VII Advanced Group Theory

34 Isomorphism Theorems

34.2 Theorem **(First Isomorphism Theorem)** Let $\phi : G \to G'$ be a homomorphism with kernel K, and let $\gamma_K : G \to G/K$ be the canonical homomorphism. There is a unique isomorphism $\mu : G/K \to \phi[G]$ such that $\phi(x) = \mu(\gamma_K(x))$ for each $x \in G$.

$$G/\text{Ker}(\phi) \cong \phi[G]$$

34.3 Lemma Let N be a normal subgroup of a group G and let $\gamma : G \to G/N$ be the canonical homomorphism. Then the map ϕ from the set of normal subgroups of G containing N to the set of normal subgroups of G/N given by $\phi(L) = \gamma[L]$ is one to one and onto.

ie.,

Let $N \trianglelefteq G$ & let $\gamma : G \to G/N$ be the canonical homomorphism $\left(\gamma(g) = gN\right)$.
Let η be the set of normal subgroups of G containing N &
$\mathcal{G}/\eta$ be the set of normal subgroups of G/N.
Then, $\phi : \eta \to \mathcal{G}/\eta$ defined by $\phi(L) = \gamma(L)$ is bijective

Proof.

Theorem 15.16 : ie; If $\phi : G \to G'$ is a group homomorphism. Then,

$$N \trianglelefteq G \implies \phi(N) \trianglelefteq \phi[G]$$
$$N' \trianglelefteq \phi(G) \implies \phi^{-1}[N'] \trianglelefteq G$$

A homomorphism $\phi : G \to G'$ preserves normal subgroups b/w G and $\phi[G]$.

L is a normal subgroup of G containing $N \Rightarrow \phi(L) = \gamma[L]$ is a normal subgroup of G/N

$N \leq L$ & L : a normal subgroup of G containing N

$\therefore$ L is closed under the group operation.

For $x \in L, n \in N$ we have $x \cdot n \in L$ since N is contained in L.

$\Rightarrow$ For any $x \in L$,
the entire coset xN in G is contained in L.

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

"canonical homomorphism"

$N \trianglelefteq G$, $\gamma : G \to G/N$ such that $\gamma(g) = gN$

$\Longrightarrow \ker(\gamma) = N$

13.15 Theorem Let $\phi : G \to G'$ be a group homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\} = aH$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

For any $g \in G$, $\gamma^{-1}[\{\gamma(g)\}] = \{x \in G \mid \gamma(x) = \gamma(g)\} = gN$

Suppose $\phi(L_1) = \phi(L_2) \Longrightarrow \gamma[L_1] = \gamma[L_2]$

Let $H, N \leq G$, then the join $H \vee N$ of H and N is the intersection of all subgroups of G containing $HN = \{hn \mid h \in H, n \in N\}$.

- $H \vee N$ is the smallest subgroup of G containing HN
- $H \vee N$ is the smallest subgroup of G containing both H & N since any such subgroup must contain HN.
- In general, HN need not be a subgroup of G.

If S is a non-empty subset of a group G, then

$\langle S \rangle$: the smallest subgroup of G containing S

: the subgroup generated by S

$$\langle S \rangle = \bigcap \{H \mid H \leq G, S \subseteq H\} = \bigcap_{H \in F} H \quad \forall\ F = \{H \mid H \leq G, S \subseteq H\}$$

$$\approx \left\{ a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \,\middle|\, a_i \in S \text{ for } i = 1, 2, \cdots, k,\ n_1, n_2, \cdots, n_k \in \mathbb{Z} \right\}$$

where $S = (a_1, a_2, \cdots, a_k)$

$$H \vee N = \langle HN \rangle$$
$$= \langle H, N \rangle$$

34.4 Lemma If N is a normal subgroup of G, and if H is any subgroup of G, then $H \vee N = HN = NH$. Furthermore, if H is also normal in G, then HN is normal in G.

If $H \leq G$ & $N \trianglelefteq G$, then $HN \leq G \Rightarrow H \vee N = HN = NH$

& if $H \trianglelefteq G$ then $HN \trianglelefteq G$

Proof. Let $h_1 h_2 \in H$ and $n_1, n_2 \in N$

$N \trianglelefteq G \Rightarrow$ left & right cosets coincide (Definition 13.19)

$gN = Ng$ for all $g \in G$

$\therefore n_1 h_2 = h_2 n_3$ for some $n_3 \in N$

$$(h_1 n_1)(h_2 n_2) = h_1 (n_1 h_2) n_2 = h_1 (h_2 n_3) n_2 = (h_1 h_2)(n_3 n_2) \in HN$$

$\Rightarrow HN$ is closed under the induced operation in G

$e = ee \in HN$

$(hn)^{-1} = n^{-1} h^{-1} = h^{-1} n_4$ for some $n_4 \in N$

$\therefore (hn)^{-1} \in HN$

$\Rightarrow HN \leq G$

Similarly, $NH \leq G$

$\therefore HN = HVN = NH$

Suppose $H \trianglelefteq G$,

Let $h \in H, n \in N$ and $g \in G$. Then,

$g(hn)g^{-1} = ghen g^{-1} = (ghg^{-1})(gng^{-1}) \in HN$

since $ghg^{-1} \in H, gng^{-1} \in N$ because $H, N \trianglelefteq G$.

34.5 Theorem **(Second Isomorphism Theorem)** Let H be a subgroup of G and let N be a normal subgroup of G. Then $(HN)/N \simeq H/(H \cap N)$.

Let G be group with $H \leq G$, $N \trianglelefteq G$ then

$$HN/N \cong H/H \cap N$$

Proof

Let $\gamma : G \longrightarrow G/N$ be the canonical homomorphism & let $H \leq G$.

13.12 Theorem Let ϕ be a homomorphism of a group G into a group G'.

1. If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.
2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
4. If K' is a subgroup of $G' \cap \phi[G]$, then $\phi^{-1}[K']$ is a subgroup of G.

If $H' \leq G'$, then $\phi^{-1}(H') \leq G$

Theorem 13.12 $\Rightarrow \gamma[H] \leq G/N$

Part 1

$\gamma|_H$: γ restricted to H (the domain of γ is restricted to H)

$\gamma|_H : H \to \gamma[H]$ s.t $\gamma|_H(x) = \gamma(x) \quad \forall \; x \in H$

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

"canonical homomorphism"

$\Rightarrow \ker(\gamma) = N$

$\ker(\gamma|_H) \subseteq H \quad \& \quad \ker(\gamma|_H) \subseteq \ker(\gamma) = N$

$\Rightarrow \ker(\gamma|_H) \subseteq H \cap N$

Take any $x \in H \cap N$, then $x \in N = \ker(\gamma)$

$\gamma(x) = e_{G/N} = N$

$x \in H \Rightarrow x \in \text{domain}(\gamma|_H)$

$\therefore \gamma|_H(x) = e_{G/N} = N \Rightarrow x \in \ker(\gamma|_H)$

$\Rightarrow H \cap N \subseteq \ker(\gamma|_H)$

$\therefore \quad \ker(\gamma|_H) = H \cap N$

Theorem 14.11: If $\phi: G \to G'$ is a homomorphism with kernel H, then the factor group (quotient group) G/H is isomorphic to the image of ϕ, ie:

$\phi: G \to G'$ is a homomorphism with $H = \ker(\phi) = \{x \mid \phi(x) = e \ \& \ x \in G\}$

$\Rightarrow G/H \cong \text{Im}(\phi)$

$\Rightarrow G/\ker(\phi) \cong \phi[G]$

34.2 Theorem **(First Isomorphism Theorem)** Let $\phi : G \to G'$ be a homomorphism with kernel K, and let $\gamma_K : G \to G/K$ be the canonical homomorphism. There is a unique isomorphism $\mu : G/K \to \phi[G]$ such that $\phi(x) = \mu(\gamma_K(x))$ for each $x \in G$.

