Lecture 15

(15.0) Recall – the assertions of Sylow Theorems

1. Sylow p-subgroups exist.
2. Any two Sylow p-subgroups are conjugate to each other.
3. # Sylow p-subgroups $\equiv 1 \pmod p$ (& divides $|G|$).

In the previous lecture we used these results to show

$$|G| = 45 \Rightarrow G \cong \begin{pmatrix} \text{A group of} \\ \text{size } 9 \end{pmatrix} \times \begin{pmatrix} \text{A group} \\ \text{of size } 5 \end{pmatrix}$$

(15.1) Direct products. –

Lemma. – Let G be a group and $N_1, N_2 \trianglelefteq G$ s.t.

(1) G is generated by N_1 & N_2

(2) $N_1 \cap N_2 = \{e\}$

Then
$$f : N_1 \times N_2 \xrightarrow{\sim} G \quad \text{is a group } \underline{\underline{\text{iso}}}.$$
$$(x_1, x_2) \longmapsto x_1 \cdot x_2$$

Proof. – Note: $N_1 \times N_2 = \{ (x_1, x_2) \mid x_1 \in N_1 \text{ and } x_2 \in N_2 \}$

Group operation (componentwise) $(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$.

Also, since $N_1 \cap N_2 = \{e\}$, we have $ab = ba$ $\forall\, a \in N_1,\, b \in N_2$.

This implies that every element of the subgroup of G, generated by N_1 & N_2, can be written as $x_1 \cdot x_2$ for some $x_1 \in N_1$ and $x_2 \in N_2$. By (1), this subgroup is same as G,

Hence <u>f is surjective</u>.

<u>f is a group hom</u>: To show: $\forall\, x_1, y_1 \in N_1$; $x_2, y_2 \in N_2$,

$$f\big((x_1,x_2)\cdot(y_1,y_2)\big) = f(x_1,x_2)\cdot f(y_1,y_2)$$

$$\left.\begin{array}{ll} \text{L.H.S.} = & x_1 y_1 \cdot x_2 y_2 \\ \text{R.H.S.} = & x_1 x_2 \cdot y_1 y_2 \end{array}\right\} \text{ are equal because } \begin{array}{c} y_1 x_2 = x_2 y_1 \\ \forall\, y_1 \in N_1;\, x_2 \in N_2. \end{array}$$

<u>f is injective</u>: $\quad f((x_1,x_2)) = e \qquad (x_1 \in N_1;\, x_2 \in N_2)$

$$\iff x_1 \cdot x_2 = e$$

$$\text{i.e. } \underset{N_1 \ni}{x_1} = x_2^{-1} \in N_2 \underset{(\text{as } N_1 \cap N_2 = \{e\})}{\Rightarrow} x_1 = x_2^{-1} = e.$$

$\square$

Remark.- This argument can be easily generalized to finite number of normal subgroups: $N_1, \ldots, N_k \trianglelefteq G$

- G is generated by $N_1, N_2, \ldots, N_k$
- $N_i \cap N_j = \{e\}$ $\forall\, i \neq j$, $1 \leq i,j \leq k$

$$\Rightarrow \quad \begin{array}{c} N_1 \times N_2 \times \cdots \times N_k \\ \cong \\ G. \end{array}$$

(15.2) As a consequence we have the following result.

Prop. Let G be a finite abelian group. If $n = |G|$ is written into its prime factors:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad \left(\begin{array}{l} p_1, \dots, p_k \text{ are} \\ \text{distinct primes} \end{array}\right)$$

and P_i = ~~a~~ the Sylow p_i subgroup of G $(1 \le i \le k)$

(G is abelian, so every subgroup is normal, hence there is only one Sylow p_i-subgroup)

Then $G \cong P_1 \times \dots \times P_k$.

Proof. - (1) Each P_i is normal in G.

(2) $P_i \cap P_j = \{e\}$ $(i \neq j)$.

(because, if $\sigma \in P_i \cap P_j$, $\operatorname{ord}(\sigma)$ divides $p_i^{a_i}$ & $p_j^{a_j}$, so $\sigma = e$.)

