

Theorem 1.4.7

(1) To say $\alpha\beta = \beta\alpha$, it suffices to show that $\forall a \in X$,

$$\alpha\beta(a) = \beta\alpha(a)$$

$$X = \{a_1, a_2, \dots, a_n\} \sqcup \{b_1, b_2, \dots, b_s\} \\ \sqcup \{\text{the rest}\}$$

C1 - $a \in \{a_1, \dots, a_n\}$ say a_i

$$\alpha(a_i) = a_{i+1}$$

$$\beta(\alpha(a)) = \beta(a_{i+1}) = a_{i+1} \quad \}$$

$$\beta(a_i) = a_i$$

$$\alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1} \quad \}$$

$$\left. \begin{array}{l} \alpha\beta(a) \\ = \beta\alpha(a) \end{array} \right\}$$

Similarly, it can be shown for
 $a \in \{b_1, \dots, b_s\}$ & $a \in \{\text{the rest}\}$

$$(2) \quad X = \{a_1, \dots, a_r\} \sqcup X \setminus \{a_1, \dots, a_r\}$$

C1 - $a \in \{a_1, \dots, a_r\}$ say a_i

$$1.1 \quad \alpha(a_i) = a_{i+1}, \quad 1 \leq i < r$$

$$(a_1 a_2) \dots (a_{r-1} a_r)(a_i) = a_{i+1}$$

$$1.2 \quad a = a_r$$

$$\alpha(a_r) = a_1$$

$$(a_1 a_2) \dots (a_{r-1} a_r) = a_1$$

C2 - $a \in X \setminus \{a_1, \dots, a_r\}$

$$\alpha(a) = a$$

$$(a_1 a_2) \dots (a_{r-1} a_r)(a) = a$$

$$(3) \quad X = \underbrace{\{a_1, \dots, a_x\}}_{3.1} \quad \amalg \quad \underbrace{X \setminus \{a_1, \dots, a_x\}}_{3.2}$$

$$\underline{3.1} \quad a = a_i \quad (\text{say}) \quad (1 < i < x)$$

$$\begin{aligned} (a_1 \dots a_x) (a_x \dots a_1) (a_i) &= (a_1 \dots a_x) (a_{i-1}) \\ &= a_i = \text{Id}_X(a_i) \end{aligned}$$

If $a = a_i$,

$$\begin{aligned} (a_1 \dots a_x) (a_x \dots a_1) (a_1) &= (a_1 \dots a_x) (a_x) \\ &= a_1 = \text{Id}_X(a_1) \end{aligned}$$

$$\underline{3.2} \quad (a_1 \dots a_x) (a_x \dots a_1) (a) = a = \text{Id}_X(a)$$

1 Not every elem of g has finite

eg - $(\mathbb{Z}, +, 0)$

2 $g^m = e \Rightarrow g^{km} = e, k \in \mathbb{Z}_{>0}$

$\curvearrowright (g^m)^k = e^k \curvearrowright$

3. $\underbrace{o(g)}_{{\text{Order of } g}} = 1 \Leftrightarrow g = e$

PT (a_1, a_2, \dots, a_r) has order 1 .

Pf - $\sigma = (a_1, \dots, a_r)$

we need to show

1. $\sigma^\lambda = e$

2. $0 < i < \lambda, \sigma^i \neq e$

$$\underline{\text{Pf}}^n : \sigma^i(\alpha_i) = \alpha_{\overline{j+i}},$$

$\overline{j+i}$ = remainder of $i+j$
divided by λ in
 $\{1, \dots, \lambda\}$

$$\begin{aligned} \underline{\text{Pf}} - \underline{\text{BC}}: \quad & \sigma(\alpha) = \alpha_{\overline{j+1}} \\ \underline{\text{IH}}: \quad & \sigma^{i+1}(\alpha_j) = \sigma(\alpha_{\overline{j+i}}) \\ &= \alpha_{\overline{j+i+1}} \end{aligned}$$

$$\text{By PMI, } \sigma^i(\alpha_j) = \alpha_{\overline{i+j}}$$

$$\begin{aligned} \underline{1. \text{ So}}, \quad \text{for } i=1, \quad & \sigma^k(\alpha_j) = \alpha_{\overline{1+j}} \\ &= \alpha_j \quad \text{if } j \\ & \underline{\sigma^k = e} \end{aligned}$$

$$\begin{aligned} \underline{2. \text{ If }} \quad & 0 < i < \lambda, \quad \sigma^i(\alpha_1) = \alpha_{\overline{i+1}} \neq \alpha_1 \\ & | < i+1 < \lambda+1 \\ \Rightarrow & | < i+1 \leq \lambda \end{aligned}$$

