Last time

- First Sylow's theorem:

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

$\exists H \subset G$, $|H| = p^k$ (H a Sylow p-subgroup)

we proved this thm. last time

- Today: second Sylow thm: Fix $H \subset G$ Sylow p-subgroup

a) if $H' \subset G$ another Sylow p-subgroup

$\Downarrow$ (so all of them are isomorphic)

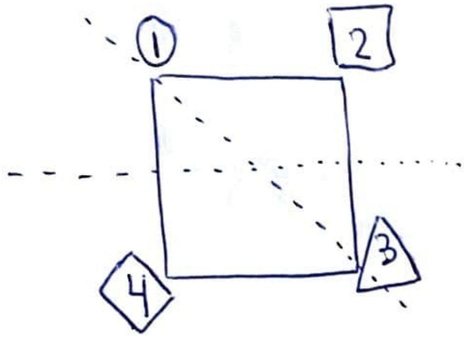
$\exists g \in G$ s.t. $H' = gHg^{-1}$

b) if $K \subset G$ any p-subgroup then $\exists g \in G$

s.t. $K \subset gHg^{-1}$

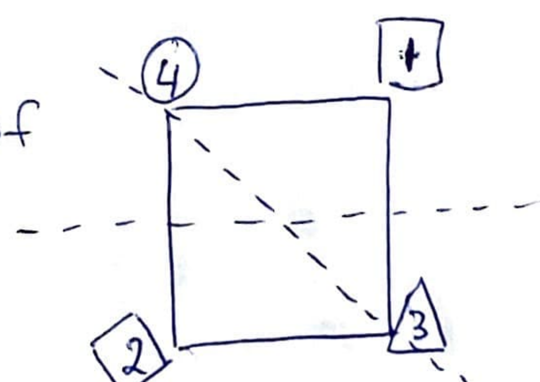
Example: $G = S_4$, $H = \langle (24), (14)(23) \rangle$

$(24) = s$, $(14)(23) = sr$



$H' = \langle (12), (13)(24) \rangle$

symmetries of



$\Rightarrow H' \simeq D_8 \simeq H$

Moreover, $H' = gHg^{-1}$ for $g:$
$$\begin{aligned} 1 &\mapsto 4 \\ 2 &\mapsto 1 \\ 4 &\mapsto 2 \\ 3 &\mapsto 3 \end{aligned}$$

$g = (142)$

of second Sylow thm

proof: enough to prove b)

$$\left(H' \subset gHg^{-1} \Rightarrow H' = gHg^{-1} \quad \& \quad |H| = |H'| \right)$$

To prove b), consider:

$$G \curvearrowright G/H =: X$$

$$g \cdot aH = gaH$$

$$K \subset G \Rightarrow K \curvearrowright X$$

subgroup

$$|X| = \frac{|G|}{|H|} = n \Rightarrow p \nmid |X|$$

Claim: $\exists x \in X$ s.t. $K_x = K$

This follows from the general lemma:

Lemma

If $K \curvearrowright X$, K a p-group, $p \nmid |X|$

$\Downarrow$

$\exists x \in X$ s.t. $K_x = K$

proof. $|X| = \sum' [K : K_{x_i}]$, $p \nmid |X|$

$\Downarrow$

$\exists x_i = x$ s.t. $p \nmid [K : K_x] = \dfrac{|K|}{|K_x|} = \dfrac{p^e}{|K_x|}$

$\Downarrow$

$|K_x| = p^e$ and $K_x = K$ ✓

So, we can find $x \in X$ s.t $K_x = K$

$\Downarrow$

$K \subset G_x$

Recall, $x = gH$ for some $g \in G$

$\Downarrow$

$G_x = gHg^{-1}$

We conclude that $K \subset gHg^{-1}$ ✓

<u>Upshot</u>: G a finite group, $|G| = p^k \cdot n$

- $\exists H \subset G$ $|H| = p$

- all of these H are <u>isomorphic</u> and are of the form gHg^{-1} for some g

- if $K \subset G$ a <u>any</u> p-subgroup $\Rightarrow K \subset gHg^{-1}$

<u>Final question:</u> how many of these H do we have?

