Lecture 6

(6.0) Recall : so far we proved
- Counting lemmas
- Isomorphism theorems

In last lecture we established some (3) equivalent ways of defining semidirect products.

Today we are going to use counting lemmas to study p-subgroups.

Reminder : $G \curvearrowright X$ (group G acting on a set X) implies (see Lemma 2.4 page 5 / Lemma 2.6 page 8)

(i) $$|G\cdot x| = \frac{|G|}{|\mathrm{Stab}(x)|} \quad \text{for any } x \in X$$

where $$G\cdot x = \{y \in X : \exists\, g \in G \text{ so that } g\cdot x = y\} \subset X$$
$$\mathrm{Stab}(x) = \{g \in G : g\cdot x = x\} \subset G$$

(ii) $$|X| = \sum_{\alpha \in G\backslash X} |G\cdot x_\alpha| = \sum_{\alpha \in G\backslash X} \frac{|G|}{|\mathrm{Stab}(x_\alpha)|}$$

where $\forall\, \alpha \in G\backslash X$, x_α is a representative from G-orbit α.

(iii) $$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $$X^g = \{x \in X : g\cdot x = x\} \quad \text{(fixed points of } g \in G\text{)}$$

(6.1) Let p be a prime number.

Definition A group G is said to be a p-group if

$$|G| = p^k \text{ for some } k \in \mathbb{Z},\ k \geq 1.$$

e.g. $\mathbb{Z}/p^k\mathbb{Z}$ is a p-group.

Lemma. Let G be a p-group acting on a (finite) set X. Then

$$|X| \equiv |X^G| \pmod{p}$$

where $X^G = \bigcap_{g \in G} X^g = \{x \in X : g.x = x \ \forall g \in G\}$

Proof. By Lemma 2.4 (see (ii) of §6.0 above)

$$|X| = \sum_{\alpha \in G\backslash X} |G.x_\alpha| = |X^G| + \sum_{\substack{\alpha \in G\backslash X \\ \text{s.t.} \\ |G.x_\alpha| > 1}} |G.x_\alpha|$$

($|X^G|$: elements whose orbit is a singleton)

but $|G.x|$ divides $|G| = p^k$ (say). So, if $|G.x| > 1$ then

$(\forall x \in X)$ $\qquad |G.x| \equiv 0 \pmod{p}$.

Hence $|X| \equiv |X^G| \pmod p$ □

(6.2) Let n be a positive integer, and p be a prime.

Write $n = p^r \cdot m$ where p does not divide m.

Lemma. $\binom{n}{p^r} \equiv m \pmod p$

Proof. Let $G = \mathbb{Z}/p^r\mathbb{Z}$ and $T = \{a_1, \dots, a_m\}$ (just a set with m elements)

$X := G \times T$ $\quad \mathcal{E} := \{Y \subset X : |Y| = p^r\}$

so that $|X| = p^r \cdot m = n$ and $|\mathcal{E}| = \binom{n}{p^r}$.

Let G act on X by: $g \cdot (h, a) = (g+h, a)$

$\forall\, g, h \in G,\ a \in T.$

Then G acts on $\mathcal{E}$ by: for $g \in G$, $Y = \{y_1, \dots, y_{p^r}\} \in \mathcal{E}$

$$g \cdot Y = \{g \cdot y_1, \dots, g \cdot y_{p^r}\} \in \mathcal{E}.$$

Claim: $\forall\, 1 \le j \le m$, set $Y_j = \{(g, a_j) : g \in G\} \in \mathcal{E}$

Then $\mathcal{E}^G = \{Y_1, \dots, Y_m\}$

Given the claim, we get, using Lemma 6.1,

$|\mathcal{E}| \equiv |\mathcal{E}^G| \pmod p$. Now $|\mathcal{E}| = \binom{n}{p^r}$ and

$|\mathcal{E}^G| = m$. Hence, $\binom{n}{p^r} \equiv m \pmod p$.

Proof of the claim: $Y_j \in \mathcal{E}^G$ is clear. Conversely, $(\forall\ 1 \le j \le m)$

let $Y \in \mathcal{E}$ be such that $g \cdot Y = Y \quad \forall\ g \in G$. Pick an element $y_0 = (g_0, a_t) \in Y$ (for some $g_0 \in G$, $1 \le t \le m$).

Then $g \cdot y_0 = (g + g_0, a_t) \in Y \quad \forall\ g \in G$

$\Rightarrow Y_t \subset Y$. But $|Y_t| = p^r = |Y|$. Hence

$Y = Y_t$ as required. □

(6.3) Again let $n = p^r \cdot m$ (p is prime, $r \ge 1$, p does not divide m).

Let G be a group of order n.

Definition: A subgroup $P < G$ of order p^r is called

a <u>Sylow p-subgroup of G</u>.

Sylow Theorems.

(A) Sylow p-subgroups exist.