Ex 1.S.2

① Show that the transpositions $(i, j) \in S_n$ generate S_n ($i \neq j$)

Pf

A $\sigma \in S_n$, $\exists \sigma_1, \dots, \sigma_p \in S_n$

s.t

$\sigma = \sigma_1 \sigma_2 \dots \sigma_p$ s.t σ_i 's are
disjoint cycles

let $\sigma_i = (\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ij_i})$

so, $\sigma = (\alpha_{11}, \dots, \alpha_{1j_1}) \dots (\alpha_{p1}, \alpha_{p2}, \dots, \alpha_{pj_p})$

By thm, A σ_i

$\sigma_i = (\alpha_{i1}, \alpha_{i2})(\alpha_{i2}, \alpha_{i3}) \dots (\alpha_{i(j_i-1)}, \alpha_{ij_i})$

$\therefore \sigma = (\alpha_{11}, \alpha_{12}) \dots (\alpha_{1(j_1-1)}, \alpha_{1j_1})(\alpha_{21}, \alpha_{22}) \dots \dots (\alpha_{p(j_p-1)}, \alpha_{pj_p})$

Hence, $(i, j) \in S_n$ generate S_n

(2) Show $(12), (13), \dots, (1n)$ generate S_n

Pf - Suppose, we can show that each transposition (i, j) can be generated by elements of the set $\{(12), (13), \dots, (1n)\}$.

Since (ij) can generate S_n , therefore $\{(12), (13), \dots, (1n)\}$ can generate S_n .

$$(ij) = (1j)(1i)(1j), \quad i \notin \{i, j\}$$

$$\text{if } \alpha \notin \{1, i, j\} \Rightarrow \text{LHS} = \text{RHS}$$

$$\begin{aligned} \alpha \in \{1, i, j\} &\rightarrow \alpha = 1 \checkmark \\ &\rightarrow \alpha = i \checkmark \\ &\rightarrow \alpha = j \checkmark \end{aligned}$$

□

(2) Show that $Y = \{(12), (23), \dots\}$ generates S_n

Pf - We will show Y generates $(1 \ k)$

BC : $(1 \ 2)$

IH : $(1 \ k-1)(k-1 \ k)(1 \ k-1) = (1 \ k)$
 $\forall k > 2$

By PMI, $(k-1, k)$ generates $(1 \ k)$

(3) Show that $(1, 2, \dots, n) \ \& \ (12)$ generate S_n

Pf let $(1, 2, \dots, n) \ \& \ (12)$ generate $(k-1 \ k)$

BC :

IH : $(1, 2, \dots, n)(k-1 \ k)(\underbrace{(1, 2, \dots, n)}_{-1}^{(n-1)}) = (k \ k+1)$

By PMI, $(1, 2, \dots, n) \ \& \ (12)$ generate $(k-1, k)$

Ex 1.S.1

$$\beta = (a_1, \dots, a_n), \quad \gamma \in S_n$$

PT $\gamma \beta \gamma^{-1} = (\gamma(a_1), \dots, \gamma(a_n))$

Pf -
$$\begin{aligned}\beta(a_i) &= a_{i+1}, \quad i \leq n \\ \beta(n) &= n \quad \text{if } n \neq a_i \quad \forall i \leq n\end{aligned}$$

We need to show

$$\begin{aligned}\gamma \beta \gamma^{-1}(\gamma(a_i)) &= \gamma(a_{i+1}) \\ \gamma \beta \gamma^{-1}(n) &= n \quad \text{if } n \neq \gamma(a_i) \\ &\quad \text{for any } i \leq n\end{aligned}$$

$$\begin{aligned}1. (\gamma \beta \gamma^{-1})(\gamma(a_i)) &= \gamma \beta \underbrace{(\gamma^{-1} \gamma)}_e (a_i) = \gamma \beta(a_i) \\ &= \gamma(a_{i+1})\end{aligned}$$

2.

$$\begin{aligned}\text{If } n &\neq \gamma(a_i) \quad \text{for any } i \leq n \\ \Rightarrow \gamma^{-1}(n) &\neq \gamma^{-1}\gamma(a_i) = a_i \quad (\because \gamma \text{ is an injection})\end{aligned}$$

$$\gamma \beta \gamma^{-1}(n) = \gamma \beta(\gamma^{-1}(n)) = \gamma \gamma^{-1}(n) = n$$

Remark : Let β_k , $1 \leq k \leq l$ be cycles
not necessarily disjoint.