$\gamma|_H : H \longrightarrow \gamma[H]$ is a homomorphism with $\ker(\gamma|_H) = H \cap N$

Then,

$$H/\ker(\gamma|_H) = H/H\cap N \cong \gamma[H]$$

Part 2

$\gamma|_{HN} : HN \longrightarrow \gamma[H]$

$\ker(\gamma|_{HN}) \subseteq HN$ & $\ker(\gamma|_{HN}) \subseteq \ker(\gamma) = N$

$\therefore \ker(\gamma|_{HN}) \subseteq N$

Take any $x \in N$, then $x \in HN$

$\Rightarrow x \in \text{domain}(\gamma|_{HN})$

$[\ker(\gamma) = N]$

$\therefore \gamma|_{HN}(x) = e_{G/N} = N \Rightarrow x \in \ker(\gamma|_{HN})$

$\Rightarrow N \subseteq \ker(\gamma|_{HN})$

$\therefore \ker(\gamma|_{HN}) = N$

$\gamma|_{HN} : HN \to \gamma[H]$ is a homomorphism with $\ker(\gamma|_{HN}) = N$

Then,

$$HN/\ker(\gamma|_{HN}) = HN/N \cong \gamma[H]$$

Thus, $H/H\cap N \cong HN/N$

Q.E.D

34.7 Theorem **(Third Isomorphism Theorem)** Let H and K be normal subgroups of a group G with $K \leq H$. Then $G/H \simeq (G/K)/(H/K)$.

Let G be a group and $H, K \trianglelefteq G$ with $K \leq H$, then,

$$G/H \cong (G/K)/(H/K)$$

Proof

Define $\phi : G \to (G/K)/(H/K)$ s.t $\phi(g) = gK(H/K)$ for $g \in G$.

For any $a, b \in G$,

$$\begin{aligned}\phi(ab) &= abK(H/K) \\ &= [(aK)(bK)](H/K) \\ &= [(aK)(H/K)][(bK)(H/K)] \\ &= \phi(a)\phi(b)\end{aligned}$$

$\Rightarrow \phi$ is a homomorphism.

$$\ker(\phi) = \{x \in G \mid \phi(x) = H/K\}$$

$\phi(x) = (xK)(H/K) = H/K$ where $x \in G$, $xK \in G/K$

$\Rightarrow xK \in H/K$ [$aH = H$ iff $a \in H$

$\Rightarrow x \in H$

$\therefore \ker(\phi) = H$

$\phi : G \longrightarrow (G/K)/(H/K)$ is a homomorphism with $\ker(\phi) = H$

> $\phi : G \to G'$ is a homomorphism with $H = \ker(\phi) = \{x \mid \phi(x) = e \ \& \ x \in G\}$
> $\Rightarrow G/H \cong \text{Im}(\phi)$
> $\Rightarrow G/\ker(\phi) \cong \phi[G]$

$\rightarrow G/\ker(\phi) = G/H \cong \phi[G]$

$\phi : G \to (G/K)/(H/K)$ s.t $\phi(a) = (aK)(H/K)$ for $a \in G$

Elements of $(G/K)/(H/K)$ are of the form $(gK)/(H/K)$ for some $g \in G$.

$$\phi(g) = (gK)(H/K)$$

$\therefore$ For every element $(gK)/(H/K)$ in the codomain, there exists an element $g \in G$ s.t $\phi(g) = (gK)(H/K)$.

$\Rightarrow \phi$ is onto

$\Rightarrow \phi[G] = gK(H/K)$

$\therefore G/H \cong gK(H/K)$

35 Series of Groups

35.1 Definition A **subnormal** (or **subinvariant**) **series of a group** G is a finite sequence $H_0, H_1, \cdots, H_n$ of subgroups of G such that $H_i < H_{i+1}$ and H_i is a normal subgroup of H_{i+1} with $H_0 = \{e\}$ and $H_n = G$. A **normal** (or **invariant**) **series of** G is a finite sequence $H_0, H_1, \cdots, H_n$ of normal subgroups of G such that $H_i < H_{i+1}$, $H_0 = \{e\}$, and $H_n = G$. ■

Subnormal (subinvariant) Series of a group G is a sequence of subgroups,

$$H_0 = \{e\} \leq H_1 \leq \cdots \leq H_{i-1} \leq H_i \leq H_{i+1} \leq \cdots \leq G = H_n$$

where $H_i \trianglelefteq H_{i+1}$ and $H_i \leq G$ for each i

Why not $\triangleleft$?

A normal (invariant) Series of a group G is a sequence of subgroups,

$$H_0 = \{e\} \leq H_1 \leq \cdots \leq H_{i-1} \leq H_i \leq H_{i+1} \leq \cdots \leq G = H_n$$

where $H_i \trianglelefteq H_{i+1}$ and $H_i \trianglelefteq G$ for each i

- If G is abelian, every series is normal

Ex:- Normal series of $\mathbb{Z}$ under addition

$$\{0\} \trianglelefteq 8\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq \mathbb{Z}$$

$$\{0\} \trianglelefteq 9\mathbb{Z} \trianglelefteq \mathbb{Z}$$

$$\{0\} \trianglelefteq \langle 18 \rangle \trianglelefteq \langle 2 \rangle \trianglelefteq \mathbb{Z}_{72}$$

$$\{0\} \trianglelefteq \langle 36 \rangle \trianglelefteq \langle 18 \rangle \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 2 \rangle \trianglelefteq \mathbb{Z}_{72}$$

$$\{0\} \trianglelefteq \langle 36 \rangle \trianglelefteq \langle 9 \rangle \trianglelefteq \langle 3 \rangle \trianglelefteq \mathbb{Z}_{72}$$

Ex:- D_4 : the group of symmetries of the square

$$D_4 = \langle a, b \mid a^4 = b^2 = e, ab = ba^{-1} \rangle$$

$$= (\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \mu_3, \mu_4)$$

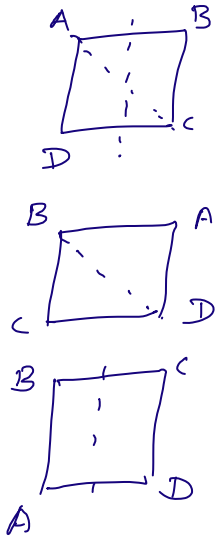
$\rho_0 \trianglelefteq \{\rho_0, \mu_1\} \trianglelefteq \{\rho_0, \rho_1, \mu_1, \mu_2\} \trianglelefteq D_4$ is a subnormal series since $\{\rho_0, \mu_1\} \not\trianglelefteq D_4$

$$\mu_3 \mu_1 \mu_3^{-1}(ABCD) = \mu_3 \mu_1 \mu_3 (ABCD)$$

$$= \mu_3 \mu_1 (BADC) = \mu_3 (BCDA)$$

$$= (CBAD) = \mu_3 (ABCD)$$

$\therefore \mu_3 \mu_1 \mu_3^{-1} = \mu_3 \notin \{\rho_0, \mu_1\}$.



