then G has an elt of order p i.e G has a subgp of order p.

Pf: Consider the set

$$A = \{(x_1, \dots, x_p) \in G \times \dots \times G \mid x_1 x_2 \cdots x_p = 1\}$$

Let $|G| = n$. Then $|A| = n^{p-1}$.

Since $p \mid |G|$ $\therefore$ $p \mid |A|$.

Let $\sigma = (1\ 2\ 3 \dots p) \in S_p$.

and $H = \langle \sigma \rangle \subset S_p$. Then $|H| = p$.

Define a gp action $H \times A \to A$

$$(\sigma^i, (x_1, x_2, \dots, x_p)) \longrightarrow (x_{\sigma^i(1)}, \dots, x_{\sigma^i(p)}).$$

$p=3$ $\sigma = (1\ 2\ 3)$. $x_1 x_2 x_3 = 1$.

$$(\sigma, (x_1, x_2, x_3)) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$
$$= (x_2, x_3, x_1).$$

$$|O(x_1, \dots, x_p)| = \frac{|H|}{|H_{(x_1, x_2, \dots x_p)}|}$$

$\therefore$ $|O(x_1, \dots, x_p)|$ is either 1 or p.

Suppose $|O(x_1, \dots, x_p)| = 1$.

$\Rightarrow$ $O(x_1, \dots, x_p) = \{(x_1, \dots, x_p)\}$.

$(x_{\sigma(1)}, \dots, x_{\sigma(p)}) = (x_1, \dots, x_p)$.

$\Rightarrow$ $x_1 = x_2 = x_3 \dots = x_p$ and $x_1^p = 1$.

$$O(1, 1, \dots, 1) = \{(1, 1, \dots, 1)\}.$$

$|A| = 1 + (k-1)p$.

$$A = O(\underline{s}_1) \sqcup \dots \sqcup O(\underline{s}_k)$$

$$|A| = [H : H_{\underline{s}_1}] + \dots + [H : H_{\underline{s}_k}]$$

Say $\underline{s}_1 = (1, \dots, 1)$ then $[H : H_{\underline{s}_1}] = 1$.

$\therefore$ The no of elts satisfying $x^p = 1$ is divisible by p. But $(1, \ldots, 1)$ are such elt. so there must be at least $p-1$ elts s.t $x^p = 1$.

__Cayley's Thm__: Every finite gp G is isomorphic to a subgp of a permutation gp. If G has order n then it is isomorphic to a subgp of S_n.

__Pf__: Consider the gp action by left multi'

$$G \times G \longrightarrow G$$
$$(g, x) \longmapsto gx.$$

Using the above gp action we can have a gp homo.

$$\varphi : G \longrightarrow S_n. \qquad \text{where } n = |G|.$$

$$\varphi(g) = \sigma_g \quad \text{where } \sigma_g : G \to G.$$

$$\sigma_g(x) = gx.$$

Then $\ker \varphi = \{ g \in G \mid \sigma_g = Id \}$.

$= \{ g \in G \mid \sigma_g(x) = x \ \forall x \in G \}$

$= \{ g \in G \mid gx = x \ \forall x \in G \}$

$= \{1\}.$

$\therefore$ G is isomorphic to its image in S_n.

Group action by conjugation:

$$G \times G \longrightarrow G$$

$$(g, x) \longmapsto gxg^{-1}$$

$$\mathrm{stb}(x) = \{ g \in G \mid gxg^{-1} = x \}$$

$$= \{ g \in G \mid gx = xg \}.$$

$$= \text{centralizer of } x := C(x).$$

$$O(x) = \{ gxg^{-1} \mid g \in G \}.$$

$$:= \text{conjugacy class of } x = C_x.$$

Note that an elt $x \in G$ have conjugacy class of size 1 implies

$gxg^{-1} = x \quad \forall g \in G$. ie iff $x \in Z(G)$.

Let G be a gp of finite order and $Z(G) = \{1, z_1, \dots, z_m\}$.

and let $C_{g_1}, \dots, C_{g_r}$ be the conjugacy classes of not contained in the centre.

$$G = \underbrace{C_1 \sqcup C_{z_1} \sqcup \dots \sqcup C_{z_m}} \sqcup C_{g_1} \sqcup \dots \sqcup C_{g_r}$$

$$|G| = |Z(G)| + \sum_{i=1}^{r} |C_{g_i}|$$

This is known as <u>class eq^n.</u>

<u>Some Application:</u>

<u>Defn</u>. A gp of order p^n, p is a prime no. and $n \in \mathbb{N}$, is called a p-gp.

Propn. Let G be a p-gp. Then $|Z(G)| \geq p$.

Pf: Suppose $Z(G) = \{1\}$. Let $|G| = p^n$.

Then $$|G| = 1 + \sum_{i=1}^{r} |C_{g_i}|$$

Note that $$|C_{g_i}| = [G : C(g_i)].$$

$$= \frac{|G|}{|C(g_i)|}$$

Thus $p \,\big|\, |C_{g_i}|$ and $p \mid |G|$.

Thus $p \mid 1$. which is a contradiction.

$\therefore$ $|Z(G)| \geq p$.

Cor. Any gp of order p^2 is abelian.

Pf: By previous propn we have
$$|Z(G)| \geq p.$$

Let $|Z(G)| = p$ and $x \in G \setminus Z(G)$.

$$Z(G) \subseteq C(x) = \{g \in G \mid gx = xg\}.$$

Note that $C(x)$ is strictly bigger than $Z(G)$ as $x \in C(x) \setminus Z(G)$.

$\therefore \quad |C(x)| = p^2$ i.e. $C(x) = G$.

$\Rightarrow x \in Z(G)$

which is a contradicti

Hence $Z(G) = G$.

Thus G is abelian.

Cor. Any gp of order p^2 is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Pf: We know that any gp of order p^2 is abelian.

Let $1 \neq x \in G$. then $|x| = p$ or $|x| = p^2$.

If $|x| = p^2$ then $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

Let there doesn't exist any elt of order p^2 i.e all non-elts are of order p.

Consider $H = \langle x \rangle$. and $|x| = p$.

Let $1 \neq y \notin H$. and $|y| = p$.

Let $K = \langle y \rangle$. Then $H \cap K = 1$.

Since G is abelian H & K are normal subgps of G. $\therefore HK$ is a subgp of G which is strictly larger than H. $\therefore |HK| = p^2$. $G = HK$.

$\therefore G \cong H \times K = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Sylow Thm:

Defn. Let G be a gp and p be a prime number.

(1) A gp of order p^n for some $n \geq 1$ is called a p-gp. Subgps of G which are p-gps are called p-subgps.

(2) If G is a gp of order $p^{\alpha} m$ where $p \nmid m$ then a subgp of order p^{α} is called a Sylow p-subgp of G.

(3) n_p = denote the no. of Sylow p-subgps of G.

Thm. Let G be a gp of order $p^\alpha m$ where $p \nmid m$ & p is a prime no.

(1). Sylow p-subgps exist i.e $\exists$ a subgp of order p^α. [Infact, $\exists$ subgps of order p^r for all $1 \le r \le \alpha$.]

(2) If P is a Sylow p-subgp of G and Q is any p-subgp of G then $\exists g \in G$ s.t $Q \le gPg^{-1}$ i.e Q is contained in some conjugate of P.

(3) $n_p \equiv 1 \pmod p$ and $n_p \mid m$.

↳ no. of Sylow p-subgp.