Lecture 15: Sylow Theorems

Aim Lecture: Examine fundamental partial converse to Lagranges Thm.

This lecture, fix prime p.

$\boxed{\text{Some Lemmas}}$

Lemma 1: Let $q, n \in \mathbb{N}$, g.c.d. $(p,q)=1$. Then
$$\binom{p^n q}{p^n} \equiv q \mod p$$

Proof: We expand in $\mathbb{F}_p[x,y]$ using Frobenius:

$$(x+y)^{p^n q} = (x^{p^n}+y^{p^n})^q = x^{p^n q} + q x^{p^n(q-1)} y^{p^n} + \dots$$
$$\| $$
$$x^{p^n q} + \dots + \binom{p^n q}{p^n} x^{p^n(q-1)} y^{p^n} + \dots$$

in $\mathbb{F}_p$

$\square$

Let G = group & $H \leq G$. Then any $J \leq G$ acts naturally on G/H by
$$\underset{\uparrow J}{j} . (\underset{\uparrow G/H}{gH}) := jgH.$$

Lemma 2: $(G/H)^J = \{gH \mid g^{-1} J g \leq H\}$.
In particular, if $(G/H)^J \neq \emptyset$ iff J is contained in some conjugate of H.

Proof:
$$gH \in (G/H)^J \iff jgH = gH \ \forall j \in J$$
$$\iff g^{-1} j g H = H \ \forall j \in J$$
$$\iff g^{-1} j g \in H \ \forall j \in J.$$

Sylow Theorems

Thm: Let G = group order $p^n q$, g.c.d.$(p,q)=1$. Then

(I) There exists a Sylow p-subgroup P.

(II) Any p-subgroup H (i.e. subgroup which is also a p-group) is contained in a conjugate of P.

In particular, any 2 Sylow p-subgroups are conjugate.

E.g.

$$S_3$$

$$\langle(123)\rangle \qquad \langle(12)\rangle \quad \langle(13)\rangle \quad \langle(23)\rangle$$

Sylow 3-subgroup   conjugate Sylow 2-subgroups

Proof Thm: (I) Let $X = \{S \subseteq G \mid |S| = p^n\}$.

G acts on X by $\underset{G}{g} . \underset{X}{S} = gS = \{gs \mid s \in S\}$.

Lemma 1 $\Rightarrow$ $|X| \equiv q \not\equiv 0 \mod p$.
Hence X has a G-orbit $G.S$ with $p \nmid |G.S|$.

Claim: $P := \mathrm{Stab}_G S$ is a Sylow p-subgroup.
Why? $[G:P] = |G.S|$ is coprime to p so $p^n \mid |P|$. Suffice now show $|P| \le p^n = |S|$ to prove claim & $\therefore$ Thm (I). Let $s \in S \subseteq G$. Since

P stabilises S, $gs \in S$ $\forall g \in P$ & $\therefore$
$Ps = \{gs \mid g \in P\} \leq S$
$|P| = |Ps| \leq |S|$.

$\square$

Now prove (II). We let the p-subgroup H act on G/P. Lect. 14 lemma $\Longrightarrow$

$$|(G/P)^H| \equiv |G/P| \mod p$$
$$= q \neq 0 \mod p.$$

Hence $(G/P)^H \neq \emptyset$ & Thm (II) follows from Lemma 2. $\square$

<u>Rem</u>: We omit Sylow's Thm (III): no. Sylow p-subgroups is $\equiv 1 \mod p$ & divides q.

Insert Prop^n

$\boxed{\text{Fundamental Thm of Algebra}}$

<u>Thm</u>: Any non-constant $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

Proof: We assume the followings facts about $\mathbb{R}$:

(a) If $g(x) \in \mathbb{R}[x]$ has odd degree then g has a real root.

(b) Any positive real has a real square root so quadratic formula & polar forms $\Longrightarrow$

(b') If $f(x) \in \mathbb{C}[x]$ has deg 2 then f has a root in $\mathbb{C}$.

Assume thm false so there's an irred. $f(x) \in \mathbb{C}[x]$ of deg ≥ 2. Its splitting field $/\mathbb{C}$ gives a non-trivial finite field $\text{ext}^{\underline{n}}$ $K/\mathbb{C}$. Replacing $K/\mathbb{R}$ with its Galois closure we may assume $K/\mathbb{R}$ Galois.

Let $G = \mathrm{Gal}(K/\mathbb{R})$ & $P \leq G$ be a Sylow 2-subgroup. Primitive elt thm (Lect. 11) $\Rightarrow K^P = \mathbb{R}(\alpha)$. Let $g(x)$ be min. poly. for $\alpha / \mathbb{R}$.

$$\deg g(x) = [K^P : \mathbb{R}] = \frac{[K:\mathbb{R}]}{[K:K^P]} = \frac{|G|}{|P|}$$

which is odd.

Then ⓐ $\Rightarrow \deg g = 1 \Rightarrow G = P$, a 2-group. Lect. 14 $\text{Prop}^{\underline{n}}$ 2 $\Rightarrow \exists$ normal chain of subgroups

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots$$

with factors $\simeq \mathbb{Z}/2\mathbb{Z}$.

$\therefore K^{G_1}$ is a deg 2 $\text{ext}^{\underline{n}}$ of $K^G = \mathbb{R}$ so by ⓑ & quadratic formula, $K^{G_1} = \mathbb{C}$. Also K^{G_2} is a deg 2 $\text{ext}^{\underline{n}}$ of $K^{G_1} = \mathbb{C}$, which doesn't exist by ⓑ'. $\square$

Move back up

$\underline{\text{Prop}^{\underline{n}}}$: Any group G of order $2p^n$, $n \in \mathbb{N}$ is solvable.
Proof: Can assume p odd. Any Sylow p-subgroup P is solvable being a p-group. Also $P \triangleleft G$ $\because [G:P] = 2$, $G/P \simeq \mathbb{Z}/2\mathbb{Z}$ solvable $\Rightarrow G$ is too. $\square$