35.4 Definition A subnormal (normal) series $\{K_j\}$ is a **refinement of a subnormal (normal) series** $\{H_i\}$ of a group G if $\{H_i\} \subseteq \{K_j\}$, that is, if each H_i is one of the K_j. ■

Ex: The series $\{0\} \trianglelefteq 72\mathbb{Z} \trianglelefteq 24\mathbb{Z} \trianglelefteq 8\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq \mathbb{Z}$

is a refinement of the series $\{0\} \trianglelefteq 72\mathbb{Z} \trianglelefteq 8\mathbb{Z} \trianglelefteq \mathbb{Z}$

35.6 Definition Two subnormal (normal) series $\{H_i\}$ and $\{K_j\}$ of the same group G are **isomorphic** if there is a one-to-one correspondence between the collections of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$ such that corresponding factor groups are isomorphic. ■

Clearly, two isomorphic subnormal (normal) series must have the same number of groups.

Ex:- The 2 series of $\mathbb{Z}_{15}$,

$\{0\} \trianglelefteq \langle 5\rangle \trianglelefteq \mathbb{Z}_{15}$ and $\{0\} \trianglelefteq \langle 3\rangle \trianglelefteq \mathbb{Z}_{15}$

are isomorphic.

$\mathbb{Z}_{15}/\langle 5\rangle \cong \mathbb{Z}_5$

$\langle 5\rangle/\{0\} = \langle 5\rangle \cong \mathbb{Z}_3$

&

$\mathbb{Z}_{15}/\langle 3\rangle \cong \mathbb{Z}_3$

$\langle 3\rangle/\{0\} \cong \mathbb{Z}_5$

Zassenhaus (Butterfly) Lemma

Let G be a group and let $H, K \leq G$ and $H^* \trianglelefteq H$, $K^* \trianglelefteq K$ then,

$$H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$$

$$K^*(H^* \cap K) \trianglelefteq K^*(H \cap K)$$

$$H^*(H \cap K) / H^*(H \cap K^*) \cong K^*(H \cap K) / K^*(H^* \cap K)$$

$$\cong (H \cap K) / [(H^* \cap K)(H \cap K^*)]$$

35.11 Theorem **(Schreier Theorem)** Two subnormal (normal) series of a group G have isomorphic refinements.

Ex:- Consider the series $\{0\} \leq 8\mathbb{Z} \leq 4\mathbb{Z} \leq \mathbb{Z}$ & $\{0\} \leq 9\mathbb{Z} \leq \mathbb{Z}$

refinement $\{0\} \leq 72\mathbb{Z} \leq 8\mathbb{Z} \leq 4\mathbb{Z} \leq \mathbb{Z}$

refinement $\{0\} \leq 72\mathbb{Z} \leq 18\mathbb{Z} \leq 9\mathbb{Z} \leq \mathbb{Z}$

Factor groups

$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$

$4\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}_2$

$8\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_9$

$72\mathbb{Z}/\{0\} \cong 72\mathbb{Z} \cong \mathbb{Z}$

one-to-one correspondance b/w factor groups

$\Downarrow$

Isomorphic refinements

Factor groups

$\mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}_9$

$9\mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}_2$

$18\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_4$

$72\mathbb{Z}/18\mathbb{Z} \cong 72\mathbb{Z} \cong \mathbb{Z}$

Proof

Let G be a group and let

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_n = G$$

and

$$\{e\} = K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_m = G$$

be a subnormal series for G.

$\therefore H_i, K_i \leq G$, $H_i \trianglelefteq H_{i+1}$, $K_i \trianglelefteq K_{i+1}$

$H_i(H_{i+1} \cap K_0) = H_i(H_{i+1} \cap \{e\}) = H_i\{e\} = H_i$

- Let $A \leq G$, $B \leq G$ and if $A \subseteq B$ then $A \trianglelefteq B$

$K_j \leq K_{j+1} \Rightarrow H_{i+1} \cap K_j \leq H_{i+1} \cap K_{j+1}$

$\therefore H_i(H_{i+1} \cap K_j) \subseteq H_i(H_{i+1} \cap K_{j+1})$

$\langle H_i(H_{i+1} \cap K_j) \rangle = \langle H_i, H_{i+1} \cap K_j \rangle \leq G$: smallest subgroup of G containing H_i and $H_{i+1} \cap K_j$ (or) subgroup generated by $\{H_i, H_{i+1} \cap K_j\}$ (or) $H_i(H_{i+1} \cap K_j)$ / intersection of all subgroups of G that contain $H_i(H_{i+1} \cap K_j)$

$= H_i \vee (H_{i+1} \cap K_j)$

$\langle H_i(H_{i+1} \cap K_{j+1}) \rangle = \langle H_i, H_{i+1} \cap K_{j+1} \rangle \leq G$

$H_i \trianglelefteq H_{i+1}$ and $H_{i+1} \cap K_j \leq H_{i+1}$ (proof required)

Lemma 34.4 $\Rightarrow H_i(H_{i+1} \cap K_j) \leq H_i \vee (H_{i+1} \cap K_j) \leq H_{i+1} \leq G$

$A \leq B$ & $B \leq G \Rightarrow A \leq G$

* $\therefore H_i(H_{i+1} \cap K_j) \leq G$ & Similarly, $H_i(H_{i+1} \cap K_{j+1}) \leq G$

* Let $A \leq G, B \leq G$ and if $A \subseteq B$ then $A \leq B$

$\therefore H_i(H_{i+1} \cap K_j) \leq H_i(H_{i+1} \cap K_{j+1})$

$\therefore$ For i in $0 \leq i \leq n-1$, form the chain of groups

$$H_i = H_i(H_{i+1} \cap K_0) \leq H_i(H_{i+1} \cap K_1) \leq \cdots \leq H_i(H_{i+1} \cap \underbrace{K_m}_{G}) = H_{i+1} = H_{i+1}(H_{i+2} \cap K_0)$$

This inserts $(m-1)$ not necessarily distinct groups between H_i & H_{i+1}.
Doing this for each i where $0 \leq i \leq n-1$, and let $H_{ij} = H_i(H_{i+1} \cap K_j)$,
we obtain the chain of groups:

$$\{e\} = H_0 = H_{0,0} \leq H_{0,1} \leq H_{0,2} \leq \cdots \leq H_{0,m-1} \leq H_{1,0}$$
$$\leq H_{1,1} \leq H_{1,2} \leq \cdots \leq H_{1,m-1} \leq H_{2,0}$$
$$\leq H_{2,1} \leq H_{2,2} \leq \cdots \leq H_{2,m-1} \leq H_{3,0}$$
$$\leq \cdots\cdots$$
$$\leq H_{n-1,1} \leq H_{n-1,2} \leq \cdots \leq H_{n-1,m-1} \leq H_{n-1,m} = H_{n,0} = H_n = G$$

Total additional elements in the chain $= n(m-1) = nm - n$

$\therefore$ This chain contains $n(m-1) + n + 1 = nm + 1$ not necessarily distinct groups in total, and $H_{i,0} = H_i$ for each i.