Consider $\beta = \beta_1 \beta_2 \cdots \beta_l$

$(b_{11}, b_{12}, \dots, b_{1n_1})$	$(b_{e1}, b_{e2}, \dots, b_{en_e})$
-------------------------------------	-------------------------------------

$$\begin{aligned}
 \gamma \beta \gamma^{-1} &= \gamma \beta_1 \beta_2 \cdots \beta_l \gamma^{-1} \\
 &= (\gamma \beta_1 \gamma^{-1}) \gamma \beta_2 \cdots (\gamma \beta_l \gamma^{-1}) \\
 &= (\underbrace{\gamma \beta_1 \gamma^{-1}}_{(\gamma(b_{11}), \gamma(b_{12}), \dots, \gamma(b_{1n_1}))}) \quad (\underbrace{\gamma \beta_2 \gamma^{-1} \cdots \gamma \beta_l \gamma^{-1}}_{(\gamma(b_{e1}), \dots, \gamma(b_{en_e}))})
 \end{aligned}$$

Ch 2 : SubGps

Lemma - let $H \subseteq G$ be a non-empty subset satisfying

$$1. \quad \forall a, b \in H, \quad a \cdot b \in H$$

$$2. \quad a \in H \Rightarrow a^{-1} \in H$$

Then H is a group.

Pf 1. H is a non-empty set

$$\exists a \in H. \quad \Rightarrow a^{-1} \in H$$

$$\Rightarrow a \cdot a^{-1} \in H$$

$$\Rightarrow e \in H$$

2. $m: G \times G \rightarrow G$

$$m_H: H \times H \rightarrow G$$

$$\therefore \forall a, b \in H, \quad a \cdot b \in H$$

$$\therefore \text{img}(m_H) \subseteq H$$

so) $m_H: H \times H \rightarrow H$

$$(a, b) \mapsto a \cdot b$$

Associativity follows from defⁿ of (G, \cdot, e)

3. $m_H(a, e) = m(a, e) = a$
 $= m(e, a) = m_H(e, a)$

4. $a \in H \Rightarrow a^{-1} \in H$

So, $m(a, a^{-1}) = e = m(a^{-1}, a)$
 $\Rightarrow m_H(a, a^{-1}) = e = m_H(a^{-1}, a)$

$\Rightarrow a^{-1}$ is inverse of in H .

Hence, (H, m, e) is a group.

eg - 1. $\{e\}$ & G are trivial subgroups
of G

2. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ subgroups

3. $2\mathbb{Z} \subset \mathbb{Z}$ is a subgroup.

\mathbb{Z} (set of all
even integers)

set of odd integers is not a subgp.

4. $n\mathbb{Z} \subset \mathbb{Z}$ is a subgp.

$$= \{n \cdot m : m \in \mathbb{Z}\}$$

5. $m|n \Rightarrow m\mathbb{Z} \subset n\mathbb{Z}$ subgp.

6. $H = \{e, (i, j)\}$

Q. Is $H = \{e, (13), (24), (13)(24)\}$
a subgrp. of S_4 ?

Pf 1. $e \in H \Rightarrow H \neq \emptyset$

2. $\forall a, b \in H, a \cdot b \in H$

3. $e^{-1} = e$
 $(13)^{-1} = (13)$
 $(24)^{-1} = (24)$
 $((13)(24))^{-1} = (13)(24)$

$\left. \begin{array}{c} \\ \\ \\ \end{array} \right\} \in H$

$\therefore H \subseteq S_4$ is a subgrp.

eg - $H = \{e, (13), (24), (13)(24), (14)\}$
is not a subgrp.

