Lecture 16

Last time

- $G \curvearrowright X \rightsquigarrow X = \bigsqcup G \cdot x_i$

  ($\bigsqcup$: partition; $G \cdot x_i = O_i$ (orbits))

- $O_i \simeq G/G_{x_i}$

  (G_{x_i}: stabilizer of x_i)

Example:

$S_3 \curvearrowright S_3$

$O = \{(123), (132)\}$, where $(123) = x$

$G_x = \{1, (123), (132)\}$

$$S_3/\{1, (123), (132)\} \xrightarrow{\sim} O$$

($\frac{6}{3} = 2$ el-ts) (2 el-ts)

$$gG_x \longmapsto g \cdot (123)$$

Applications

Counting formula 1

$$G \curvearrowright X$$ (G finite, X finite)

Let $\mathcal{O} \subset X$ (orbit), $x \in \mathcal{O}$

Then

$$|G| = |G_x| \cdot |\mathcal{O}| \,; \quad |\mathcal{O}| = [G : G_x]$$

proof. $\mathcal{O} \simeq G/G_x \Rightarrow |\mathcal{O}| = |G/G_x| = \dfrac{|G|}{|G_x|}$ ✓

Rem: counting formula is very useful if

one wants to count the number of el-ts in $\underline{G_x}$

__Ex__ $S_3 \curvearrowright \{(123), (132)\}$, with $(123) = x$

Counting formula $\Rightarrow |G_x| = 3 \Rightarrow G_x = \{1, (123), (132)\}$ (no other el-ts)

Counting formula 2

$$G \curvearrowright X = O_1 \sqcup \ldots \sqcup O_k, \quad x_i \in O_i$$

$\Downarrow$

$$|X| = |O_1| + \ldots + |O_k| = [G : G_{x_1}] + \ldots + [G : G_{x_k}]$$

__Example__ $S_3 \curvearrowright S_3$ (conjugation)

$$S_3 = \underbrace{\{1\}}_{O_1} \sqcup \underbrace{\{(12),(23),(13)\}}_{O_2} \sqcup \underbrace{\{(123),(132)\}}_{O_3}$$

$$G_1 = S_3, \quad G_{(12)} = \{1,(12)\} = \langle (12) \rangle, \quad G_{(123)} = \langle (123) \rangle$$

$$|S_3| = 6 = \frac{6}{6} + \frac{6}{2} + \frac{6}{3} \quad \checkmark$$

Concrete applications

← we now use general theory to prove two nontrivial results about groups

Proposition

G a finite group of order p^k (p a prime, $k \in \mathbb{Z}_{\geq 1}$)

↗ such groups are called p-groups

Then $Z \subset G$ ← center is nontrivial (recall that $Z = \{ g \in G \mid gh = hg \ \forall h \in G \}$)

proof: consider $G \curvearrowright G$ conjugation

$$G = O_1 \sqcup \dots \sqcup O_k$$

conj. classes

Element $g \in G$ lives in Z iff

$\{g\} = O_i$ for some i.

If $|O| > 1$, $|O|$ - divisor of p^k

$\Downarrow$

$p \mid |O|$

We see that $|G| = |Z| + p \cdot ?$

⇙

$p \mid |Z| \Rightarrow Z$ contains at least p elements

so Z - nontrivial

Example: D_8 - has $8 = 2^3$ elements

center is $\{1, r^4\}$ - nontrivial

Theorem (Cauchy's)

G - finite group, $p \mid |G|$ ← some prime number

Then G contains element of order p.

__proof.__

(1) G - p-group $(|G| = p^k)$

then take any non-identity $g \in G$,

let m - order of g. $m \mid |G| \Rightarrow m = p^\ell$ (for some $\ell > 0$)

$\Downarrow$

$p \mid m \Rightarrow g^{\frac{m}{p}}$ - has order p ✓

(2) G - abelian

__Strong__ induction on $|G|$:

take $g \in G$ - arbitrary non-identity

$H := \langle g \rangle \subset G$.

If p divides $|H|$ ($=$ order of g)

$\Downarrow$

$g^{\frac{|H|}{p}}$ ← has order p ✓

If $p \nmid |H| \Rightarrow p \mid |G/H|$

← quotient group

Induction hypothesis $\Rightarrow \exists\, xH \in G/H$ s.t.

$(xH)^p = H$. Let m ← order of x.

$(xH)^m = H \Rightarrow p \mid m \Rightarrow x^{\frac{m}{p}}$ ← has order p

✓

③ G ← arbitrary

↑

enough to prove that there exists

a non-trivial $H \subset G$

↑

p-group

Theorem (first Sylow's thm)

if $|G| = p^k \cdot n$ $(\gcd(p,n) = 1)$

$\Downarrow$

$\exists H \subset G$ s.t. $|H| = p^k$

H is called Sylow's <u>p-subgroup</u>

As we discussed:

<u>Sylow's first thm</u> $\Rightarrow$ Cauchy's thm

So our goal is to prove Sylow's first thm

Examples

$G = S_3, \quad p = 3 \Rightarrow |H| = 3, \quad H = \langle (123) \rangle$ works

$G = S_4, \quad p = 2 \Rightarrow |H| = 8$

Indeed, $H = D_8 \hookrightarrow S_4$!

proof of Sylow's thm

Strong induction on $|G|$.

If $p \mid Z$ (center of G) then $Z \supset N$ ← subgroup of order p

Set $\bar{G} := G/N \Rightarrow |\bar{G}| = p^{k-1} \cdot n$

Induction $\Rightarrow \exists\ \overline{H} \subset \overline{G}$

$\quad$ ↳ order $= p^{k-1}$

$$\begin{array}{ccc} G & \xrightarrow{\pi} & \overline{G} \\ \cup & & \cup \\ P & \longrightarrow & \overline{P} \end{array}$$

↳ $\pi^{-1}(\overline{P})$ ← subgroup of G

$$|P| = p \cdot |\overline{P}| = p^k \ ✓$$

Now assume $p \nmid Z$.

$$G = Z \sqcup O_{x_1} \sqcup \dots \sqcup O_{x_r}$$

↳ conj. classes of non-central elements

$$|G| = |Z| + \sum_{i=1}^{r} [G : G_{x_i}]$$

$p \mid |G|$, $p \mid |Z| \Rightarrow \exists i$ s.t. $p \nmid [G : G_{x_i}]$

Then $|G_{x_i}| = p^k \cdot ?$

G_{x_i} is **proper** subgroup of G

(x_i is non-central)

⇓

induction hypothesis ⇒ $H \subset G_{x_i}$

is

subgroup of order p^k ✓