Lecture 14

(14.0) Recall – the statement of Sylow theorems :-

1. Sylow p-subgroups exist.
2. They are unique up to conjugation.
3. # Sylow p-subgroups $\equiv 1 \mod p$.
   (& divides $|G|$)

Example. – Let G be a finite group with $|G| = 45$
$= 3^2 \cdot 5$

Let $n_3 = \# \{P \leq G \text{ such that } |P| = 9\}$

$n_5 = \# \{Q \leq G \text{ such that } |Q| = 5\}$

By Sylow theorems.

$$\boxed{\begin{array}{l} n_3 \equiv 1 \pmod 3 \\ n_3 \text{ divides } 5 \end{array}} \implies n_3 = 1$$

$$\boxed{\begin{array}{l} n_5 \equiv 1 \pmod 5 \\ n_5 \text{ divides } 9 \end{array}} \implies n_5 = 1 .$$

Meaning. – In any group with 45 elements, there is

a <u>unique</u> subgroup of size 9 – say P

a <u>unique</u> " " " 5 – say Q.

Observation – If $P_0 \leq G$ is the only Sylow p-subgp, then P_0 is normal; because for any $g \in G$,

$$gP_0g^{-1} \leq G \text{ is another Sylow } p\text{-subgroup, hence } (\text{!})$$

$$\forall g \in G \; ; \; P_0 = gP_0g^{-1} \implies P_0 \text{ is normal in } G.$$

Back to $|G| = 45$. We know

$$\begin{tikzcd} & G & \\ P \arrow[ur, phantom, "\triangleleft"] & & Q \arrow[ul, phantom, "\triangleright"] \end{tikzcd}$$

has 9 elts. $\rightarrow P$

$Q \leftarrow$ has 5 elts (so $Q \cong \mathbb{Z}/5\mathbb{Z}$)

More observations. – (i) If $H \leq G$ is the subgroup generated by P & Q, then both 9 & 5 divide $|H|$, so

$$|H| \geq 45 \implies H = G.$$

(ii) $P \cap Q \ni \sigma \implies \operatorname{ord}(\sigma)$ divides 9 & 5

$$\implies \sigma = \{e\}.$$

(14.1) Lemma. – Let G be a group, $N_1, N_2 \trianglelefteq G$ such that $N_1 \cap N_2 = \{e\}$. Then

$$ab = ba \quad \forall\, a \in N_1,\; b \in N_2.$$

Proof. $a b a^{-1} b^{-1} = (a b a^{-1}) \cdot b^{-1} \in N_2$

b^{-1}: in N_2, given.

$(a b a^{-1})$: in N_2 as $b \in N_2$ & N_2 is normal

$a b a^{-1} b^{-1} = a \cdot (b a^{-1} b^{-1})$

a: in N_1; $(b a^{-1} b^{-1})$: in N_1 same argument

N_1

also given

$\Rightarrow \forall\, a \in N_1,\ b \in N_2$: $a b a^{-1} b^{-1} \in N_1 \cap N_2 = \{e\}$
so $ab = ba$. □

(14.2) Back again to $|G| = 45$.

G is generated by P, Q; two normal, "mutally commuting" subgroups, i.e.,

$$G = \{ p \cdot q \mid p \in P,\ q \in Q \}$$

group operation $(p \cdot q) \cdot (p' q') = (p p') \cdot (q q')$

(pp'): mult. in P; (qq'): mult. in Q

$qp' = p'q$ because of Lemma 14.1 above.

So, to completely describe G, we need full description of

$Q \cong \mathbb{Z}/5\mathbb{Z}$ ✓

P has 9 elements?

(14.3) Now assume H is a group with $|H| = p^2$, where $p \in \mathbb{Z}_{\geq 2}$ is a prime.

From last lecture, we know that the center of H, $Z(H)$, is not trivial. So, either $\boxed{|Z(H)| = p}$ or p^2. In the latter case, H is abelian and we can argue as follows:

Pick $\sigma \in H \setminus \{e\}$. $\boxed{\text{ord}(\sigma) = p}$ or p^2.
$\quad \hookrightarrow H \cong \mathbb{Z}/p^2\mathbb{Z}$

So we come to the following conclusion.

Either $H \cong \mathbb{Z}/p^2\mathbb{Z}$ or (not exclusive) $\exists \begin{cases} H_1 \trianglelefteq H, \\ H_1 \leq Z(H) \text{ with } \\ |H_1| = p \end{cases}$

(First case : $H_1 = Z(H)$
Second case : $H_1 = \langle \sigma \rangle \subset Z(H) = H$.)

As $H_2 := H/H_1$ also has p elements, we know

$$H_2 = \{e, \bar{y}, \bar{y}^2, \ldots, \bar{y}^{p-1}\} \text{ where, } \bar{y} \in H/H_1 \setminus \{e.H_1\}$$

Let us pick a representative, say $\sigma_2 \in H$, such that $\bar{y} = \sigma_2 . H_1$.

As $(\bar{y})^p = \bar{e}$ in H/H_1 ; we get $\sigma_2^p \in H_1$.

- $\sigma_2^p \in H_1 \setminus \{e\} \Rightarrow \sigma_2$ has order p^2; i.e.

$$H \cong \mathbb{Z}/p^2\mathbb{Z}$$

or $\sigma_2^p = e$. Now we may choose $\sigma_1 \in H_1$ such that

$$H_1 = \{e, \sigma_1, \sigma_1^2, \dots, \sigma_1^{p-1}\}$$

By our hypotheses $(H_1 \subset Z(H))$ σ_1 commutes with σ_2 and we obtain the following subgroup of H, generated by σ_1 & σ_2

$$\{\sigma_1^i \sigma_2^j \;:\; 0 \le i,j \le p-1\} \subset H$$

$\uparrow$ already has p^2 elements, so $= H$.

We have proved:

Proposition. – $\boxed{|H| = p^2,\ p: \text{prime} \;\Rightarrow\; H \cong \mathbb{Z}/p^2\mathbb{Z} \text{ or } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.}$

(14.4) We already know one group of size $8\ (= 2^3)$ which is not abelian, namely $D_8 = \langle s, r \mid s^2 = r^4 = e;\ srs = r^{-1}\rangle$.

$$D_8 \trianglerighteq Z(D_8) = \langle r^2 \rangle = \{e, r^2\}$$

Chain in D_8: $\{e\} \trianglelefteq \langle r^2\rangle = Z(D_8) \trianglelefteq D_8$

$\langle r^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$; quotient $D_8 / Z(D_8)$ has 4 elements.

$$D_8 / Z(D_8) = \langle s, r \mid s^2 = r^2 = e \, ; \; sr = rs \rangle$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} .$$

Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ 8 elements.

Group operation : $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1 \qquad (-1)^2 = +1$

$$i \cdot j = k \; ; \; j \cdot i = -k$$
$$j \cdot k = i \; ; \; k \cdot j = -i$$
$$k \cdot i = j \; ; \; i \cdot k = -j$$

$$Z(Q_8) = \{+1, -1\} \cong \mathbb{Z}/2\mathbb{Z} .$$

$$Q_8 / Z(Q_8) = \{1, i, j, k\} \qquad i^2 = j^2 = k^2 = 1$$

all commute

$i \cdot j = k$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Ex. D_8 and Q_8 are not isomorphic. Even though their respective chains of normal subgroups "looks the same".

For instance # of elements of order 2 in $D_8 = 4 \; (s, sr, sr^2, sr^3)$

$Q_8 = 1 \; (-1)$.

(14.5) Putting everything from (14.0) – (14.3) together we get:

There are exactly two groups of size 45:

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

or

$$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$