$\therefore (13)(14) \notin H$

Ex - $y \subseteq X$

$$\text{Aut}(X, Y) = \{ \varphi \in \text{Aut}(X) : \varphi(Y) = Y \}$$

Show that $\text{Aut}(X, Y)$ is a sub gp.
of $\text{Aut}(X)$

Pf 1. $\text{Id}_X(Y) = Y$

$$\therefore \text{Id}_X \in \text{Aut}(X, Y)$$

$$\therefore \text{Aut}(X, Y) \neq \emptyset$$

2. Consider $\varphi_1, \varphi_2 \in \text{Aut}(X, Y)$

$$\varphi_1 \circ \varphi_2(Y) = \varphi_1(\varphi_2(Y)) = \varphi_1(Y) = Y$$

$$\therefore \varphi_1 \circ \varphi_2 \in \text{Aut}(X, Y)$$

3. $\because \varphi \in H \Rightarrow \varphi \in G \quad \exists \varphi^{-1} \in G$

$$\begin{aligned} \varphi(Y) = Y &\Rightarrow (\varphi^{-1} \circ \varphi)(Y) = \varphi^{-1}(Y) \\ &\Rightarrow Y = \varphi^{-1}(Y) \end{aligned}$$

$$\therefore \varphi^{-1} \in \text{Aut}(X, Y)$$

$$\therefore \varphi \circ \varphi^{-1} = \text{Id}_X = \varphi^{-1} \circ \varphi$$

$\therefore \varphi^{-1}$ is inverse of φ in H

Hence, $\text{Aut}(X, Y)$ is a subgp.

eg - $X = \{1, 2, 3, 4\}$, $Y = \{1, 3\}$
Find $\text{Aut}(X, Y)$

$$\text{Aut}(X, Y) = \left\{ e, \underbrace{(2 \ 4)}, \underbrace{(1 \ 3)}, \underbrace{(1 \ 3)(2 \ 4)} \right\}$$
$$\begin{array}{ll} 1 \rightarrow 1 & 1 \rightarrow 3 \\ 3 \rightarrow 3 & 3 \rightarrow 1 \end{array}$$

Note - 1 If $y_1 \subseteq y_2 \subseteq X$,

then $\text{Aut}(X, Y_1) \subseteq \text{Aut}(X, Y_2) \subseteq \text{Aut}(X)$

2. If X is finite,

$$\text{Aut}(X, Y) = \text{Aut}(X, X-Y)$$

Let $S \subseteq G$ be a subset.

centralizer of S in G

$$C_G(S) = \{ g \in G : gx = xg \quad \forall x \in S \}$$

Pf. of $C_G(S)$ being a gp. -

O. $e \in C_G(S)$ $\because e \cdot n = n \cdot e \quad \forall n \in S$

$$\therefore C_G(S) \neq \emptyset$$

L. $a, b \in C_G(S) \Rightarrow an = na \quad \forall n \in S$
 $b n = n b$

$$(ab)n = a(bn) = a(nb) = (an)b = n(ab)$$

so, $a \cdot b \in C_G(S)$

2. $a \in C_G(S) \Rightarrow an = na \quad \forall n \in S$
 $\Rightarrow a^{-1}ana^{-1} = a^{-1}naa^{-1}$
 $\Rightarrow na^{-1} = a^{-1}n$

so, $a^{-1} \in C_G(S)$

Hence $C_G(S)$ is a subgp. of G .

eg - 1. $g = s_3$, $S = \{(12)\}$

$$G_S(g) = \{g \in S_3 : g \cdot (12) = (12)g\}$$

$\frac{g}{e}$	$\frac{g(12)}{(12)}$	$\frac{(12)g}{(12)}$	= ?
(12)	e	e	✓
(23)	(13)	(123)	✗
(13)	.	.	✗
(123)	.	.	✗
(132)	.	.	✗

2 If $g = s_4$,
 $(34) \in G_S(g)$ for $S = \{(12)\}$

↳ cycle disjoint
with (12)

G is called abelian (or commutative)
if $ab = ba \quad \forall a, b \in G$

If G is abelian, then $C_S(G) = G \quad \forall S \subseteq G$

<u>Note</u> -	<u>Abelian</u>	<u>Non-abelian</u>
	$(\mathbb{Z}, +, 0)$	$S_n \quad (n > 2)$
	$(M_n(\mathbb{R}), +, 0)$	$(GL(n, \mathbb{R}), \cdot, g_{dn})$

Ex - Let $g \in G$

$$H_{(g)} = \{g^i : i \in \mathbb{Z}\}$$

Show that $H_{(g)}$ is a subgp.