<u>Answer:</u>

Thm (third Sylow's thm), $|G| = p^k \cdot n$

Let s = number of Sylow p-subgroups

<u>Then:</u> - $s \mid m$

- $s \equiv 1 \mod p$ $\left(\begin{cases} s \mid 2 \\ s \equiv 1 \mod 3 \end{cases} \Rightarrow s = 1 \right)$

<u>Example</u> $G = S_3$, $p = 3$ $\Rightarrow$ $H = \langle (123) \rangle$

only one $s = 1$

$|G| = 2^2 \cdot \underbrace{3}_{m}$ $\left(\begin{cases} s \mid 3 \\ s \equiv 1 \mod 2 \end{cases} \Rightarrow s \in \{1, 3\} \right)$

$G = S_4 \Rightarrow H = \begin{cases} \langle (24), (14)(23) \rangle \\ \langle (12), (13)(24) \rangle \\ \langle (14), (13)(24) \rangle \end{cases}$ $\underline{s = 3}, 1 \mid 3$

$3 \equiv 1 \mod 2$

proof.

Consider $G \curvearrowright X$ ← set of all Sylow p-subgroups

$$g \cdot H = gHg^{-1}$$

We know (by second Sylow thm) that

$G \curvearrowright X$ – transitive

Fix $H \in X$, $G_H = \{ g \in G \mid gHg^{-1} = H \}$

$$\begin{array}{c} G_H \\ \cup \\ H \end{array}$$

$$s = |X| = \frac{|G|}{|G_H|} \;\Big|\; \frac{|G|}{|H|} = m$$

$s \mid m$ ✓

Now consider $H \curvearrowright X$ (restriction of $G \curvearrowright X$ to H)

$H \in X$ is fixed by H.

To show that $s \equiv 1 \mod p$ enough to check that no other H' is fixed by H (use counting formula)

If H fixes $H' \Rightarrow \forall h \in H, \; hH'h^{-1} = H'$

so $H \subset G_{H'}$. Sylow p-subgroup of $G_{H'}$

But H' also lives in $G_{H'}$.

Second Sylow thm applied to $G_{H'}$

implies that $\exists g \in G_{H'}$ s.t. $gH'g^{-1} = H$

But $gH'g^{-1} = H'$ (see the definition of $G_{H'}$)

$\Downarrow$

$H = H'$ ✓

Why Sylow thms are important?

Many reasons, one is that using them one can <u>classify</u> <u>all</u> groups of order pq. ($p<q$ primes)

Thm: G a group, $|G| = pq$ then:

$$G \simeq (\mathbb{Z}/p\mathbb{Z}) \ltimes (\mathbb{Z}/q\mathbb{Z}) \text{ for}$$

some homomorphism $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\varphi} \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

How to describe homomorphisms?

Claim: $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}, +) \xleftarrow{\sim} ((\mathbb{Z}/q\mathbb{Z})^{\times}, \cdot)$

$$(x \mapsto mx) \longleftarrow m$$

So $\varphi \leftrightarrow$ element $m \in \mathbb{Z}/q\mathbb{Z}$

s.t. $\boxed{m^{p} = 1}$

Example $q = 5$, $p = \cancel{4}\ 2$

$\Downarrow$

$(\mathbb{Z}/5\mathbb{Z})^{\times} = \{1, 2, 3, 4\}$

$m = 1$ ✓

$m = 2$ ✗ $(2^2 = 4 \neq 1)$

$m = 3$ ✗ $(3^2 = 4 \neq 1)$

$m = 4$ ✓

$q = 5$, $p = 4$ $\Rightarrow$ $m = 1, 2, 3, 4$ ✓

How to prove thm. above (idea)

$p < q$

(1) $S \leftarrow$ number of q-subgroups of G

$$\left.\begin{array}{l} S \equiv 1 \mod q \\ S \mid p \quad (p < q) \end{array}\right\} \Rightarrow \underline{S = 1}$$

Pick $H \subset G$ Sylow q-subgroup

(2) $H \subset G$ normal (use that $S = 1$)

$\Rightarrow gHg^{-1} = H \quad \forall g \in G$

(3) $H \leftarrow$ cyclic $(|H| = q)$

(4) Pick any $K \subset G$ p-subgroup $(|K| = p)$

cyclic

(5) $K \xrightarrow{\varphi} Aut(H)$

$k \mapsto (h \mapsto khk^{-1})$

⑥ $K \simeq \mathbb{Z}/p\mathbb{Z}, \quad H \simeq \mathbb{Z}/q\mathbb{Z}$

$\varphi \leftarrow$ homomorphism $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

$$\begin{array}{ccc} (k,h) & \longmapsto & kh \\ \cap & & \cap \end{array}$$

⑦ $K \rtimes H \xrightarrow{\simeq} G$

homomorphism ✓

injective ✓

$(K \cap H = \{1\})$

is

$\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z})$