Last time: we defined solvable and nilpotent groups

has a subnormal series with abelian quotients

G is solvable

$\Leftrightarrow$ its derived series

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

(where $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$)

eventually reaches $G^{(k)} = 1$

G is nilpotent

$\Leftrightarrow$ its lower central series

$$\cdots \trianglelefteq G^{\{2\}} \trianglelefteq G^{\{1\}} \trianglelefteq G^{\{0\}} = G$$

(where $G^{\{i\}} = [G^{\{i-1\}}, G]$)

eventually reaches $G^{\{k\}} = 1$

Example: $S_3 \cong D_6$ is solvable ($S_3^{(1)} = A_3 \cong \mathbb{Z}/3\mathbb{Z} \Rightarrow S_3^{(2)} = 1$)

but not nilpotent ($S_3^{\{1\}} = A_3 \Rightarrow S_3^{\{2\}} = [A_3, S_3] = A_3 \Rightarrow \cdots \Rightarrow S_3^{\{k\}} = A_3 \ \forall k$)

$(132)(13)(132)^{-1}(13)^{-1} = (123)$

In a few weeks, we will fully classify finite nilpotent groups,

thus generalizing the classification of finite abelian groups.

Today: Sylow theorems 1,2,3

Motto: Maximal prime power order subgroup of a finite group G behave in a very controlled way

Fix p = prime number

Study groups G of order $p^n r$, $n \geq 0$, $(p,r) = 1$

Def: a sylow p-subgroup of such a G is a subgroup of order p^n.

Sylow theorem 1: Sylow p-subgroups always exist

Proof: induction by $|G|$

assume $n > 0$ otherwise trivial

(Judge can action below holds

Only one option left

Option 1: $\exists$ proper $H < G$ s.t. $[G:H]$ is coprime with p

$\Downarrow$

$|H| = p^n \pi'$ for some $\pi' | \pi$

$\Downarrow$

ind hyp says that H has a subgroup of order p^n. $\square$

Option 2: $\forall$ proper $H < G$, $p \mid [G:H]$

Class equation of G: $|G| = \sum_{\text{conj. classes } \tilde{g}} [G : C_G(\tilde{g})]$

every $C_G(\tilde{g})$ is a proper subgroup of G, except when $C_G(\tilde{g}) = G$, i.e. $\tilde{g} = \{\tilde{g}\}$ and $\tilde{g} \in Z(G)$

$\Downarrow$

$(\text{multiple of } p) = (\text{multiple of } p) + \underbrace{1 + \dots + 1}_{|Z(G)|}$

$\Downarrow$

p divides $|Z(G)|$, in particular, $Z(G) \neq \{e\}$

$\Downarrow$ (Prop 17)

$Z(G)$ has an element h of order $= p$

∇

define $H \cong \mathbb{Z}/p\mathbb{Z}$ subgroup generated by H

so $\overline{G} = G/H$ has order $p^{n-1}r$

↳ normal because $H \leq Z(G)$

So ind. hyp says that $\overline{G}$ has a subgroup $\overline{P}$ of order p^{n-1}

$\pi \uparrow$ $\uparrow$

$G \longleftarrow P = \pi^{-1}(\overline{P})$

Because all fibers of π have order p $\Rightarrow$ $|P| = p^n$

$\square$

Standard notation for Sylow p-subgroups: P.

Cor: a finite group G is a p-group $\Leftrightarrow$ $|G| \in p^{\mathbb{Z}}$

↳ every element has order in $p^{\mathbb{Z}}$

"$\Leftarrow$" follows from Lagrange

"$\Rightarrow$" assume $|G| = p^n r$ with $r \neq 1$

take a prime q which divides r

$\Downarrow$

G has a ~~non-trivial~~ Sylow Q-subgroup

any element of Q has order in $g^{\mathbb{Z}}$ ✂

Cor: the center of a non-trivial p-group is non-trivial

i.e. if $|G| = p^n$ for $n>0$, then $|Z(G)| = p^m$ for $m>0$.

