Lecture 13

(13.0) Recall that (see Lecture 10, page 6):

For $p \in \mathbb{Z}_{\geq 2}$ prime, $r, m \geq 0$: $\binom{p^r \cdot m}{p^r} \equiv m \pmod{p}$.

The following crucial idea was used in the proof (see (10.7)):

> if $G \curvearrowright X$ and $|G| = p^r$ (a power of prime)
> then $|X| \equiv |X^G| \pmod{p}$.

Proof. - As X breaks into a disjoint union of G-orbits:

$$|X| = \sum_{\substack{\mathcal{O}: \text{orbit} \\ \text{under } G\text{-action}}} |\mathcal{O}|$$

For each orbit $\mathcal{O}$, $|\mathcal{O}|$ divides $|G| = p^r$. Thus $|\mathcal{O}| = 1$ or $|\mathcal{O}| \equiv 0 \pmod{p}$. Hence we get:

$$|X| \equiv \#\text{ orbits of size } 1 \pmod{p}$$

Orbits of size $1 = \{x \in X \mid g.x = x \ \forall\, g \in G\} =: X^G$

So $|X| \equiv |X^G| \pmod{p}$ as claimed. □

(13.1) An interesting application. -

The highlighted statement from the previous page is an example of an "abstract result". It applies uniformly to all groups of size = power of a prime.

Definition. A finite group G will be called a <u>p-group</u> if $|G| = p^r$ for some $r \geq 0$. (let's exclude $r = 0$ {e} group of size p^0.)

Now let us see an interesting special case: G : a p-group acting on itself by conjugation.

So we get : $\underline{\#\text{ fixed points}} \equiv |G| = 0 \pmod p$.

$\#\{ x \in G \mid gxg^{-1} = x \ \forall\, g \in G \}$ ← defined to be <u>center of G</u>, denoted by $Z(G)$.

Thus we obtain another abstract result :

$$|G| = p^r \Rightarrow |Z(G)| = p^s$$

for some s: $1 \leq s \leq r$ (s <u>cannot</u> be 0 because $|Z(G)| = 0 \bmod p$.)

Note : $Z(G) \trianglelefteq G$ is <u>a normal abelian subgroup of G.</u>

So it seems we can say something "inductively" for every p-group:

G: p-group, say of size p^r

$\downarrow \nabla$

$Z(G)$: abelian, normal subgroup of size p^s $(1 \le s \le r)$

$\rightsquigarrow$

$\overline{G} = G/Z(G) =: G_1$ a smaller p-group (strictly) size: p^{r-s} $(1 \le s \le r)$

Base case: $|G| = p \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$. In particular we know that every $g \in G \setminus \{e\}$ generates G (its order has to divide p, and is not 1, so it must be p.); i.e.

$G = \{e, g, g^2, \dots, g^{p-1}\}$ for any choice of $g \in G \setminus \{e\}$.

We record the inductive observation made above in the following

Proposition. - Let G be a p-group. Then there exists a chain of normal subgroups

$$\{1\} \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots \trianglelefteq Z_r = G$$

such that each quotient Z_{i+1}/Z_i is abelian (of necessarily a p-group) p-group.

$(1 \le i \le r-1)$

(13.2) Now assume $|G| = n$ and p is a prime number.

Let us write $n = p^r \cdot m$ where $\gcd(p, m) = 1$ (m is not divisible by p).

Theorem. (Sylow). –

Part 1. – There exists a subgroup $P \leq G$ such that

$$|P| = p^r.$$

[Definition. – A <u>Sylow p-subgroup</u> of G is any subgroup $H \leq G$, which is a p-group and p does not divide $(G : H)$, index of H in G, which - recall - is same as $\frac{|G|}{|H|}$.]

Part 2. – Let P_1, P_2 be two Sylow p-subgroups of G. Then there exists $g \in G$ such that $P_2 = g P_1 g^{-1}$.

[Meaning. – Let Sylow(p) = set of all Sylow p-subgroups of G. $\circlearrowleft_G$ by conjugation (i.e. $g : H \longmapsto gHg^{-1}$.)

Then this action is <u>transitive</u> (i.e., there is only one G-orbit)]

Part 3. – Let $n_p = \#\{\text{Sylow } p\text{-subgroups of } G\}$. Then

$$\boxed{\begin{array}{l} n_p \equiv 1 \pmod p \\ n_p \text{ divides } m \end{array}}$$

(recall: $|G| = p^r \cdot m$.)

(13.3) Proof of Sylow Theorem - Part 1. -

Let X = set of all p^r-element subsets of G.

$G \circlearrowright$ $\quad g \cdot \{\sigma_1, \sigma_2, \dots, \sigma_{p^r}\} = \{g\sigma_1, g\sigma_2, \dots, g\sigma_{p^r}\}$.

