lecture 17, 10/11/2015

Sylow's Theorems (1878)

We strengthen Cauchy's Thm.

Fix a finite group G of order n, p a prime.

Thm (Sylow I) If $p^i | n$, G has a subgp of order p^i.

Pf: By induction on i. For $i=0$ nothing to prove

For $i=1$, this is Cauchy's thm.

Suppose $p^{i+1} | n$, $i \geq 1$. let $H < G$ be a subgp of order p^i.

Idea: Fix p-subgp H' s.t. H normalizes H'. Then HH' is a subgp of order dividing $|H| \cdot |H'|$, a power of p.

For this let H act by translation on G/H.

This is an action of the p-gp H ($i \geq 1$) on a set of size $\frac{n}{p^i} = p \cdot \frac{n}{p^{i+1}}$

We know: $\#\mathrm{Fix}(H) \equiv |G/H| \equiv 0 \ (p)$. Also H fixes the coset $H \in G/H$ so H has at least p fixed points.

Suppose gH is fixed by H, i.e. if $h \in H$ then $hgH = gH$

so $g^{-1}hgH = H$ so $g^{-1}hg \in H$.

But also $h \cdot gHg^{-1} = gHg^{-1}$. so $h \in gHg^{-1}$.

so $H \subset gHg^{-1}$. But $|gHg^{-1}| = |H|$ so $H = gHg^{-1}$.

Conclusions: $gH \in \mathrm{Fix}(H)$ iff $g \in N_G(H)$,

So $\mathrm{Fix}(H) = N_G(H)/H$. But $H \trianglelefteq N_G(H)$, and we get that p divides the order of the group $N_G(H)/H$.

By Cauchy's thm, $N_G(H)/H$ has a subgp C of order p

By Correspondence thm, its inverse image in $N_G(H)$ has order p^{i+1}. ∎

Recall: Thm Let $N \trianglelefteq G$. Then maps $H \mapsto q(H)$, $q^{-1}(C) \longleftarrow\!\shortmid C$ | $q: G \to G/N$ quotient map

give a bijection of $\{$subgps of G containing $N\} \longleftrightarrow \{$subgps of $G/N\}$.

preserves index, normality, containment.

e.g. $[q^{-1}(C) : N] = [C : \underbrace{q(N)}_{\{e\}}] = |C|$

(proved in PS7)

---

recap of pf of Sylow I: given H, wanted $H' \supset H$, order p^{r+1}.

Enough to find C in $N_G(H)/H$ of order p

By Cauchy, enough to prove $p \mid [N_G(H) : H]$.

(Also necessary: if H' p-gp, $H < H'$ of index p then $H \trianglelefteq H'$ so $H' < N_G(H)$)

Conclusion: If $n = p^r \cdot m$, $p \nmid m$, then G has subgps of order p^r.

In fact, any p-subgp H is contained in a subgp of order p^r.

Def: In any gp G, a maximal (by inclusion) p-subgp is called a *p-Sylow subgroup*. Write $Syl_p(G)$ for the set of those, $n_p(G)$ for their number.

Saw: If G is finite, $p^r \| n = \#G$, then $P < G$ is a p-Sylow subgp iff $\#P = p^r$.

Examples: If G has order 24, 2-sylow subgps have order 8,
3-sylow " " " 3.

Lemma: Let P be a normal p-Sylow subgp. Then P contains all p-subgps of G, hence is the unique p-Sylow subgp

Pf: Let P' be another p-subgp. Thm 2nd isom thm we proved that $PP'=P'P$ is a subgp. This is a p-gp:

Let $g \in P'P$. By 2nd isom thm, $P'P/P \cong P'/P\cap P'$.

Now P' is a p-gp, so $P'/P'\cap P$ is a p-gp, so image of g in PP'/P is a p-element so g^{p^r} maps to e for some r, which means $g^{p^r} \in P$. But P is a p-gp too, so order of g^{p^r} is a power of p, ie.

$$(g^{p^r})^{p^s} = e \quad \text{by} \quad (g^{p^r})^{p^s} = g^{p^r \cdot p^s} = g^{p^{r+s}}. \qquad \blacksquare$$

We just saw PP' is a p-subgp, containing P.
But P is a max'l p-subgp, so $P'P = P$, so $P' \subset P'P = P$. $\blacksquare$

Converse also true: suppose P is the unique p-Sylow subgp, consider gPg^{-1}. This is also a p-Sylow subgp (conjugation is an automorphism) so $gPg^{-1} = P$.

Ex: directly show gPg^{-1} is a p-subgp, maximal such.

$n = p^r m$, $p \nmid m$

Thm: (Sylow II, III) The p-Sylow subgps of G (finite!) are all conjugate (so $n_p(G) \mid n$). Moreover, $n_p(G) \equiv 1 \ (p)$ (so $n_p(G) \mid m$)

Pf: Let $P \in \mathrm{Syl}_p(G)$, consider action of P on $\mathrm{Syl}_p(G)$ by conjugation. P fixes P' iff $P < N_G(P')$. But P' is a normal Sylow subgp of $N_G(P')$ hence so $P < N_G(P')$ iff $P' = P$. So P is the unique fixed point. Also, P is a finite p-gp, so $1 = \#\mathrm{Fix}(P) \equiv \#\mathrm{Syl}_p(G) = n_p(G) \ (p)$

Now let $C = \{ gPg^{-1} \mid g \in G \}$ be the conjugacy class of P.
Want to show $C = Syl_p(G)$.
Suppose not. Then there is $P' \in Syl_p(G)$, but $P' \notin C$
Consider actions of G and P' on C by conjugation.

① P' has no fixed points in C (its only fixed point on $Syl_p(G)$ is $P' \notin C$)

so $\#C \equiv 0 \ (p)$

② Also $\#C = [G : N_G(P)] \mid [G:P] = \frac{p^r \cdot m}{p^r} = m$

but $p \nmid m$ - contradiction.

So $C = Syl_p(G)$, all are conjugate ∎

Then let G be a finite gp, $\#G = n = p^r \cdot m$, $p \nmid m$.

Then:

1. G has subgps of order p^r.
2. they are all conjugate, $n_p(G) \mid m$.
3. $n_p(G) \equiv 1 \ (p)$

Example: suppose $n = 12 = 2^2 \cdot 3$. $n_2(G) \mid 3$ so $n_2(G) \in \{1, 3\}$.
$n_3(G) \mid 4$, $n_3(G) \equiv 1 \ (3)$ so $n_3(G) \in \{1, 4\}$.

Example: suppose $n = 30 = 2 \cdot 3 \cdot 5$.
$n_3(G) \mid 10$, $n_3(G) \equiv 1 \ (3)$ so $n_3(G) \in \{1, 10\}$
$n_5(G) \mid 6$, $n_5(G) \equiv 1 \ (5)$ so $n_5(G) \in \{1, 6\}$