(3) If H is the smallest subgroup containing $P_1, \dots, P_k$, then $\forall i \in \{1, \dots, k\}$

$|P_i| = p_i^{a_i}$ divides $|H|$

$\Rightarrow$ n divides $|H|$ $\Rightarrow$ $H = G$.

and we are done by the previous lemma $\square$

(15.3) Remark. Later we will study in some details, groups which are <u>not abelian</u> and yet have the property that every Sylow p-subgroup is normal (i.e. $n_p = 1$ $\forall$ prime p dividing $|G|$.)

The same argument, as in the proof of Proposition (15.2), will apply to such groups (called <u>nilpotent groups</u>.)

(15.4) Proposition (15.2) and the following result, together, yield a classification of finite abelian groups.

Theorem. If $|G| = p^n$ and <u>G is abelian</u>, then there exist numbers $a_1, a_2, \ldots, a_k$ such that (say, $a_1 \leq a_2 \leq \ldots a_k$)

$$G \cong \mathbb{Z}/_{p^{a_1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/_{p^{a_k}}\mathbb{Z} \qquad \left(\begin{array}{l}\text{so,}\\ a_1 + \ldots + a_k = n.\end{array}\right)$$

Moreover, k and $a_1, \ldots, a_k$ are uniquely determined.

Proof. The proof follows an induction (on n) argument. The base case being trivially true ($n = 0$).

Take $a = $ maximum $\{ s$ such that $\operatorname{ord}(\sigma) = p^s$ for some $\sigma \in G \}$

and choose $\sigma \in G$ of order p^a. We get

$H = \langle \sigma \rangle \trianglelefteq G$. As $|G/H| = p^{n-a}$,
$(\cong \mathbb{Z}/p^a\mathbb{Z})$ (G is abelian)

by induction $G/H \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_{k-1}}\mathbb{Z}$.

Meaning: we can find $y_1, \dots, y_{k-1}$ in G/H of orders $p^{a_1}, \dots, p^{a_{k-1}}$ respectively which

- generate G/H.
- $\langle y_i \rangle \cap \langle y_j \rangle = \{e\}$ $\forall\, i \neq j$, $1 \leq i, j \leq k-1$.

We <u>need to prove that</u>, for every $i = 1, 2, \dots, k-1$, <u>we can find</u> $\sigma_i \in G$ such that $y_i = \sigma_i \cdot H$, $\operatorname{ord}(\sigma_i) = p^{a_i}$ (in G).

[Careful: if we choose an arbitrary representative $\tilde{\sigma}_i$ of the coset $y_i \in G/H$; all we can say is $(\tilde{\sigma}_i)^{p^{a_i}} \in H$, not that it is 1.]

<u>Assuming such $\sigma_1, \ldots, \sigma_{k-1} \in G$ can be chosen</u>, take

$\sigma_k = \sigma$ (a generator of H) and $a_k = a$ ($p^a = |H|$).

Set $H_i = \langle \sigma_i \rangle \trianglelefteq G$ ($H_i \cong \mathbb{Z}/p^{a_i}\mathbb{Z}$.)

- G is generated by $\{\sigma_1, \ldots, \sigma_{k-1}, \sigma_k\}$.

[Ex. (Generating set of N) $\cup$ $\left(\begin{array}{l}\text{choice of coset representatives} \\ \text{of a generating set of } G/N\end{array}\right)$

$=$ a generating set of G.]

- $H_i \cap H_j = \{e\}$ $\forall\ i \neq j$ $(1 \leq i, j \leq k)$

Note: $(\forall\ 1 \leq i \leq k-1)$

$$\begin{tikzcd}
H_i \arrow[d, "\cong"'] & \trianglelefteq & G \arrow[d, "\pi \text{ natural projection}"] \\
\pi(H_i) & \trianglelefteq & G/H \\
 & & \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_{k-1}}\mathbb{Z} \arrow[u, "\cong"']
\end{tikzcd}$$

$\mathbb{Z}/p^{a_i}\mathbb{Z}$ by our choice of σ_i

i^{th} copy $\mathbb{Z}/p^{a_i}\mathbb{Z}$

As $H_i \cong \pi(H_i)$, $\operatorname{Ker}(\pi) \cap H_i = \{e\}$, i.e. $H_k \cap H_i = \{e\}$ $\forall\ 1 \leq i \leq k-1$.

[Ex. use the same argument as above to prove $H_i \cap H_j = \{e\}$ $\forall\ 1 \leq i \neq j \leq k-1$.]

