

Last time: Semidirect products

Thm (Cayley's Thm) Every finite gp G is isom to a subgp of S_n for some n . If $|G| = n$, then G is isom to a subgp of S_n .

Defⁿ A permutation repⁿ of a gp G is $\varphi: G \rightarrow S_n$, a homom.

Propⁿ G a gp. There is a bijective corr between perm rep^s of G and actions of G on $\{1, 2, \dots, n\}$.

Pf. Suppose G acts on $\{1, 2, \dots, n\}$.
 For each g , have $m_g: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$

Define $\phi: G \rightarrow S_n$ as $\phi(g) = m_g$

$$\phi(g_1 g_2) = m_{g_1 g_2} = m_{g_1} \circ m_{g_2} = \phi(g_1) \phi(g_2)$$

$\uparrow$
 action

Conversely, suppose $\phi: G \rightarrow S_n$ is a homom. Then

define $m_g: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ as $m_g = \phi(g)$.

This defines an action G on $\{1, 2, \dots, n\}$. ⑩

Cor Let $\text{Perm}(S)$ denote the gp of permutations of a set S .

Then, there is a bijective correspondence between actions of a gp G on S and homom $\varphi: G \rightarrow \text{Perm}(S)$.

actions of a gp G on S and homom $\varphi: G \rightarrow \text{Perm}(S)$.

Pf Same.

Defn An action $G \curvearrowright S$ is said to be faithful if

$$gs = s \quad \forall s \in S \implies g = 1.$$

Equivalently, $\ker \{G \rightarrow \text{Perm}(S)\} = \{1\}$.

Pf of Cayley's Thm

- $S = G$ $G \curvearrowright G$ by left multiplication
- This defines $\phi: G \rightarrow \text{Perm}(S) \cong S_n$ if $|G| = n$.
- $G \curvearrowright G$ by left mult is faithful
 $\implies \phi: G \rightarrow S_n$ is injective
 $\implies G \cong \phi(G) \leq S_n$ as desired.

An important action of G on itself: $G \curvearrowright G$ by conjugation.

$$g * x = gxg^{-1}, \quad g \in G, x \in G$$

The stabilizer of an elt $x \in G$ for this action is

$$\cdot Z(x) = \{g \in G: gxg^{-1} = x\} = \{g \in G: gx = xg\}$$

called the centralizer of x

The orbit of an elt $x \in G$ for this action is

$$C(x) = \{ x' \in G : \exists g \in G \text{ st. } x' = g x g^{-1} \}$$

called the conjugacy class of x

Counting formula $|G| = |C(x)| |Z(x)|$

Also the conj. classes partition G

$$(*) \quad |G| = \sum_i |C_i| = |C_1| + |C_2| + \dots + |C_k|$$

C_i a conj.
class

C_j are the conj. classes

Moreover, the $|C_j|$ divide $|G|$

This eqn (*) is called the class eqn of G .

Propⁿ a) $Z(x)$ contains x , and contains the center Z of G .

b) $x \in G$ is in Z , the center $\iff Z(x) = G \iff C(x) = \{x\}$.

Example of class eqn

$$G = S_3, \quad 1, x, y$$

• $Z(x)$: know $|Z(x)| |C(x)| = 6$, know $Z(x)$ contains $1, x, x^2$

But $y \notin Z(x)$ because $yx \neq xy$

But $y \notin Z(x)$ because $yx \neq xy$
 $\Rightarrow Z(x) = \{1, x, x^2\}$ has size 3,
 $\Rightarrow |C(x)| = 2$

• $Z(y)$: know it contains $1, y$. $x \notin Z(y)$
 $\Rightarrow |Z(y)| = 2 \Rightarrow |C(y)| = 3$.

$$\Rightarrow 6 = |S_3| = 1 + 2 + 3$$

p-gps

A gp G is called a p-gp if $|G| = p^e$ for some prime p .

Propⁿ The center of a p-gp is not trivial.

Pf. Consider the class eqⁿ.

$$p^e = |G| = \underbrace{1}_{\text{for the identity}} + |C_1| + |C_2| + \dots + |C_r|$$

Sizes of $|C_j| \mid p^e \Rightarrow$ if $|C_j| \neq 1$ then it is div by p .
 $\Rightarrow \exists j$ w $|C_j| = 1 \Rightarrow$ center is nontrivial $\square$

More generally

Thm (Fixed pt Thm) $G \leq S$, G a p-gp, $|S|$ finite

Thm (Fixed pt Thm) $G \curvearrowright S$, G a p -gp, $|S|$ finite not a multiple of p . Then $\exists s \in S$ so that $O_s = \{s\}$, i.e. $g \cdot s = s \ \forall g \in G$.

If $S = G \setminus \{1\}$ then $G \curvearrowright S$ by conjugation and Thm then $\Rightarrow$ Propⁿ.

Pf of Thm $|S| = |O_{s_1}| + |O_{s_2}| + \dots + |O_{s_k}|$. Δ

Size of each orbit divides size of G

$\Rightarrow$ orbits are either singletons or are of size a multiple of p

$\Rightarrow$ Because $|S|$ is not a mult of p , must have at least one singleton on RHS of (Δ) . $\Rightarrow$

Propⁿ Every gp of order p^2 is abelian.

Pf: G a gp of order p^2 . $Z(G) \neq \{1\}$.

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

Assume for sake of contradiction $|Z(G)| = p$.

Then $\exists x \in G$ with $x \notin Z(G)$.

Then $Z(x) \ni \{x, Z(G)\} \Rightarrow |Z(x)| > p \Rightarrow |Z(x)| = p^2$

$\Rightarrow Z(x) = G \Rightarrow x \in Z(G) \rightarrow \text{contradiction}$. $\Rightarrow$

Cor If $|G| = p^2$, then either G is cyclic of order p^2 or G is a product of two cyclic gps of order p .

Pf: Every elt of G has order 1, p or p^2 .

• If $\exists$ elt of order p^2 , then $G \hat{=} C_{p^2}$ and we're done.

• Otherwise, every elt $\neq 1$ in G has order p .

Let $x \in G$ be such an elt. $\langle x \rangle \subsetneq G$

Let $y \in G$ be an elt not in $\langle x \rangle$.

Claim: $\text{mult}: \langle x \rangle \times \langle y \rangle \rightarrow G$

Pf: mult is a gp homom because x & y commute.

• Image is subgp of $G \neq \langle x \rangle \Rightarrow$ image is G

$\Rightarrow$ map is surj gp homom $\Rightarrow$ isom b/c both sides have size p^2 . $\square$