because $|G| = p^n r$ with $r=1$, option 1 in the proof of Sylow 1 cannot hold $\Rightarrow$ option 2 holds $\Rightarrow p \mid |Z(G)| \mid p^n$ □

Sylow theorem 2: all Sylow p-subgroups of G are conjugates of each other, i.e.

given a Sylow p-subgroup $P \leq G$, then

$P' \leq G$ is a Sylow p-subgroup $\Leftrightarrow \exists\, g \in G$ s.t. $P' = gPg^{-1}$

Proof: "$\Leftarrow$" $P' = gPg^{-1}$ always a subgroup, b/c

$h_1, h_2 \in P$, $gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1}$

$|P'| = |gPg^{-1}| = |P| = p^n$

$(gh_1g^{-1} = gh_2g^{-1} \Leftrightarrow h_1 = h_2)$

so P' is a Sylow p-subgroup

↳ subgroup ↳ prime number

"$\Rightarrow$" P, P' are Sylow p-subgroup ; must find $g \in G$ s.t $P' = gPg^{-1}$

left action $P \curvearrowright G/P'$ = set of right cosets

$$h \cdot (gP') = hgP'$$

$$|G/P'| = \sum_{\text{orbits } P\cdot x} |\text{orbit}| \overset{\text{orbit-stab thm}}{=\!=} \sum_{\text{orbits } P\cdot x} \frac{|P|}{|\text{Stab}_P(x)|}$$

but $|P| \in p^{\mathbb{N}}$ hence $p \mid \frac{|P|}{|\text{Stab}_P(x)|}$ unless $\text{Stab}_P(x) = P$

not a multiple of p

$\Downarrow$

$\exists\, x = gP'$ s.t. s.t. $\text{Stab}_P(x) = P$, i.e. $hx = x \;\forall h \in P$

$\Updownarrow$

$hgP' = gP'$

$\Updownarrow$

$g^{-1}hgP' = P'$

$\Updownarrow$

$g^{-1}hg \in P'$

$\Updownarrow$

$h \in gP'g^{-1}$

$P \subseteq gP'g^{-1}$ $\Longleftarrow$

sylow p-subgroups, so $|P| = |P'|$

$\Downarrow$

$P = gP'g^{-1}$

□

$\exists$ unique Sylow p-subgroup P $\iff$ P is normal

$\Updownarrow$ $\Updownarrow$

$P = gPg^{-1}$ $\forall g \in G$

Sylow theorem 3:

$|G| = p^n r$, $(p, r) = 1$

let $n_p = \#$ Sylow p-subgroups of G

- $n_p = [G : N_G(P)]$ for any Sylow p-subgroup P
- $n_p \mid r$
- $n_p \equiv 1 \mod p$

Proof: $G \curvearrowright \{\text{Sylow } p\text{-subgroups}\}$

$g \cdot P = gPg^{-1}$

transitive, i.e. $\exists$ unique orbit by Sylow 2

$$n_p = |\{\text{Sylow } p\text{-subgroup}\}| = |\text{single orbit}| \overset{\text{O-S}}{=\!=} \frac{|G|}{|\text{Stab}_G(P)|}$$

$\Downarrow$!

$n_p = [G : \text{Stab}_G(P)]$

some fixed Sylow p-subgp

$$n_p = [G : \mathrm{Stab}_G(P)]$$

$$g \in \mathrm{Stab}_G(P) \iff g \cdot P = P \iff gPg^{-1} = P \iff g \in N_G(P)$$

$$\Downarrow$$

$$n_p = [G : N_G(P)]$$

but $P \subseteq N_G(P) \Rightarrow |P|$ divides $|N_G(P)|$

$$\Downarrow$$

$$n_p = \frac{|G|}{|N_G(P)|} \text{ divides } \frac{|G|}{|P|} = \frac{p^n r}{p^n} = r$$

fix a Sylow p-subgroup P

$$P \curvearrowright \{\text{Sylow } p\text{-subgroups}\}$$

$$g \cdot P' = gP'g^{-1}$$

not necessarily transitive

$$n_p = |\{\text{Sylow } p\text{-subgroup}\}| = \sum_{\text{orbits } P\cdot x} |P \cdot x| \overset{O\text{-}S}{=\!=} \sum_{\text{orbits } P\cdot x} \frac{|P|}{|\mathrm{Stab}_P(x)|}$$

p divides $\dfrac{|P|}{|\mathrm{Stab}_P(x)|}$ unless $\mathrm{Stab}_P(x) = P \iff P \cdot x = x$