Zassenhaus (Butterfly) Lemma

Let G be a group and let $H, K \leq G$ and $H^* \trianglelefteq H$, $K^* \trianglelefteq K$ then,

$$H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$$
$$K^*(H^* \cap K) \trianglelefteq K^*(H \cap K)$$
$$H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K)$$
$$\cong (H \cap K)/[(H^* \cap K)(H \cap K^*)]$$

$N \trianglelefteq G, H \leq G \Rightarrow HN = NH \leq G$

$N, H \trianglelefteq G \Rightarrow HN = NH \trianglelefteq G$

$\therefore$ $H^* \trianglelefteq H$, $H \cap K \leq H$ ← proof required

$\Rightarrow H^*(H \cap K) \leq H \leq G$

$\Rightarrow H^*(H \cap K) \leq G$

$H_i \trianglelefteq H_{i+1}$, $H_{i+1} \cap K_j \leq H_{i+1}$

$\Rightarrow H_i(H_{i+1} \cap K_j) \leq H_{i+1} \leq G$

$\therefore H_i(H_{i+1} \cap K_j) \leq G$

$\therefore \langle H_i(H_{i+1} \cap K_j) \rangle = H_i(H_{i+1} \cap K_j)$

$H_i \trianglelefteq H_{i+1}$ and $K_j \trianglelefteq K_{j+1}$,

$$\therefore H_{i,j} = H_i(H_{i+1} \cap K_j) \trianglelefteq H_i(H_{i+1} \cap K_{j+1}) = H_{i,j+1}$$

Zassenhaus lemma $\Rightarrow$ The chain is a subnormal chain.

and therefore refines the 1st series.

In a symmetric fashion, we set $K_{j,i} = K_j(K_{j+1} \cap H_i)$ for $0 \le j \le m-1$ and $0 \le i \le n$. This gives a subnormal chain

$$\begin{aligned}\{e\} = K_{0,0} &\le K_{0,1} \le K_{0,2} \le \cdots \le K_{0,n-1} \le K_{1,0} \\ &\le K_{1,1} \le K_{1,2} \le \cdots \le K_{1,n-1} \le K_{2,0} \\ &\le K_{2,1} \le K_{2,2} \le \cdots \le K_{2,n-1} \le K_{3,0} \\ &\le \cdots \\ &\le K_{m-1,1} \le K_{m-1,2} \le \cdots \le K_{m-1,n-1} \le K_{m-1,n} \\ &= G. \end{aligned} \tag{4}$$

This chain (4) contains $mn + 1$ not necessarily distinct groups, and $K_{j,0} = K_j$ for each j. This chain refines the series (2).

$H_{i+1}, K_{j+1} \le G$ and $H_i \trianglelefteq H_{i+1}$, $K_j \trianglelefteq K_{j+1}$

$\therefore$ Zassenhaus lemma $\Longrightarrow$

$$H_i(H_{i+1} \cap K_{j+1})/H_i(H_{i+1} \cap K_j) \simeq K_j(K_{j+1} \cap H_{i+1})/K_j(K_{j+1} \cap H_i),$$

or

$$H_{i,j+1}/H_{i,j} \simeq K_{j,i+1}/K_{j,i}$$

for $0 \le i \le n-1$ and $0 \le j \le m-1$.

35.12 Definition A subnormal series $\{H_i\}$ of a group G is a **composition series** if all the factor groups H_{i+1}/H_i are simple. A normal series $\{H_i\}$ of G is a **principal** or **chief series** if all the factor groups H_{i+1}/H_i are simple. ■

* A composition (principal) series can not have further refinements

• Both of these coincide for abelian groups

15.17 Definition A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M. ■

15.18 Theorem M is a maximal normal subgroup of G if and only if G/M is simple.

Observe that by Theorem 15.18, H_{i+1}/H_i is simple if and only if H_i is a maximal normal subgroup of H_{i+1}. Thus for a composition series, each H_i must be a maximal normal subgroup of H_{i+1}. *To form a composition series of a group G, we just hunt for a maximal normal subgroup H_{n-1} of G, then for a maximal normal subgroup H_{n-2} of H_{n-1}, and so on. If this process terminates in a finite number of steps, we have a composition series.* Note that by Theorem 15.18, a composition series cannot have any further refinement. *To form a principal series, we have to hunt for a maximal normal subgroup H_{n-1} of G, then for a maximal normal subgroup H_{n-2} of H_{n-1} that is also normal in G, and so on.*

Ex:- $\mathbb{Z}$ has no composition series.

If $\{0\} = H_0 \leq H_1 \leq \cdots \leq H_{n-1} \leq H_n = \mathbb{Z}$ is a subnormal series then $H_1 = r\mathbb{Z}$ for some $r \in \mathbb{Z}^+$. Then,

$H_1/H_0 = r\mathbb{Z}/\{0\} \cong r\mathbb{Z}$

"$=$" is not used because LHS is a factor group

$kr\mathbb{Z} \leq r\mathbb{Z}$ for any $k \in \mathbb{Z}$

$r\mathbb{Z}$ is an abelian group $\Rightarrow$ all subgroup are normal

$2r\mathbb{Z} \lhd \mathbb{Z}$

$\Rightarrow$ $\mathbb{Z}$ has no composition (also no principal) series.

$\{0\} \triangle n^8\mathbb{Z} \triangleleft n^4\mathbb{Z} \triangleleft n^2\mathbb{Z} \triangleleft n\mathbb{Z} \triangle \mathbb{Z}$

$H_1/H_0 = n^8\mathbb{Z}/\{0\} \cong n^8\mathbb{Z} = \langle n^8 \rangle$ & $kn^8\mathbb{Z} \triangleleft n^8\mathbb{Z}$

Ex:- $\{e\} \trianglelefteq A_n \trianglelefteq S_n$ is a composition series. (also a principal series of S_n.

$A_n/\{e\} \cong A_n$ which is simple ~~for~~ $n \geq 5$

$S_n/A_n \cong \mathbb{Z}_2$ which is simple

15.17 Definition A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M. ■

15.18 Theorem M is a maximal normal subgroup of G if and only if G/M is simple.

Observe that by Theorem 15.18, H_{i+1}/H_i is simple if and only if H_i is a maximal normal subgroup of H_{i+1}. Thus for a composition series, each H_i must be a maximal normal subgroup of H_{i+1}. *To form a composition series of a group G, we just hunt for a maximal normal subgroup H_{n-1} of G, then for a maximal normal subgroup H_{n-2} of H_{n-1}, and so on. If this process terminates in a finite number of steps, we have a composition series*. Note that by Theorem 15.18, a composition series cannot have any further refinement. *To form a principal series, we have to hunt for a maximal normal subgroup H_{n-1} of G, then for a maximal normal subgroup H_{n-2} of H_{n-1} that is also normal in G, and so on*. The main theorem is as follows.

