Lec 18

G - finite grp. Fix prime p. Write $\# G = p^e \cdot m$ $\rightsquigarrow$ $p \nmid m$ $\rightsquigarrow$ no divisib

Defn a p-Sylow subgrp of G is a subgrp of order p^e

Eg let $G = S_n$.

- if $n < p$ $\Rightarrow$ $p \nmid \# S_n \Rightarrow$ p-Sylow is trivial
- if $n = p$ $\Rightarrow$ p exactly divides ($p \| \# S$) $\Rightarrow$ the subgps gen'd by a p-cycle is a p-Sylow

  $\boxed{p \mid \# S \text{ but } p^2 \nmid \# S}$ $\leftarrow$ not bigger
- in fact for $p \le n < 2p$ $p \| \# S_n$ and get same answer.
- If $n = 2p$, p is odd, $p^2 \| \# S_n$,

  G a p-Sylow by taking the subgrp gen'd by two disjoint p cycles eg

  $(1\ 2\ 3 \dots p)$ and $(p{+}1 \ \dots \ 2p)$
- If $p \neq 2, 3$ get p-sylow by 3 disj p cycles.
- if $n = p^2$ $\Rightarrow$ $p^{p+1} \| \# S_{p^2}$ $\to$ p disj p cycles not enough

$$1 \ \cdots\ p \mid p{+}1 \cdots 2p \mid \cdots \mid p^2 - p + 1 \ \cdots \ p^2 \mid$$

σ_1, σ_2, σ_p, τ

need to

$$\tau = (1\ \ p{+}1\ \ 2p{+}1 \cdots p^2 - p + 1)(2\ \ p{+}2\ \ 2p{+}2 \cdots) \cdots (p\ \ 2p \cdots)$$

$$\tau \sigma_1 \tau^{-1} = \sigma_2 \Rightarrow \tau \sigma_i \tau^{-1} = \sigma_{i+1} \ (i{+}1 \bmod p)$$

so want p Sylow gen by $\underline{\sigma_1, \dots \sigma_p, \tau}$

rinse and repeat for $p^2 + p \ \dots\ , p^3, \dots$

First Sylow Thm

Every grp $_{\wedge}^{\text{finite}}$ has a p-Sylow grp

Cor | Cauchy's Thm if $p \mid \# G \Rightarrow G$ has elt of ord p.

$\hookrightarrow$ find the elt in the p-Sylow

let p-Sylow H. let $h \neq 1 \in H$.

$\operatorname{ord}(h) \mid p^e \Rightarrow \operatorname{ord}(h) = p^k \Rightarrow \operatorname{ord}(h^{p^{k-1}}) = p$

Second Sylow Thm

Say $K \leq G$ subgrp. $H \leq G$ is p-Sylow

$\exists g \in G$ so $gHg^{-1} \cap K$ is a p-Sylow subgrp of K

Cor | All p-Sylows of G are conjugate.

Apply Thm where H, K are p-Sylows of G.

$\exists g \in G$ so $gHg^{-1} \cap K$ p-Sylow of K.

$\# H = \# gHg^{-1} = \# K = p^e$

$gHg^{-1} \cap K$ has order p^e (order of $K = p^e$ so order of p-Sylow p^e)

$\Rightarrow$ only p Sylow of K is K

$\Rightarrow gHg^{-1}$ & K ord p^e and so does int $\Rightarrow gHg^{-1} = K$

Cor | Every p-subgrp of G is contained in a p-Sylow of G

let K be the p subgrp.

Third Sylow Thm

$\# G = p^e \cdot m$. let s = num of p-Sylow subgrps.

Then, 1) $s \mid m$

2) $s \equiv 1 \pmod p$

Rmk | $s = 1 \iff$ the p-Sylow of G is normal.

Pf of 1) let $\mathcal{S} = \{ S \subseteq G \mid \#S = p^e \}$
subset

$G \curvearrowright \mathcal{S}$ by left mult $(g,S) \longmapsto S$

Note: $\#\mathcal{S} = \binom{p^e \cdot m}{p^e} = \dfrac{(p^e m)!}{p^e! \, (p^e m - p^e)!}$

Lemma) $p \nmid \#\mathcal{S}$ → all the p's above cancel in numerator & denom

Let $S_1, \dots, S_r$ be rep of orbits of G on $\mathcal{S}$

$\mathcal{S} = O_{S_1} \sqcup \dots \sqcup O_{S_r} \Rightarrow \#\mathcal{S} = \sum_{i=1}^{r} \#O_{S_i}$

Since $p \nmid \#\mathcal{S} \Rightarrow p \nmid \#O_{S_i}$ for some $i \in \mathbb{N}_r$ call $S_i = S$

hence $S \in \mathcal{S}$ s.t $p \nmid \#O_S$

By orbit stabilizer thm

$\#\mathrm{Stab}(S) \cdot \#O_S = p^e \cdot m$

no p's

let $H = \mathrm{Stab}(S)$ orbits of $H \curvearrowright G$ by left mult

are the cosets Hg of H in G

orbit of G?

think abt this

Since S is H stable, it is a union of H-orbits.

$S = Hg_1 \sqcup \dots \sqcup Hg_k \Rightarrow \#H \mid \#S = p^e$

$\Rightarrow \#H = p^a \Rightarrow \#H = p^e$