Observation 1. - If $H = \{h_1, \dots, h_{p^r}\} \in X$

$$\text{Stab}_G(H) = \{g \in G \text{ such that } g \cdot H = H\}$$

in particular $g h_1 = h_i$ for some $1 \le i \le p^r$;

meaning $g = h_i h_1^{-1}$ ( )

$\Rightarrow$ $\text{Stab}_G(H) \subseteq \{e, h_2 h_1^{-1}, \dots, h_{p^r} h_1^{-1}\}$; hence,

$$\boxed{|\text{Stab}_G(H)| \le p^r} \quad \forall\, H \in X.$$

(note: if we get equality, we have proved the theorem - p.1.)

Observation 2. - $|X| = \binom{p^r \cdot m}{p^r} \equiv m \pmod p$

$\neq 0 \pmod p$.

As $|X|$ = sum of sizes of orbits, there must be some orbit, say $\mathcal{O} \subset X$, such that $|\mathcal{O}| \not\equiv 0 \pmod p$.

Pick $H \in \mathcal{O}$. Then $|\text{Stab}_G(H)| = \dfrac{|G|}{|\mathcal{O}|} = \dfrac{\overleftarrow{p^r \cdot m}}{\underleftarrow{\text{not divisible by } p}} = p^r \cdot m'$

But $|\text{Stab}_G(H)| \le p^r$, so $m' = 1$ and

$\text{Stab}_G(H)$ is a Sylow p-subgroup. $\square$

(13.4) Proof of Sylow Theorem - Part 2. -

We will prove a slight generalization: let $H, P \leq G$ s.t.

H is a (sub) p-group of G

P is a Sylow p-subgp of G.

Claim: $\exists\ g \in G$ such that $H \subset gPg^{-1}$.

Let us think about the assertion of the claim. If $H \subset gPg^{-1}$ we have: $H \cdot g \subset g \cdot P$, i.e. $H \cdot gP \subset g \cdot P$.

Meaning: the coset $g \cdot P \in G/P$ is fixed by H.

So let us consider $H \curvearrowright G/P$ $\quad h \cdot (gP) = hgP$.

(H: p-group; G/P: has m elements & $m \not\equiv 0 \pmod p$.)

By the general rule stated and proved on page #1:

$$0 \not\equiv m = |G/P| \equiv \#\, H\text{-fixed points in } G/P \pmod p$$

so there is atleast one fixed point, i.e. $\exists\ g \in G$ s.t.

$$h(gP) = gP \quad \forall\ h \in H$$

i.e. $H \subset gPg^{-1}$. $\square$

(13.5) Proof of Sylow Theorem - part 3. -

Let $\mathcal{S}_p$ = set of Sylow p-subgroups of G. So far we know:

$\mathcal{S}_p \neq \phi$ (Part 1) $\quad G \curvearrowright \mathcal{S}_p$ is a transitive action.

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

Let $n_p = \# \mathcal{S}_p$. As $\mathcal{S}_p$ is a single orbit, we know

$$\boxed{n_p \text{ divides } |G| = p^r \cdot m}$$

We want to show $n_p \equiv 1 \pmod{p}$, using our guiding principle on page 1.

Choose $P_0 \in \mathcal{S}_p$ and let $P_0 \curvearrowright \mathcal{S}_p$ (restriction of $G \curvearrowright \mathcal{S}_p$)

$$\begin{array}{ccc} \psi & & \psi \\ \sigma & & P \end{array} \quad \rightsquigarrow \left(\sigma \cdot P = \sigma P \sigma^{-1}\right).$$

Again: $|\mathcal{S}_p| \equiv \#\, P_0\text{-fixed points in } \mathcal{S}_p \pmod{p}$

$$\| \; n_p$$

Thus it would suffice to show: $\boxed{P_0\text{-fixed points in } \mathcal{S}_p = \{P_0\}.}$

Let $Q \in$ P_0 – fixed points in $\mathcal{S}_p$. That is, $Q \leq G$ is another Sylow p-subgroup of G and ~~$pQp^{-1} = Q \ \forall p \in P_0$~~.

$xQx^{-1} = Q; \forall x \in P_0$.

Consider $H := \{ g \in G \text{ such that } gQg^{-1} = Q \} \leq G$.

$P_0 \leq H$
$Q \leq H$
} are 2 Sylow p-subgroups of H.

(Why: $|G| = p^r \cdot m$ & $H \leq G \Rightarrow |H|$ divides $|G|$.

But $P_0 \subset H \Rightarrow |H| = p^r m'$

(m' some divisor of m).

As $\gcd(p, m) = 1 \Rightarrow$ Sylow p-subgroups of H must also have size p^r.)

By Part 1 of Sylow theorem, $\exists\ h \in H$ s.t. $hQh^{-1} = P_0$.

But by definition of H, $hQh^{-1} = Q$. So $Q = P_0$ as we wanted to prove. $\square$