Lecture 7

(7.0) Summary of techniques so far.

- Let p be a prime number, G a finite group acting on a set X. $|G| = p^k$ for some $k \geq 1$. Then

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

(Lemma 6.1 of Lecture 6, page 2)

- Sylow Theorems: (Thm 6.3 page 4)
  - (A) Sylow p-subgroups exist.
  - (B) Sylow p-subgroup is unique upto conjugation.
  - (C) $|G| = p^r \cdot m$ (p: prime not dividing m and $r \geq 1$)

    n_p = # of Sylow p-subgroups in G. Then

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

- Prop. 4.5 (page 6) Prop (5.1) (page 2)

Semidirect product $H \rtimes N$	$\longleftrightarrow$	Split short exact seq. $1 \to N \to G \to H \to 1$	$\longleftrightarrow$	Gp. homs. $H \to \mathrm{Aut}(N)$ Gp.

(7.1) Problem 5 of Problem Set 2.

If $\exists\ H < Z(G)$ s.t. G/H is cyclic then G is

(H: subgroup)

abelian.

Proof. Since G/H is cyclic, there exists $s \in G$ s.t.

$$G = \bigsqcup_{\ell \geq 0} s^\ell H$$

Now let $g_1 = s^{\ell_1} \cdot x_1$ and $g_2 = s^{\ell_2} \cdot x_2 \in G$ $\left(\begin{matrix} \ell_1, \ell_2 \in \mathbb{Z}_{\geq 0} \\ x_1, x_2 \in H \end{matrix}\right)$

Then $g_1 g_2 = s^{\ell_1} x_1 s^{\ell_2} x_2 = s^{\ell_1+\ell_2} x_1 x_2$ (as $x_1 \in Z(G)$)

$= s^{\ell_1+\ell_2} x_2 x_1 = s^{\ell_2} x_2 s^{\ell_1} x_1 = g_2 g_1$ □

(7.2) Theorem Let p be a prime number. Let G be a finite group of order p^2. Then $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Proof. Let $Z = Z(G)$ be the center of G.

Claim 1: $|Z(G)|$ is divisible by p. (i.e., $Z(G) \neq \{e\}$).

Proof of Claim 1: Let $G \circlearrowright G$ by conjugation, i.e.,

$$g \cdot h = ghg^{-1}$$

Then $G^G = \{x \in G : gxg^{-1} = x \ \forall g \in G\} = Z$

By Lemma 6.1 (page 2), $|Z| \equiv |G| \mod p$

$= 0 \mod p$

So $|Z| \neq 1$. As $|Z|$ divides $|G|$, it must be a power of p [This argument holds for any p-group G].

Thus there are two options: $|Z| = p^2 \Rightarrow G = Z$ is abelian.

or $|Z| = p$. But then $|G/Z| = p \Rightarrow G/Z \simeq \mathbb{Z}/p\mathbb{Z}$. (cyclic)

By (7.1) above, this means G is abelian (i.e. $G = Z$)

contradicting $|Z| = p$.

In conclusion, $|G| = p^2 \Rightarrow G$ is abelian.

Now for any $\sigma \in G$, $(\sigma \neq e)$ order of σ is either p or p^2. If there is some element of order p^2, then G is cyclic and hence isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.

Otherwise every element (non-identity) has order $= p$.

Claim 2. G abelian, $|G| = p^2$, $\forall \sigma \in G$, $\sigma \neq e$, $\text{ord}(\sigma) = p$

$\Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof of Claim 2: Pick any $\sigma \in G \setminus \{e\}$. $\langle\sigma\rangle \simeq \mathbb{Z}/p\mathbb{Z}$

Let $\tau \in G \setminus \langle\sigma\rangle$. Then $\langle\tau\rangle \simeq \mathbb{Z}/p\mathbb{Z}$

- $\langle\sigma, \tau\rangle = G$ because $\langle\sigma, \tau\rangle > p$ and divides p^2.
- $\langle\sigma\rangle$, $\langle\tau\rangle$ are normal in G (as G is abelian)
- $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$. Otherwise $\exists\ n \in \{1, \ldots, p-1\}$ s.t. $\tau^n \in \langle\sigma\rangle$. Then $\langle\tau^n\rangle = \langle\tau\rangle \subset \langle\sigma\rangle$ contradiction.

Hence, $G \simeq \langle \sigma \rangle \times \langle \tau \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

(7.3) Let us record the observation we made in the proof of claim 1. <u>If G is a p-group, then $Z(G)$ is non-trivial</u>.

There are non-abelian groups of order p^3 (and higher powers of p).

e.g. D_4 = dihedral group of order 8

4 terms each side hence D_4.

$$= \langle s_1, s_2 \; ; \; s_1^2 = s_2^2 = 1, \; s_1 s_2 s_1 s_2 = s_2 s_1 s_2 s_1 \rangle$$

$$D_4 = \{1, s_1, s_2, s_1 s_2, s_2 s_1, s_1 s_2 s_1, s_2 s_1 s_2, s_1 s_2 s_1 s_2 = s_2 s_1 s_2 s_1\}$$

- $Z(D_4) = \{1, s_1 s_2 s_1 s_2\}$ has order 2.
- $D_4 / Z(D_4) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$s_1 \cdot Z \longmapsto (1, 0)$

$s_2 \cdot Z \longmapsto (0, 1)$

(it couldn't have been $\mathbb{Z}/4$, since in that case (7.1) applies, contradicting non-commutativity of D_4)