Pf - O. $g = g^1 \Rightarrow g \in H_{(g)}$
 $\therefore H_{(g)} \neq \emptyset$

1. $a, b \in H_{(g)} . \exists i, j \text{ s.t } a = g^i \text{ & } b = g^j$
 $a \cdot b = g^{(i+j)} \in H_{(g)}$

2. $a \in H_{(g)} \quad \exists i \text{ s.t } a = g^i$

$$a^{-1} = g^{-i} = g^{m-i} \in H_{\langle g \rangle}$$

e.g - $\underline{1}$. $n \in \mathbb{Z}$, $H_{\langle n \rangle} = \{an : a \in \mathbb{Z}\} = n\mathbb{Z}$

2. S_3

$$H_{\langle (12) \rangle} = \{e, (12)\}$$

$$H_{\langle (123) \rangle} = \{e, (123), (132)\}$$

Then - Cardinality of $H_{\langle g \rangle}$ is equal to the order of g .

Pf - $\underline{1}$. $O(g)$ is infinite

Suppose $H_{\langle g \rangle} = \{e, g, g^2, \dots\}$ is finite

$$\begin{aligned} \therefore \exists i, j \in \mathbb{Z} \text{ s.t. } i \neq j \quad & \& g^i = g^j \\ \Rightarrow g^i g^{-j} &= g^j g^{-j} \\ \Rightarrow g^{(i-j)} &= e \end{aligned}$$

$\Rightarrow O(g)$ is finite.

which is a contd".

so, $|H_{\langle g \rangle}|$ is infinite

2. $O(g)$ is finite.

Let $O(g) = m$

Claim - $H_{\langle g \rangle} = \{g^i : 0 \leq i < m\}$ &
 $|H| = |\{g^i : 0 \leq i < m\}| = m$

Claim 1 - $H_{\langle g \rangle} \subseteq \{g^i : 0 \leq i < m\} = H$

Let $g^a \in H_{\langle g \rangle}$; $a \in \mathbb{Z}$

By division algorithm, $\exists k, \lambda \in \mathbb{Z}$

s.t $a = km + \lambda$, $0 \leq \lambda < m$

$$g^a = g^{km+\lambda} = (g^m)^k g^\lambda = e^k \cdot g^\lambda = g^\lambda \in H$$

Hence, $H_{\langle g \rangle} = H$ (\because Obv. $H \subseteq H_{\langle g \rangle}$)

Claim 2 : $|H'| = m$

Clearly $|H'| \leq m$

Suppose $g^i = g^j$, $i \neq j$, $0 \leq i, j < m$
 $\Rightarrow g^{(i-j)} = e$ & $i-j < m$

which is a contdn as $O(g) = m$

Hence, $|H'| = m$

Consider $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

	\mathbb{Z}_2	\mathbb{Z}_3	\mathbb{Z}_4
$O(1)$	2	3	4
$O(2)$	-	3	2
$O(3)$	-	-	4
⋮			

Similarly, $O(1) = O(n-1) = n$ in \mathbb{Z}_n

Note - If $\gcd(a, n) = 1$, then $O(a) = n$
 $(0 < a < n)$ in \mathbb{Z}_n

Pf - Let $O(a) = k \Rightarrow ka = 0 \pmod{n}$
 $\because \gcd(a, n) = 1$, $\therefore k = 0 \pmod{n}$
 $\Rightarrow k = n$

Hence, $O(a) = n$

In general, $O(b) = \frac{n}{\gcd(n, b)}$

Given a gp. G & a sg. HCG.
we want to define an eq. relⁿ on G .

for $x, y \in G$. we define $x \sim y$ if $xy^{-1} \in H$.

Checking ER

R: $x \in G$, $xx^{-1} = e \in H$

S: $x \sim y \Rightarrow xy^{-1} \in H$

$\because H$ is sg.

$\therefore (xy^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H \quad \left((xy^{-1})^{-1} = yx^{-1} \text{ trivial} \right)$

T: $x \sim y, y \sim z \Rightarrow xy^{-1}, yz^{-1} \in H$

$\Rightarrow xy^{-1} \cdot yz^{-1} \in H$

$\Rightarrow xz^{-1} \in H$

$\therefore x \sim z$

Thus, this is an eq. relⁿ.