($\mathrm{Stab}_P(x) = P$ means $|\mathrm{Stab}_P(x)| = p^n$)

$$n_p \equiv \#\{\text{of fixed points, i.e. } x \text{ s.t. } P\cdot x = x\} \quad \text{modulo } p$$

$$= \#\{\text{Sylow } p\text{-subgroups } P' \text{ s.t. } P\cdot P' = P'\} \quad \text{mod } p$$

$P\cdot P' = P'$

$\forall g \in P,\ g\cdot P' = P'$

$\Leftrightarrow$

$\forall g \in P,\ gP'g^{-1} = P'$

$\Leftrightarrow$

$P \subseteq N_G(P')$

$\Leftrightarrow$

$P = P'$

$n_p \equiv 1 \bmod p$ $\Leftarrow$ because $\exists$ single fixed Sylow p-subgroup for action $\circledast$, namely P' itself

Claim: $P \subseteq N_G(P') \iff P = P'$

"$\Leftarrow$" obvious

"$\Rightarrow$" $\dfrac{|G|}{|N_G(P')|} = \pi' \mid \pi$, so $|N_G(P')| = p^m \dfrac{\pi}{\pi'}$

P, P' are Sylow p-subgroups of $N_G(P')$

but $P' \trianglelefteq N_G(P') \rightsquigarrow P' = P$.

Application: Sylow 2-subgroups of D_{2N}

(Sylow p-subgroups of $\mathbb{Z}/N\mathbb{Z}$, $N = p^n\pi$.

$\exists$ a unique such subgroup, i.e. $\{0, r, 2r, \ldots, (p^n-1)r\}$)

Lemma: if $H \trianglelefteq G$, then $\forall$ Sylow p-subgroup $P \leq G$

then $H \cap P$ is a Sylow p-subgroup of H

Proof: a p-subgroup $P \leq G$ is Sylow $\iff$ $p \nmid [G:P]$

2^{nd} iso theorem $\Rightarrow |HP| = \dfrac{|H|\,|P|}{|H \cap P|} \Rightarrow [HP:P] = [H: H \cap P]$.

but $HP \leq G$ so $[HP:P] \mid [G:P]$ not a multiple of p

hence $p \nmid [HP:P] = [H: H \cap P] \Rightarrow H \cap P$ is Sylow of H

is a p-group because P is a p-subgroup

$\mathbb{Z}/N\mathbb{Z} \trianglelefteq D_{2N}$; take any $P < D_{2N}$

Sylow 2-subgroup ; $N = 2^n r$

Lemma: $P \cap \mathbb{Z}/N\mathbb{Z}$ = a Sylow 2-subgroup of $\mathbb{Z}/N\mathbb{Z}$

$= \{0, r, 2r, \ldots (2^n-1)r\}$.

cardinality 2^n

but $|P| = 2^{n+1}$

$$P = \{0, r, \dots, (2^n-1)r\} \sqcup \{0, r, \dots, (2^n-1)r\} \cdot \tau$$

for some right coset representative τ ; τ can't be a rotation, else the entire 2^{n+1}-sized group P would be contained in the $2^n r$-sized group of rotations $\Rightarrow$ τ reflection

P is completely determined by τ, but changing τ by another coset representative does not change P $\Rightarrow 2^n$ choices of τ produce same P

$$n_2 = \frac{|\text{reflections } \tau|}{|\text{reflections } \tau \text{ in the same } \{0, r, \dots, (2^n-1)r\} \text{ coset}|} = \frac{2^n \cdot r}{2^n} = r$$

This upholds Sylow 3