35.15 Theorem **(Jordan–Hölder Theorem)** Any two composition (principal) series of a group G are isomorphic.

Proof Let, Why $\triangleleft$ instead of $\trianglelefteq$?

$\{H_i\}_{i=1}^{n} : \{0\} \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft G$

$\{K_i\}_{i=1}^{m} : \{0\} \triangleleft K_1 \triangleleft K_2 \triangleleft \cdots \triangleleft K_{m-1} \triangleleft G$

be two composition (principal) series of G.

$\Rightarrow$ Each H_{i+1}/H_i, K_{i+1}/K_i is simple

35.11 Theorem **(Schreier Theorem)** Two subnormal (normal) series of a group G have isomorphic refinements.

Theorem 15.18 $\Rightarrow$ H_i, K_i are maximal normal subgroups of H_{i+1}, K_{i+1}

$\therefore$ There is no proper normal subgroup $N \triangleleft H_{i+1}$ of G properly containing H_i.

$\therefore$ There is no proper normal subgroup $N \triangleleft H_{i+1}$ of G properly containing H_i.

$\Rightarrow$ There is no refinements to be made for both the series

35.11 Theorem **(Schreier Theorem)** Two subnormal (normal) series of a group G have isomorphic refinements.

$\therefore$ $\{H_i\}$ and $\{K_i\}$ must already be isomorphic $(m = n)$.

35.6 Definition Two subnormal (normal) series $\{H_i\}$ and $\{K_j\}$ of the same group G are **isomorphic** if there is a one-to-one correspondence between the collections of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$ such that corresponding factor groups are isomorphic. ■

Clearly, two isomorphic subnormal (normal) series must have the same number of groups.

$\therefore$ $H_{i+1}/H_i \cong K_{j+1}/K_j$

Q.E.D

35.16 Theorem If G has a composition (principal) series, and if N is a proper normal subgroup of G, then there exists a composition (principal) series containing N.

$N \triangleleft G$

35.12 Definition A subnormal series $\{H_i\}$ of a group G is a **composition series** if all the factor groups H_{i+1}/H_i are simple. A normal series $\{H_i\}$ of G is a **principal** or **chief series** if all the factor groups H_{i+1}/H_i are simple. ■

- Both of these coincide for abelian groups

15.17 Definition A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M. ■

15.18 Theorem M is a maximal normal subgroup of G if and only if G/M is simple.

⇒ For a composition series $\{H_i\}$, H_i must be a maximal normal subgroup of H_{i+1}.

Proof. $N \triangleleft G$

The series $\{e\} \leq N \leq G$ is both a subnormal & a normal series.

Given that, G has a composition series $\{H_i\}$.

35.11 Theorem **(Schreier Theorem)** Two subnormal (normal) series of a group G have isomorphic refinements.

⇒ There is a refinement of $\{e\} \leq N \leq G$ to a subnormal series isomorphic to a refinement of $\{H_i\}$.

$\{H_i\}$ is a composition series ⇒ $\{H_i\}$ can have no further refinement

⇒ $\{e\} \leq N \leq G$ can be refined to a subnormal series isomorphic to the composition series $\{H_i\}$.

$\left(H_{i+1}/H_i \cong K_{j+1}/K_j\right)$

⇒ $\{e\} \leq N \leq G$ can be refined to a subnormal series all of whose factor groups are simple, i.e., to a composition series.

Ex:-

Z_4 : $|H| = 1, 2, 4$

$\therefore H^{(1)} = \langle 0 \rangle, H^{(2)} = \left\langle \frac{4}{2} \right\rangle = \langle 2 \rangle, H^{(4)} = \left\langle \frac{4}{4} \right\rangle = \langle 1 \rangle$ $\Big\}$ $\langle 0 \rangle \leq \langle 2 \rangle \leq \langle 1 \rangle = Z_4$

Z_9 : $|K| = 1, 3, 9$

$\therefore H^{(1)} = \langle 0 \rangle, H^{(3)} = \left\langle \frac{9}{3} \right\rangle = \langle 3 \rangle, H^{(9)} = \left\langle \frac{9}{9} \right\rangle = \langle 1 \rangle$ $\Big\}$ $\langle 0 \rangle \leq \langle 3 \rangle \leq \langle 1 \rangle = Z_9$

$Z_4 \times Z_9$: $1, 2, 3, 4, 6, 9, 12, 18, 36$

A composition (and also a principal) series of $Z_4 \times Z_9$ containing $\langle (0,1) \rangle$ is :

$$\langle (0,0) \rangle \leq \langle (0,3) \rangle \leq \langle (0,1) \rangle \leq \langle (2,1) \rangle \leq \langle (1,1) \rangle \leq Z_4 \times Z_9$$

36 SYLOW THEOREMS

(Fundamental Theorem of Finitely Generated Abelian Groups) Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (**Betti number** of G) of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.

The fundamental theorem for finitely generated abelian groups (Theorem 11.12) gives us complete information about all finite abelian groups. The study of finite nonabelian groups is much more complicated. The Sylow theorems give us some important information about them.

Lagrange's theorem $\Longrightarrow$ $|H| \mid |G|$ for $H \leq G$

G is abelian $\Rightarrow$ $\exists$ subgroups of every order dividing $|G|$

$|A_4| = 12$ but A_4 has no subgroup of order 6.

$\therefore$

$\exists$ non-abelian group G may have no subgroup of some order d dividing $|G|$ $\Rightarrow$ Converse of the Lagrange's theorem does not hold.

- The Sylow theorems give a weak converse. Namely, they show that if d is a power of a prime and d divides $|G|$, then G does contain a subgroup of order d. (Note that 6 is not a power of a prime.) The Sylow theorems also give some information concerning the number of such subgroups and their relationship to each other. We will see that these theorems are very useful in studying finite nonabelian groups.

Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that ■

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

$G_x = \{g \in G \mid gx = x\}.$

$X_g = \{x \in X \mid gx = x\}$

Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

If $x \in X$, the cell containing x is the **orbit of** x.

$Gx = \{gx : g \in G\}$

Let X be a finite G-set.

For $x \in X$, the orbit of x in X under G is,

$$Gx = \{gx \mid g \in G\}$$

- The orbit Gx collects all elements of X that can be reached from x using the group action.
  ie; if $x_1, x_2 \in Gx$ then $\exists g \in G$ s.t $gx_1 = x_2$
- If x_1, x_2 are in the same orbit, then $Gx_1 = Gx_2$
- If $x_1 \in Gx$ then $gx_1 \in Gx$ $\forall g \in G$

16.16 Theorem Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

Suppose, there are r orbits in X under G, and let $\{x_1, x_2, \ldots, x_r\}$ contain one element from each orbit in X.