This eq. relⁿ breaks G into disjoint eq. classes.

What are the eq. classes?

Ppⁿ: For any $g \in G$, the eq. class of g is precisely the set

$$EC(g) = Hg := \{ hg \mid h \in H \}$$

i.e. $x \in G$ s.t. $x \sim g \Leftrightarrow x \in Hg$

Pf - ① $EC(g) \subset Hg$

$$\text{Suppose } x \sim g \Rightarrow xg^{-1} \in H$$

$$\Rightarrow \exists h \in H \text{ s.t. } xg^{-1} = h$$

$$\Rightarrow xg^{-1}g = hg$$

$$\Rightarrow x = hg$$

$$\Rightarrow x \in Hg$$

$$\therefore EC(g) \subset Hg$$

② $Hg \subset EC(g)$

Consider $x \in Hg \Rightarrow \exists h \in H$ s.t

$$x = hg$$

$$\Rightarrow xg^{-1} = hgg^{-1}$$

$$\Rightarrow xg^{-1} = h$$

$$\Rightarrow xg^{-1} \in H$$

$$\Rightarrow x \sim g$$

$$\therefore Hg \subset EC(g)$$

Hence, $EC(g) = Hg$.

$$q = \coprod EC(g) = \coprod Hg$$

$$\begin{aligned}Rg : G &\rightarrow G \\x &\mapsto xg\end{aligned}$$

Claim : Rg is a bijection.

Pf - It is suff. to show
that $\exists Rg^{-1}$ s.t

$$Rg \circ Rg^{-1} = \text{id}_G = Rg^{-1} \circ Rg$$

$$Rg \circ Rg^{-1}(x) = Rg(xg^{-1}) = xg^{-1}g = x$$

$$Rg^{-1} \circ Rg(x) = Rg^{-1}(xg) = xgg^{-1} = x$$

$\Rightarrow Rg$ is a bijection.

Alternatively, we could have directly shown that Rg is injective & surjective.

$$\text{Clearly, } Hg = Rg(H)$$

A bijective map preserves 'size' of sets.

so, if G is a finite group, then
 H is finite.

$$\therefore \#Rg(H) = \#Hg \\ = \#H$$

$$\therefore \#H = \#Hg$$

$$\begin{aligned} \text{Since, } G &= EC(g_1) \sqcup EC(g_2) \dots \sqcup EC(g_e) \\ &= Hg_1 \sqcup Hg_2 \dots \sqcup Hg_e \end{aligned}$$

$$\begin{aligned} \#G &= (\#H)l \\ \Rightarrow \#H &\mid \#G \end{aligned}$$

□

(Lagrange's Thm)

Structure of Pf

1. Put eq. relⁿ on G
2. Checked that eq. classes are of the form $E(x) = Hx$
3. Showed $Rg: G \rightarrow G$, $Rg(x) = xg$ is a bijection $\Rightarrow \#(Hg) = \#H$
 $\Rightarrow \#G = \#H (\# \text{eq. classes})$

L. $\#G = p$. Let $g \in G$, $g \neq e$.
Then $\langle g \rangle = G$

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$$

Pf - By LT, $\#\langle g \rangle \mid \#G = p$

$$\Rightarrow \#\langle g \rangle = 1, p$$

$\begin{matrix} x \\ \therefore g \neq e \end{matrix}$

$$\Rightarrow \#\langle g \rangle = p = \#G$$
$$\Rightarrow \underline{\langle g \rangle = G}$$

□

C: If $\#G = p$ (prime), then G is generated by every non-triv. elem. of G .

C: If $\#G = p$, then for $g \neq e$, $O(g) = p$
 $(\because O(g) = \#(g))$

C: Let G be a finite gp. Then
 $O(g) \mid \#G$ for $g \in G$

$$\left\{ \begin{array}{l} \because O(g) = \underbrace{\#(g)}_{LT} \mid \#G \end{array} \right\}$$

R: Given $d \mid \#G$, does there exist $g \in G$
s.t. $d = O(g)$?

No!

$\therefore \#G \mid \#G$, does there exist an elem. g
with $O(g) = \#G$?

If yes, let g be such elem.

Then $\#(g) = o(g) = \#g \Rightarrow \langle g \rangle = g$

But, $\langle g \rangle$ is Abelian, while G may not be Abelian

$$eg - S_3$$

Now, consider $d(\#G) & d \subset \#G$.