(B) If $H < G$ is a p-group, then there exists a Sylow p-subgroup $P < G$ such that $H \subset P$. Any two * Sylow p-subgroups $P, Q < G$ are conjugate to each other (i.e., $\exists\, g \in G$ s.t. $Q = gPg^{-1}$.)

(C) Let n_p = number of Sylow p-subgroups of G. Then

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \text{ divides } m.$$

(6.4) Proof of Sylow Theorem (A).

Let $\mathcal{E} = \{Y \subset G \text{ subset} : |Y| = p^r\}$

$G \curvearrowright \mathcal{E}$ by: for $g \in G$, $Y = \{y_1, \ldots, y_{p^r}\} \in \mathcal{E}$

$$g \cdot Y = \{g \cdot y_1, \ldots, g \cdot y_{p^r}\} \in \mathcal{E}$$

Using lemmas (6.1) and (6.2), we know that there is some $X \in \mathcal{E}$ whose orbit has cardinality

not divisible by p. (Otherwise, if every G-orbit in $\mathcal{E}$ has cardinality divisible by p, then $|\mathcal{E}| = \sum_{\alpha \in G\backslash\mathcal{E}} |G \cdot x_\alpha|$ will be $\equiv 0 \pmod p$. That is, $\binom{n}{p^r} \equiv 0 \pmod p$ contradicting Lemma (6.2)).

Let $H_X = \mathrm{Stab}_G(X) < G$. Then

$$|\text{Orbit of } X| = \frac{|G|}{|H_X|} \not\equiv 0 \pmod p$$

$\Rightarrow$ p^r divides $|H_X|$.

Now choose $x_0 \in X$ and define

$$\begin{array}{ccc} H_X & \longrightarrow & X \\ \Psi & & \Psi \\ g & \longmapsto & g x_0 \end{array}$$

This map (of sets) is injective since $gx_0 = hx_0$

$\Rightarrow g = h$

(right multiply by x_0^{-1})

$\Rightarrow |H_X| \leq |X| = p^r$

Thus $|H_X| = p^r$ and hence H_X is a Sylow p-group

□

(6.5) Proof of Sylow Theorem (B).

Let $H < G$ be a p-(sub)group and let $P < G$ be a Sylow p-subgroup. Consider the action of H on $G/P =: X$:

$$h \cdot (gP) := (hg)P$$

By Lemma (6.1) above, $|X^H| \equiv |X| \pmod p$.

As $|X| = m \not\equiv 0 \pmod p$, $|X^H| \not\equiv 0 \pmod p$ i.e.

$\exists\ gP \in X^H$. That is, $hgP = gP \ \forall\ h \in H$

$$\Rightarrow \quad g^{-1}hg \in P \quad \forall\ h \in H$$

Hence $H \subset gPg^{-1}$ ← a Sylow p-subgroup.

Now, if H were also a Sylow p-subgroup, then

$$|H| = p^r = |gPg^{-1}|$$

$$\Rightarrow \quad H = gPg^{-1}$$

i.e. any two Sylow p-subgroups are conjugate to each other. □

(6.6) Proof of Sylow Theorem (C).

Let $\mathcal{S}$ = set of all Sylow p-subgroups of G.

($\mathcal{S} \neq \phi$ by (A)). Let $P \in \mathcal{S}$ be a Sylow p-subgroup.

Consider $P \curvearrowright \mathcal{S}$ by conjugation: $\forall\, x \in P;\ Q \in \mathcal{S}$:

$$x \cdot Q = x Q x^{-1} \in \mathcal{S}.$$

Claim. $\mathcal{S}^P = \{P\}$

If the claim is true, then by Lemma 6.1

$$n_p = |\mathcal{S}| \equiv |\mathcal{S}^P| = 1 \pmod{p}.$$

Proof of the claim: Let $Q \in \mathcal{S}^P$. That is, Q is a Sylow p-subgroup of G such that $x Q x^{-1} = Q\ \forall\, x \in P$

Define $N_Q = \{g \in G : g Q g^{-1} = Q\} < G$

(normalizer of Q in G)

Then P, Q are two Sylow p-groups of N_Q.

By (B) of Sylow Theorems, $\exists$ $x \in N_Q$ s.t. $P = x Q x^{-1}$

$= Q$

(by defn. of N_Q) ∎

It remains to show that n_p divides m. For this consider $G \curvearrowright \mathcal{S}$ by conjugation $\left(g \cdot \tilde{P} = g\tilde{P}g^{-1}\right)$, choose $P \in \mathcal{S}$ and use (B) to see that

$$n_p = |\mathcal{S}| = |\text{Orbit of } P|$$

$$= \frac{|G|}{|\text{Stab}(P)|} = \frac{|G|}{|N_P|}$$

N_P ← normalizer of P

Now $P < N_P \Rightarrow |N_P| = p^r \cdot m'$ for some m' dividing m

$$\Rightarrow n_p \cdot m' = m$$

□