(7.4) Definition: Dihedral group of order $2N$, denoted

$$D_N = \langle s_1, s_2 \; ; \; s_1^2 = s_2^2 = 1, \; (s_1 s_2)^N = 1 \rangle$$

$$= \left\{ 1, \; s_1, \; s_1 s_2, \; \dots, \; \overbrace{s_1 s_2 \cdots}^{N-1 \text{ terms}}, \; s_1 s_2 s_1 s_2 \cdots : N \text{ terms} \right\}$$

as a set

$$\left. \begin{matrix} s_2, \; s_2 s_1, \; \dots, \; \underbrace{s_2 s_1 \cdots}_{N-1 \text{ terms}} \end{matrix} \right\}, \quad = s_2 s_1 s_2 s_1 \cdots$$

$$|D_N| = 2N.$$

(7.5) Theorem. If G is a p-group, then there exists a sequence

$$G_0 = G \supset G_1 \supset \cdots \supset G_r = \{e\} \quad \text{s.t.}$$

(i) $G_{j+1} \triangleleft G_j$ (normal subgroup) $\forall \; 0 \le j \le r-1$

(ii) $G_j / G_{j+1} \simeq \mathbb{Z}/p\mathbb{Z}$ $\forall \; 0 \le j \le r-1$

(hence $|G| = p^r$).

Proof. ~~Claim 1~~. The proof is by induction on r, where $|G| = p^r$. The base case $r = 1$ is trivial.

Now let $Z = Z(G)$ be the center of G. Pick $x \in Z$, $x \neq e$ (exists: see (7.3) on previous page). Let p^s be the order

of x. Then $x^{p^{s-1}}$ has order p and hence we get $H = \langle x^{p^{s-1}} \rangle \subset Z$ (hence normal in G). $H \simeq \mathbb{Z}/p\mathbb{Z}$.

Now $|G/H| = p^{r-1}$ and by induction hypothesis, we can find a sequence

$$G/H = \overline{G}_0 \rhd \overline{G}_1 \rhd \cdots \rhd \overline{G}_{r-1} = \{e \cdot H\}$$

Let $\pi : G \longrightarrow G/H$ and define $G_j = \pi^{-1}(\overline{G}_j)$.

By first isomorphism theorem, G_{j+1} is normal in G_j and $G_j/G_{j+1} \simeq \overline{G}_j/\overline{G}_{j+1} \simeq \mathbb{Z}/p\mathbb{Z}$. Hence the sequence $G = G_0 \supset G_1 \supset \cdots \supset G_{r-1} \overset{\#}{=} H \supset G_r = \{e\}$ satisfies conditions of the theorem $\square$

(7.6) An example. Let $\mathbb{F}_5$ be the field with 5 elements.

$G = GL_2(\mathbb{F}_5) = \{\text{invertible } 2\times 2 \text{ matrices with entries from } \mathbb{F}_5\}$

- $|G| = 480$: # of choices for 1st column $= 25 - 1 = 24$ (here $25 = |\mathbb{F}_5^2|$. but the first column cannot be $\binom{0}{0}$).

# of choices for the second column $= |\mathbb{F}_5^2 \setminus \{\lambda \cdot 1^{st}\text{column}\}_{\lambda \in \mathbb{F}_5}|$
$= 20$

• $480 = 2^5 \cdot 3 \cdot 5$.

A Sylow 5-subgroup : $\left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{F}_5 \right\}$

A Sylow 3-subgroup : $\left\langle \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \right\rangle$

↑ ord 3 matrix

A Sylow 2-subgroup : $\left\{ \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \cdot \begin{bmatrix} 0 & \mu_1 \\ \mu_2 & 0 \end{bmatrix} : \lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{F}_5 \setminus \{0\} \right\}$

(7.7) Another example: Classify groups of order 45.

$45 = 3^2 \cdot 5$ (let G be a group such that $|G| = 45$)

Step 1. (Use Sylow Theorems)

• There exist subgroups P_3 and P_5 of order 9 and 5 resp.

• # of Sylow p-subgroups $= n_p$

$n_5 \equiv 1 \pmod 5$ $\quad n_5 \mid 9 \quad \Rightarrow \quad n_5 = 1$

$n_3 \equiv 1 \pmod 3$ $\quad n_3 \mid 5 \quad \Rightarrow \quad n_3 = 1$

$\Rightarrow P_3, P_5 \trianglelefteq G$

Now $P_5 \simeq \mathbb{Z}/5\mathbb{Z}$ (any non-identity element will have order > 1 and dividing 5, hence 5)

By Theorem (7.2) $P_3 \simeq \mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Step 2. G is a semidirect product

- $G = P_3 \cdot P_5$ because the group generated by P_3 & P_5 is $P_3 \cdot P_5 = P_5 \cdot P_3$ as one of them (actually both) is normal. So its order is divisible by both 9 & 5, so it must be $45 = |G|$.
- $P_3 \cap P_5 = \{e\}$. If $x \in P_3 \cap P_5$ then $x^9 = e = x^5 \Rightarrow$

$$x = (x^9)^{-1} \cdot (x^5)^2 = e.$$

Step 3. Thus G arises from a group hom $\alpha : P_3 \to \mathrm{Aut}_{gp}(P_5)$

But $\mathrm{Aut}_{gp}(P_5) \cong \mathbb{Z}/4\mathbb{Z}$ and there are no non-trivial group homs from $\mathbb{Z}/9\mathbb{Z}$ (or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$) to $\mathbb{Z}/4\mathbb{Z}$.

Hence $G = P_3 \times P_5 \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

□