Still, the answer remains no.

If g_1, g_2 are 2 gps. then there is a natural group structure on $g_1 \times g_2$.

$$(g_1, g_2) \cdot (g_1', g_2') := (g_1g_1', g_2g_2')$$

Note that,

$$\begin{aligned} \text{Assoc} \quad & (g_1, g_2) \cdot ((g_1', g_2') \cdot (g_1'', g_2'')) \\ &= ((g_1, g_2) \cdot (g_1', g_2')) \cdot (g_1'', g_2'') \end{aligned}$$

Id $e = (e_1, e_2)$

Inv. $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$

Now, consider $G = \{\pm 1\}$

$$O(g) = 2 \quad \forall g \in G \times G \times G \times G$$

which is a counterexample

Ex 1 If $H \subset \mathbb{Z}$, then $\exists n$ s.t $H = \{n\}$

Pf - let $H \subset \mathbb{Z}$ be a sg.

If $H = \{0\}$, then there is nothing to show

Else, $\exists n \in \mathbb{Z}$ s.t $n \neq 0$ & $n \in H$.

$$\Rightarrow (-n) \in H$$

Either n or $(-n)$ is (tve)

$\therefore H$ contains a (tve) integer

Consider the smallest (tve) int $n_0 \in H$

Claim $H = \{n_0\}$

$$= \{\dots, -2n_0, -n_0, 0, n_0, 2n_0, \dots\}$$

Consider $h \in H$.

By EDL, $\exists q \in \mathbb{Z}$, $0 \leq r < n_0$ s.t $h = qn_0 + r$

If $r = 0$, $h = qn_0 \Rightarrow h \in \{n_0\}$

$r \neq 0 \Rightarrow h = \underbrace{h - qn_0}_{\in H} + \underbrace{qn_0}_{\in H} \Rightarrow h \in H$ & $0 < r < n_0$

which is a contdⁿ since we assumed
no to be the smallest such int.

Ex 2:

L: Let $g \in G$ be an elem. of finite order n . Let $m \geq 1$ be an int. s.t $m \mid n$.

Then $g^{\frac{n}{m}}$ has order m .

Pf - $(g^{\frac{n}{m}})^m = g^n = e$

We need to now check that m is the smallest such int.

If not, $\exists 1 \leq k < m$ s.t $(g^{\frac{n}{m}})^k = e$
 $g^{\frac{nk}{m}} = e$

But, $\frac{nk}{m} < n$ which is a contdⁿ
 $\therefore O(g) = n$

Ex 3:

$$\text{Pf} - H_a = \{e, a, \dots, a^{n-1}\}$$

$$H_b = \{e, b, \dots, b^{m-1}\}$$

Consider $g \in H_a \cap H_b$

$$\because g \in H_a$$

$$\because g \in H_b$$

$$\therefore o(g) | \#H_a \Rightarrow o(g) | n \}$$

$$\therefore o(g) | \#H_b \Rightarrow o(g) | m \}$$

coprime

$$\Rightarrow o(g) = 1$$

$$\Rightarrow \underline{g = e}$$

Ex 4 :

$$\begin{aligned} \perp \quad (ab)^{mn} &= a^{mn} b^{mn} \quad (\because G \text{ is abelian}) \\ &= (a^m)^n (b^n)^m \\ &= e \end{aligned}$$

$$\text{Let } o(ab) = k, \quad (ab)^k = e$$

$$\text{Suppose } g = a^k = b^{-k}$$

Then $g \in H_a \cap H_b$

$$\Rightarrow g = e$$

$$\Rightarrow a^k = b^{-k} = e$$

$$\Rightarrow a^k = e \quad \& \quad b^k = e$$

$$\Rightarrow m|k \quad \Rightarrow n|k$$

$$\Rightarrow mn|k \quad (\because \gcd(m, n) = 1)$$

To prove k is smallest,

$$k \leq mn \quad \& \quad mn|k \Rightarrow k = mn$$

$$\left. \begin{array}{l} \text{L: } O(g) = n \quad \& \quad g^m = e \Rightarrow n|m \\ \text{Pf: } m = nq + r \Rightarrow \underbrace{g^r}_{\substack{\text{contd}^n \\ 0 \leq r < n}} = e \end{array} \right\}$$

L: If $n|k$ & $m|k$, then $\text{lcm}(m, n)|k$

Pf - $n = p_1^{l_1} \cdots p_r^{l_r} q_1^{a_1} \cdots q_s^{a_s}$
 $m = p_1^{s_1} \cdots p_r^{s_r} c_1^{d_1} \cdots c_t^{d_t}$

where p_i, q_i, c_i are primes
 $l_i, s_i, a_i, d_i > 0$

$$\text{gcd}(n, m) = p_1^{\min\{l_1, s_1\}} \cdots p_r^{\min\{l_r, s_r\}}$$

Pf - Let $d|n$ & $d|m$.

