10/10

Lemma (Recall!)

$G \circlearrowright S$. If $|G| = p^n$, then $|S| \equiv |S_0| \pmod p$

Definition

A group G is said to be a p-group if $o(g) = p^n$ for some $n \geq 1$ $\forall g \in G$

If G is a group, then a subgroup $H \leq G$ is said to be a p-subgroup if H is a p-group.

Lemma

G is a finite p-group $(\Leftrightarrow)$ $|G| = p^n$ for some $n > 1$

(Proof)

(Exercise!)

Lemma

If H is a p-subgroup of a group G then $[N_G(H) : H] \equiv [G : H] \pmod p$

In particular, $N_G(H) \neq H$ if $p \mid [G : H]$

$H \circlearrowright S = \{\text{left cosets of } H \text{ in } G\}$

$\Rightarrow |S| = [G : H]$

Let $H \circlearrowright S$ by left translation

$xH \in S_0$

$g(xH) = xH$ $\forall g \in H$

$\Rightarrow x^{-1}gx \in H$ $\forall g \in H$

$\Rightarrow x^{-1}Hx \subseteq H$ ($x^{-1}Hx = H$ in this case)

$\Rightarrow xH \in N_G(H)/H$

Sylow Theorems

(I) If G is a group of order $p^n m$, $m \in \mathbb{N}$, $n \geq 1$, $\gcd(p, m) = 1$

then

(i) For each $1 \leq i \leq n$, G contains a subgroup of order p^i

(ii) Every subgroup of order p^i is contained in a normal subgroup of order p^{i+1} $(i < n)$

- (i) follows from Cauchy's theorem
- Suppose G has a subgroup H of order p^i, $i < n$

$$[G : H] = p^{n-i}$$

$$p \mid [G : H]$$

$$p \mid |N_G(H)/H|$$

$\exists$ a subgroup $H_1/H \leq N_G(H)/H$ [By Correspondence Theorem]

$$p \,\|\, |N_G(H)/H|$$

$$|H_1/H| = p \Rightarrow |H_1| = p^{i+1}$$

$$H \trianglelefteq N_G(H) \Rightarrow H \trianglelefteq H_1 \leq N_G(H)$$

Definition

Let G be a finite group

A subgroup $H \leq G$ is said to be a Sylow p-subgroup if H is a maximal p-subgroup of G.

$H < P < G$, then $H = P$ (or) $P = G$

Corollary :

If G is a group of order $p^n m$

① H is a Sylow p subgroup of G
$\Leftrightarrow |H| = p^n$

② $Syl_p(G) = \{$ sylow p subgroups of $G\}$

$H \in Syl_p(G)$

$\Rightarrow xHx^{-1} \in Syl_p(G)$

$|xHx^{-1}| = |H| = p^n$

③ If H is the only Sylow p-subgroup of G, then $H \trianglelefteq G$

(Follows) $xHx^{-1} = H \Rightarrow H \trianglelefteq G$

(II) If H is a p-subgroup of G, and $P \in Syl_p(G)$, then $\exists\, x \in G$ s.t $xHx^{-1} \leq P$

In particular, any two Sylow p-subgroups are conjugate

(Proof)

$S = \{$ left cosets of P in $G\}$

$H \curvearrowright S$ by left translation

$|S| \equiv |S_0| \pmod p$

$|S| = [G:P] = m$

$!(S_0 \neq \emptyset)$

$xP \in S_0 \Rightarrow g(xP) = xP \quad \forall g \in H$

$\Rightarrow x^{-1}gx \in P \quad \forall g \in H$

$\Rightarrow x^{-1}Hx \leq P$

Sylow Theorem – (III)

Let G be a finite group and $n_p := |Syl_p(G)|$

(i) $n_p \mid |G|$

(ii) $n_p \equiv 1 \pmod p$ i.e, $n_p = 1 + kp$ for some $k \geq 0$

(Proof)

$G \curvearrowright S$ = set of subgroups of G by conjugation

$G \times S \to S$

$(g, H) \to gH$

Let $P \in Syl_p(G)$

$O(P) = Syl_p(G)$ [orbit is again the same set of sylow p subgroups]

$\Rightarrow |O(P)| = n_p$

By Orbit-Stabilizer theorem,

$$\frac{|G|}{|G_P|} = |O(P)|$$

$\Rightarrow \boxed{n_p \mid |G|}$

$P \curvearrowright Syl_p(G)$ by conjugation

- $P \in Syl_p(G)$

  $|S| = n_p$ $\qquad$ $|S| \equiv |S_0| \pmod p$

- $Q \in S_0$

$\Leftrightarrow g \cdot Q = Q \quad \forall g \in P$

$\Leftrightarrow gQg^{-1} = Q \quad \forall g \in P$

$\Leftrightarrow \; g \in N_G(Q) \quad \forall g \in P$

$\Leftrightarrow \; P \leq N_G(Q)$

$P \leq N_G(Q) \leq G$

$\Rightarrow P \in Syl_p(N_G(Q))$

$\Rightarrow Q \in Syl_p(N_G(Q))$

$P \in Syl_p(G) \Rightarrow P = xQx^{-1} = Q$

for some $x \in N_G(Q)$
because it is normal
subgroup

$Q = P \Rightarrow |S_0| = 1$ [check !]

$S_0 = \{P\}$

$\Rightarrow n_p \equiv 1 \pmod{p}$

Hence proved

- A group G is called a simple group if G has no proper normal subgroups

Example

Let p, q be primes and G be a group of order $p^n q$ where $p > q$

Then G is not simple

$n_p \mid p^n q$

If $n_p = 1 + kp$ and $k \neq 0 \Rightarrow$ contradiction

$k = 0 \Rightarrow n_p = 1$

Example

If G is a group of order $2p$, then

$$G \cong \mathbb{Z}/2p\mathbb{Z} \quad \text{or} \quad G \cong D_{2p}$$

$|G| = 2p$

$H \leq G, \ |H| = p$

$[G:H] = 2 \Rightarrow H \trianglelefteq G$

$K = \langle b \rangle$ suchthat $o(b) = 2$

$|H \cap K| \mid |H| \Rightarrow \quad |H \cap K| = 1$

$|H \cap K| \mid |K| \Rightarrow \quad \Rightarrow H \cap K = \{e\}$

$$\left.\begin{array}{l} H \trianglelefteq G \\ K \leq G \end{array}\right\} \Rightarrow HK \leq G$$

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

Let $G = \langle a, b \rangle$

$H = \langle a \rangle, \ K = \langle b \rangle$

$bab^{-1} = a^s \qquad 0 \leq s \leq p-1$

$$\begin{aligned} a &= b^2 a b^{-2} \\ &= b(bab^{-1})b^{-1} \\ &= b a^s b^{-1} \end{aligned}$$

$(bab^{-1})^s = a^{s^2}$

$a^{s^2-1} = e \Rightarrow p \mid s^2 - 1 \Rightarrow s = \pm 1$ or $1, p-1$

$\Rightarrow G = \langle a, b \mid o(a) = p, \ o(b) = 2, \ bab^{-1} = a \rangle$

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

$bab^{-1} = a^{p-1} \rightarrow \cong D_{2p}$