Every element of X is in precisely one orbit, so

$$|X| = \sum_{i=1}^{r} |Gx_i|$$

There may be one element orbits in X.

Let, $\boxed{X_G = \{x \in X \mid gx = x \ \forall \ g \in G\}}$

$\therefore X_G$ is the union of the one-element orbits in X.

Suppose, there are s one-element orbits, where $0 \leq s \leq r$.

$\Rightarrow |X_G| = s$

$\therefore$ With possible reordering of the x_i,

$$\boxed{|X| = \sum_{i=1}^{r} |Gx_i| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|}$$

36.1 Theorem Let G be a group of order p^n and let X be a finite G-set. Then $|X| \equiv |X_G| \pmod{p}$.

$$|G| = p^n \Rightarrow |X| \equiv |X_G| \pmod{p}$$

Proof

Theorem 16.16 $\Rightarrow |Gx| = (G : G_x) = |G/G_x|$

$$G \text{ is finite} \Rightarrow |Gx| = |G/G_x| = \frac{|G|}{|G_x|} > 1$$

$$\Rightarrow |G| = |G_x||Gx| \quad \therefore |Gx_i| \mid |G|$$

$$\therefore |Gx_i| \mid p^n \Rightarrow |Gx_i| = 1 \text{ (or) } p^k \text{ for some } k \in \{1, 2, \ldots, n\}$$

$$\therefore p \mid |Gx_i| \text{ for } s+1 \le i \le r$$

$$\therefore p \mid \sum_{i=s+1}^{r} |Gx_i| = |X| - |X_G|$$

$$\therefore p \mid (|X| - |X_G|)$$

$$\therefore |X| \equiv |X_G| \pmod{p}$$

36.2 Definition Let p be a prime. A group G is a p-**group** if every element in G has order a power of the prime p. A subgroup of a group G is a p-**subgroup of** G if the subgroup is itself a p-group. ■

G is a p-group $\iff |G| = p^n$

36.3 Theorem (**Cauchy's Theorem**) Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and, consequently, a subgroup of order p.

$p \mid |G| \Rightarrow \exists\, g \in G \text{ s.t } g^p = e \Rightarrow \exists\, H \leq G \text{ s.t } |H| = p$

Proof.

Let the set X be the set of p-tuples $(g_1, g_2, \cdots, g_p)$ such that $g_1 g_2 \cdots g_p = e$. i.e.,

$$X = \{(g_1, g_2, \cdots, g_p) \mid g_i \in G \text{ and } g_1 g_2 \cdots g_p = e\}$$

In forming a p-tuple in X, we may choose $g_1, g_2, \cdots, g_{p-1}$ be any elements of G. Then g_p is uniquely determined as

$g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$.

$\therefore |X| = |G|^{p-1}$

$p \mid |G| \Rightarrow p \mid |G|^{p-1} \Rightarrow \boxed{p \mid |X|}$

Let σ be the cycle $(1,2,\cdots,p)$ in S_n. We let σ act on X,

$$\sigma(g_1,g_2,\cdots,g_p)=(g_{\sigma(1)},g_{\sigma(2)},\cdots,g_{\sigma(p)})=(g_2,g_3,\cdots,g_p,g_1)$$

$$g_2g_3\cdots g_pg_1=g_1^{-1}g_1(g_2g_3\cdots g_p)g_1=g_1^{-1}(g_1g_2\cdots g_p)g_1=g^{-1}eg_1=e$$

$$\therefore\ \sigma(g_1,g_2,\cdots,g_p)=(g_2,g_3,\cdots,g_p,g_1)\in X$$

$$\sigma^k(g_1,g_2,\cdots,g_p)=(g_{k+1},g_{k+2},\cdots,g_p,g_1,g_2,\cdots,g_k)$$

$$g_{k+1}g_{k+2}\cdots g_pg_1g_2\cdots g_k=(g_1g_2\cdots g_k)^{-1}(g_1g_2\cdots g_k)g_{k+1}g_{k+2}\cdots g_p(g_1g_2\cdots g_k)$$

$$=(g_1g_2\cdots g_k)^{-1}(g_1g_2\cdots g_kg_{k+1}g_{k+2}\cdots g_p)(g_1g_2\cdots g_k)$$

$$=(g_1g_2\cdots g_k)^{-1}e(g_1g_2\cdots g_k)=e$$

$$\therefore\ \sigma^k(g_1,g_2,\cdots,g_p)=(g_{k+1},g_{k+2},\cdots,g_p,g_1,g_2,\cdots,g_k)\in X$$

$\Longrightarrow$ The action of the cyclic subgroup $\langle\sigma\rangle=\{e,\sigma,\sigma^2,\cdots,\sigma^{p-1}\}$ of S_p on X forms a G-set.

$$|\langle\sigma\rangle|=p$$

36.1 Theorem Let G be a group of order p^n and let X be a finite G-set. Then $|X|\equiv|X_G|\pmod p$.

$$|G|=p^n\Longrightarrow|X|\equiv|X_G|\pmod p$$

$$|X|=|X_{\langle\sigma\rangle}|\pmod p$$

$$X_G=\{x\in X\mid gx=x\ \ \forall\ g\in G\}$$

↳ union of all one element orbits in G

$|X| - |X_{\langle\sigma\rangle}| = tp$ for $t \in \mathbb{Z}$ But $p \mid |X|$

$$\Rightarrow \boxed{p \mid |X_{\langle\sigma\rangle}|}$$

$X_{\langle\sigma\rangle}$: union of all one element orbits in $\langle\sigma\rangle$

ie : $(g_1, g_2, \cdots, g_p) \in X_{\langle\sigma\rangle} \Rightarrow \sigma^k(g_1, g_2, \cdots, g_p) = (g_1, g_2, \cdots, g_p)$

which happens iff $g_1 = g_2 = \cdots = g_p$

$(e, e, \cdots, e) \in X_{\langle\sigma\rangle} \Rightarrow |X_{\langle\sigma\rangle}| \neq 0$

$p \mid |X_{\langle\sigma\rangle}| \Rightarrow$ at least p elements in $X_{\langle\sigma\rangle}$

$\therefore \exists$ some element $a \in G$, $a \neq e$ such that $(a, a, \cdots, a) \in X_{\langle\sigma\rangle}$

Hence, $a^p = e \Rightarrow a$ has order p

$\therefore \langle a \rangle$ is a subgroup of G of order p

Q.E.D

36.4 Corollary Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of p.

G is a p-group $\iff |G| = p^n$

(or) If every element in G has order p^k for some k and prime p, then $|G| = p^n$ for some n

36.2 Definition Let p be a prime. A group G is a p-**group** if every element in G has order a power of the prime p. A subgroup of a group G is a p-**subgroup of** G if the subgroup is itself a p-group. ■

□

Let G be a group & let X = the set of all subgroups of G.