So, again we are in a position to apply Lemma 15.1 to get $G \cong H_1 \times \dots \times H_k$ as required.

It remains to prove that $\sigma_1, \dots, \sigma_{k-1} \in G$ can be chosen as claimed above. This problem can be handled one $i \in \{1, \dots, k-1\}$ at a time, ~~as~~ which we carry out separately below.

(15.4) Let H be an abelian group with p^l elements.
Assume that there exists $H_1 \cong \mathbb{Z}/p^{l_1}\mathbb{Z} \trianglelefteq H$

such that $H_2 := H/H_1 \cong \mathbb{Z}/p^{l_2}\mathbb{Z}$ (so $l = l_1 + l_2$)

and $l_1 = \max\{s \mid \text{ord}(\sigma) = s \text{ for some } \sigma \in H\}$.

Let $y \in H_2$ be a generator of H_2. Then we can find $\sigma_2 \in H$ such that $y = \sigma_2 \cdot H_1$
$\text{ord}(\sigma_2) = p^{l_2}$

For notational convenience, we write these abelian groups additively (i.e. 0 denotes the neutral element
$x+y$ " " group operation

$$m \cdot x = \underbrace{x + x + \dots + x}_{m\text{-times}}$$

and $\mathrm{ord}(x) = r$ means $r \cdot x = 0$.)

Proof.- Let us choose $\sigma_1 \in H_1$ a generator of H_1.

$x \in H$ such that $x \cdot H_1 = y \in G/H_1 = H_2$

is a generator of H_2.

Then $p^{l_2} \cdot y = 0$ in H_2 implies $p^{l_2} \cdot x \in H_1 = \{ j \cdot \sigma_1 \mid 0 \le j \le p^{l_1} - 1 \}$

i.e. $p^{l_2} \cdot x = p^s \cdot \boxed{m\sigma_1}$ $\left(\begin{array}{c} s \ge 0 \\ (m,p) = 1 \end{array} \right)$

$\boxed{m\sigma_1} \longrightarrow$ has order p^{l_1} still

This implies order of $x = p^{l_1 + l_2 - s} = p^{l - s} \le p^{l_1}$ ← this was the largest!

i.e. we get $s \ge l - l_1 = l_2$

Then $p^{l_2} \cdot \left(x - p^{s - l_2} \boxed{m\sigma_1} \right) = 0$

Take $\boxed{\sigma_2 = x - p^{s-l_2} m \sigma_1}$ $\square$

(15.5) How to read off $k, a_1, a_2, \dots, a_k$ from G?

For an abelian p-group (written additively), say H,

consider
$$\sigma : H \longrightarrow H$$
$$x \longmapsto px = \underbrace{x + x + \dots + x}_{p \text{ terms}}$$

σ is a group hom. because H is abelian.

e.g. if $H = \mathbb{Z}/p^{b_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{b_\ell}\mathbb{Z}$ then

$$|\operatorname{Ker}(\sigma)| = p^{\ell}$$

ℓ = # of factors $= \log_p(|\operatorname{Ker}(\sigma)|)$

b_ℓ = ~~largest~~ smallest t such that $\sigma^t(x) = 0 \quad \forall x \in H$

For an arbitrary abelian p-group G; $|G| = p^n$; $\sigma : G \longrightarrow G$, $g \longmapsto p \cdot g$

$\sigma^0 = \mathrm{Id}$ (convention)

$$\{e\} = \operatorname{Ker}(\sigma^0) \subseteq \operatorname{Ker}(\sigma) \subseteq \operatorname{Ker}(\sigma^2) \ \dots \ \subseteq \operatorname{Ker}(\sigma^n) = G.$$

We obtain the following table of numbers where $a_1, \dots, a_k$ (& k) appear when the size $\boxed{\text{of } \operatorname{Ker}(\sigma^{r+1})/\operatorname{Ker}(\sigma^r)}$ jumps "irregularily":

r	$r=0$	$r=1$		$r=a_1$		$r=a_2$		$r=a_k$
$\log_p\left(\left\lvert \frac{\operatorname{Ker}(\sigma^{r+1})}{\operatorname{Ker}(\sigma^r)} \right\rvert\right)$	k	k	$\dots$	$\downarrow$ $k-1$	$\dots$	$\downarrow$ $k-2$	$\dots$	$0 \longrightarrow$ remains 0 after