G acts on X by conjugation, i.e.,

Group action $* : G \times X \to X$ s.t if $H \in X \Rightarrow H \leq G$ and $g \in G$ then

$$g * H = \underbrace{gHg^{-1}}_{\text{conjugate subgroup}}$$

$\Rightarrow X$ is a G-set

$$G_x = \{g \in G \mid gx = x\}$$

$$G_H = \{g \in G \mid g * H = H\}$$
$$= \{g \in G \mid gHg^{-1} = H\} \quad \text{is a subgroup of } G$$

Proof.

- $g_1 g_2 \in G_H \Rightarrow g_1 H g_1^{-1} = H \;\&\; g_2 H g_2^{-1} = H \Rightarrow (g_1 g_2) H (g_1 g_2)^{-1} = g_1 (g_2 H g_2^{-1}) g_1^{-1} = g_1 H g_1^{-1} = H$

  $\therefore g_1 g_2 \in G_H$

- $g \in G_H \Rightarrow$ let $h \in H$, then $ghg^{-1} = h'$ for some $h' \in H \Rightarrow g^{-1} h' g = h \in H$

  $\therefore g^{-1} H g \subseteq H$

  For any $h \in H$, $ghg^{-1} = h' \in H \Rightarrow h = g^{-1} h' g \in g^{-1} H g$

  $\therefore H \subseteq g^{-1} H g$

- $e \in G \Rightarrow eHe^{-1} = H \Rightarrow e \in G_H$

* The subgroup $G_H = \{g \in G \mid gHg^{-1} = H\} = N[H]$ is the normalizer of H in G.

→ $H \trianglelefteq G_H = N[H]$

→ $G_H = N[H]$ is the largest subgroup of G having H as a normal subgroup

36.6 Lemma Let H be a p-subgroup of a finite group G. Then

$$(N[H] : H) \equiv (G : H) (\text{mod } p).$$

Proof

Let X : the set of left cosets of H in G. s.t $|X| = (G:H)$

Let H act on X by left translation s.t

$$h(gH) = (hg)H \in X$$

$\Rightarrow$ X is an H-set

$X_H = \{x \in X \mid hx = x \ \forall h \in H\}$: left cosets that are fixed under action by all elements of H.

$= \{gH \mid h(gH) = gH \ \forall h \in H\}$

$h(gH) = gH \Rightarrow (hg)H = gH \Rightarrow (g^{-1}H)((hg)H) = (g^{-1}H)(gH)$

$(g^{-1}hg)H = g^{-1}gH = eH = H \Rightarrow (g^{-1}hg)H = H \Rightarrow g^{-1}hg \in H$

$\therefore$

$h(gH) = gH \ \forall h \in H$ iff $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H \ \forall h \in H$

$h(gH) = gH \ \forall h \in H$ iff $(g^{-1}h(g^{-1})^{-1})H = H \ \forall h \in H$

The subgroup $G_H = N[H] = \{g \in G \mid gHg^{-1} = H\}$

$\therefore$

$h(gH) = gH \ \forall h \in H$ iff $g^{-1} \in N[H]$

$h(gH) = gH \ \forall h \in H$ iff $g \in N[H]$

$\therefore \quad X_H = \{gH \mid g \in N[H]\} \Longrightarrow |X_H| = (N[H] : H)$

$|X| = (G : H)$

36.1 Theorem Let G be a group of order p^n and let X be a finite G-set. Then $|X| \equiv |X_G| \pmod{p}$.

$|G| = p^n \Rightarrow |X| \equiv |X_G| \pmod{p}$

H is a p-group $\Rightarrow |X| \equiv |X_H| \pmod{p}$

$\therefore \quad (G : H) \equiv (N[H] : H) \pmod{p}$

Q.E.D

36.7 Corollary Let H be a p-subgroup of a finite group G. If p divides $(G : H)$, then $N[H] \neq H$.

Proof.

Lemma 36.6 $\Longrightarrow (G : H) \equiv (N[H] : H) \pmod{p}$

If $p \mid (G : H)$ then $(G : H) \equiv 0 \pmod{p}$

$\Rightarrow (N[H] : H) \equiv 0 \pmod{p}$

$\Rightarrow p \mid (N[H] : H)$

$\Rightarrow (N[H] : H) = \dfrac{|N[H]|}{|H|} \neq 1$

$\Rightarrow |N[H]| \neq |H|$

$\Rightarrow N[H] = H$

36.8 Theorem **(First Sylow Theorem)** Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and where p does not divide m. Then

1. G contains a subgroup of order p^i for each i where $1 \leq i \leq n$,
2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.

Proof

36.3 Theorem **(Cauchy's Theorem)** Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and, consequently, a subgroup of order p.

$p \mid |G| \Rightarrow \exists\, g \in G$ s.t $g^p = e \Rightarrow \exists\, H \leq G$ s.t $|H| = p$

(1)

$p \mid p^n m = |G| \Rightarrow \exists\, g \in G$ s.t $g^p = e$

ie., $\exists\, H \leq G$ s.t $|H| = p$

Induction

Let $H \leq G$ s.t $|H| = p^i$ for some $i < n$

36.6 Lemma Let H be a p-subgroup of a finite group G. Then

$$(N[H] : H) \equiv (G : H) \pmod{p}.$$

$(G:H) = \frac{|G|}{|H|} = \frac{p^n m}{p^i} \xrightarrow{i<n} p \mid (N[H] : H)$

$H \trianglelefteq N[H] \Rightarrow$ we can form $N[H]/H$

$p \mid (N[H] : H) \Rightarrow p \mid |N[H]/H|$

Cauchy's theorem $\Rightarrow \exists\, K \leq N[H]/H$ s.t $|K| = p$

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

"canonical homomorphism"

$H \trianglelefteq N[H] \Rightarrow \gamma : N[H] \to N[H]/H$ given by $\gamma(x) = xH$ is a homomorphism (canonical) with kernel H.

13.12 Theorem Let ϕ be a homomorphism of a group G into a group G'.

1. If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.
2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
4. If K' is a subgroup of $G' \cap \phi[G]$, then $\phi^{-1}[K']$ is a subgroup of G.

If $H' \leq G'$, then $\phi^{-1}(H') \leq G$

$$K \leq N[H]/H \implies \gamma^{-1}[K] = \{x \in N[H] \mid \gamma(x) \in K\} \leq N[H] \leq G$$

$$\therefore \quad \gamma^{-1}[K] \leq G$$

Now, consider

γ_K : γ restricted to $\gamma^{-1}[K]$

$$\gamma_K : \gamma^{-1}[K] \to K \quad \text{s.t} \quad \gamma_K(x) = x \quad \forall \; x \in \gamma^{-1}[K]$$

$$\ker(\gamma_K) = \ker(\gamma) \cap \gamma^{-1}[K]$$

Let $x \in \ker(\gamma) = H$, then $\gamma(x) = xH = H = e_{N[H]/H}$

$$K \leq N[H]/H \implies H = e_{N[H]/H} \in K \quad \text{ie.,} \quad \gamma(x) \in K$$

$$\therefore \quad x \in \gamma^{-1}[K]$$

$$\implies \ker(\gamma) \subseteq \gamma^{-1}[K]$$

$$\therefore \quad \ker(\gamma_K) = \ker(\gamma) \cap \gamma^{-1}[K] = \ker(\gamma) = H$$

$\phi : G \to G'$ is a homomorphism with $H = \ker(\phi) = \{x \mid \phi(x) = e \;\&\; x \in G\}$

$\implies G/H \cong \mathrm{Im}(\phi)$

$\implies G/\ker(\phi) \cong \phi[G]$

$$\therefore \quad \gamma^{-1}[K]/H \cong K \implies \left|\gamma^{-1}[K]/H\right| = |K|$$

$$\therefore \quad \frac{|\gamma^{-1}[K]|}{|H|} = |K| \implies |\gamma^{-1}[K]| = |H| \cdot |K|$$

$$= p^i \cdot p = p^{i+1}$$

$\exists\ \gamma^{-1}[K] \leq G \quad s.t \quad |\gamma^{-1}[K]| = p^{i+1}$

Q.E.D

---

② $\gamma^{-1}[K] \leq G$ and $H = \ker(\gamma) \subseteq \gamma^{-1}[K]$

$\therefore H \leq \gamma^{-1}[K] \leq N[H] \leq G$

where $|H| = p^i$ and $|\gamma^{-1}[K]| = p^{i+1}$

$H \trianglelefteq N[H] \implies H \trianglelefteq \gamma^{-1}[K]$

Q.E.D

36.9 Definition A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G, that is, a p-subgroup contained in no larger p-subgroup. ■

where, the order of the subgroup is the largest power of p dividing the order of the group $|G|$.

If $|G| = p^n \cdot m$ where p^n is the largest power of p dividing $|G|$ and m is coprime to p. Then, $|P_i| = p^n$

36.2 Definition Let p be a prime. A group G is a **p-group** if every element in G has order a power of the prime p. A subgroup of a group G is a **p-subgroup of G** if the subgroup is itself a p-group. ■

G is a p-group $\iff |G| = p^n$

36.10 Theorem **(Second Sylow Theorem)** Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G.

$P_2 = gP_1g^{-1}$ for some $g \in G$

A subgroup K of G is a **conjugate subgroup** of H if $K = i_g[H] = gHg^{-1}$ for some $g \in G$

Proof

Let $H = P_1$ & let X : the set of left cosets of P_2

Let H act on X by,

$$hx = h(gP_2) = (hg)P_2 \in X$$

$\Rightarrow X$ is an H-set

36.1 Theorem Let G be a group of order p^n and let X be a finite G-set. Then $|X| \equiv |X_G| \pmod p$.

$|G| = p^n \Rightarrow |X| \equiv |X_G| \pmod p$

$|X| = |X_{P_1}| \pmod p$ where $|X| = (G : P_2) = \frac{|G|}{|P_2|} = \frac{p^n m}{p^n} = m \not\equiv 0 \pmod p$

$\therefore |X_{P_1}| \neq 0$

$X_H = \{x \in X \mid hx = x \ \forall h \in H\}$

$= \{gP_2 \mid h(gP_2) = gP_2 \ \forall h \in H\}$: left cosets that are fixed under action by all elements of H

$h(gP_2) = gP_2 \Rightarrow (hg)P_2 = gP_2 \Rightarrow (g^{-1}P_2)((hg)P_2) = (g^{-1}P_2)(gP_2)$

$(g^{-1}hg)P_2 = (g^{-1}g)P_2 = eP_2 = P_2 \Rightarrow (g^{-1}hg)P_2 = P_2 \Rightarrow g^{-1}hg \in P_2$

$\therefore$

$h(gP_2) = gP_2 \ \forall h \in P_1$ iff $g^{-1}hg \in P_2 \ \forall h \in P_1$

$\Rightarrow g^{-1} P_1 g \subseteq P_2$

$|P_1| = |P_2| \Rightarrow |g^{-1} P_1 g| = |P_1| = |P_2|$

$\therefore \quad g^{-1} P_1 g = P_2$

Q.E.D

36.11 Theorem **(Third Sylow Theorem)** If G is a finite group and p divides $|G|$, then the number of Sylow p-subgroups is congruent to 1 modulo p and divides $|G|$.

$p \mid |G| \Rightarrow \#\{\text{Sylow } p\text{-subgroups}\} \equiv 1 \pmod p$

$\#\{\text{Sylow } p\text{-subgroups}\} \mid |G|$

$\left\{ |G| = p^n m \right.$

36.2 Definition Let p be a prime. A group G is a ***p*-group** if every element in G has order a power of the prime p. A subgroup of a group G is a ***p*-subgroup of G** if the subgroup is itself a p-group. ■

G is a p-group $\iff |G| = p^n$

Proof

Part 1

Let H : one Sylow p-subgroup of G

Let X : the set of all Sylow p-subgroups

Define H act on X by,

$$hT = hTh^{-1} \in X \qquad [\text{Theorem } 36.10]$$

where $T \in X$

$\Rightarrow X$ is a P-set

Theorem 36.1 $\Rightarrow |X| \equiv |X_H| \pmod p$

$$X_H = \{T \in X \mid hT = T \ \forall\ h \in H\} = \{T \in X \mid hTh^{-1} = T \ \forall\ h \in H\}$$

$hTh^{-1} = T \ \forall\ h \in H$ iff $h \in N[T] \ \forall\ h \in H$

$$G_H = \{g \in G \mid gHg^{-1} = H\} = N[H] \quad \& \quad H \trianglelefteq G_H = N[H]$$

$\therefore H \trianglelefteq N[T]$ and ofcause $T \trianglelefteq N[T]$

36.9 Definition A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G, that is, a p-subgroup contained in no larger p-subgroup. ■

where, the order of the subgroup is the largest power of p dividing the order of the group $|G|$.

If $|G| = p^n \cdot m$ where p^n is the largest power of p dividing $|G|$ and m is coprime to p. Then, $|P_i| = p^n$

H & T are Sylow p-subgroups of G

↳ H & T are Sylow p-subgroups of $N[T]$

Second Sylow theorem ⇒ H & T are conjugate subgroups of $N[T]$

$\exists\ g \in N[H]$ s.t $gTg^{-1} = H$

but $T \trianglelefteq N[T] \Rightarrow gTg^{-1} = T \quad \forall\ g \in N[T]$

$\therefore\ H = gTg^{-1} = T$

G is a p-group $\iff |G| = p^n$

$H = T \Rightarrow X_H = \{H\} \Longrightarrow |X_H| = 1$

$\therefore\ |X| \equiv |X_H| \equiv 1 \pmod p$ Q.E.D

Part 2

H act on X by conjugation,

$|X_H| = 1 \Rightarrow$ there is only one orbit in X under H

16.16 Theorem Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$. & $Gx = \{gx \mid g \in G\}$ the orbit of x in G

$\therefore \quad |X_p| = |X| = |\text{orbit of } H| = (G : G_H) = \dfrac{|G|}{|G_H|}$, $H \in X$

($G_H = N[H]$ Normalizer of H)

$(G : G_H) \mid |G| \implies |X| \mid |G|$

$\therefore$ The # of Sylow p-subgroups divides $|G|$

Q.E.D