Consider a prime p s.t $p \nmid d$
 $\Rightarrow p = p_i \quad , \quad 1 \leq i \leq r$

$$\text{So, } d = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{where } \alpha_i \geq 0$$

$$\begin{aligned} d|n \Rightarrow \alpha_i \leq l_i \\ d|m \Rightarrow \alpha_i \leq s_i \end{aligned} \quad \Rightarrow \quad \alpha_i \leq \min\{l_i, s_i\} \quad \forall i$$
$$\Rightarrow d \mid \prod p_i^{\min\{l_i, s_i\}}$$

$$\text{lcm}(n, m) = \prod p_i^{\max\{l_i, s_i\}} \prod q_i^{a_i} \prod c_i^{d_i}$$

Pf - Let $\underbrace{n|d}_{p_i|d \text{ & } q_i|d}$ & $\underbrace{m|d}_{p_i|d \text{ & } c_i|d}$

$$\text{So, } d = e \cdot \prod p_i^{\alpha_i} \prod q_i^{\beta_i} \prod c_i^{\gamma_i}$$

where e is s.t its prime factors are diff. from p_i, q_i, c_i 's.

$$n|d \Rightarrow \alpha_i \geq l_i \text{ & } \beta_i \geq a_i$$

$$m|d \Rightarrow \alpha_i \geq s_i \text{ & } \gamma_i \geq d_i$$

$$\Rightarrow \alpha_i \geq \max\{l_i, s_i\}$$

$$\Rightarrow \prod p_i^{\max\{l_i, s_i\}} \prod q_i^{a_i} \prod c_i^{d_i} | d$$

$$\therefore \prod p_i^{\max\{l_i, s_i\}} \prod q_i^{a_i} \prod c_i^{d_i} \text{ is lcm}(n, m).$$

$$\text{Hence, } \text{lcm}(n, m) | d$$

L: If $\gcd(n, m) = 1$, then $\text{lcm}(n, m) = mn$.

Pf - $\ell_i = \delta_i = 0$

$$\Rightarrow \text{lcm}(n, m) = \prod q_i^{a_i} \prod c_i^{d_i}$$

Ex 4 Let p_i be the prime factors of either m or n

$$m = \prod_i p_i^{\alpha_i} \quad n = \prod_i p_i^{\beta_i}$$

$$\alpha_i, \beta_i \geq 0$$

Consider $m' = \prod_{i: \alpha_i \geq \beta_i} p_i^{\alpha_i}$ & $n' = \prod_{i: \beta_i > \alpha_i} p_i^{\beta_i}$

Note that $m'|m$ & $n'|n$ & $\gcd(m, n) = 1$

Also, $\text{lcm}(m, n) = m'n'$

Consider $a' = a^{m|m|} & b' = b^{n|n|}$

Clearly $O(a') = m'$ & $O(b') = n'$

Hence, we have reduced the question to the previous one & it follows that $O(a'b') = \text{lcm}(m, n)$.

Ch 3 : Homomorphism

Gp H³Sm - let G & H be gps.

$$f : G \rightarrow H \quad s.t$$

$$f(xy) = f(x)f(y) \quad \forall x, y \in G$$

Note : Multiplication b/w x & y is that of G while that b/w $f(x)$ & $f(y)$ is that of H .

L: $f(e_G) = e_H$

Pf: $e_G \cdot e_G = e_G \Rightarrow f(e_G \cdot e_G) = f(e_G)$
 $\Rightarrow f(e_G)f(e_G) = f(e_G)$

$$\therefore h = f(e_G) \in H \Rightarrow \exists h^{-1} \in H$$

$$h^2 = h$$

$$h^2 h^{-1} = h h^{-1}$$

$h = e_H$

Hence, $f(e_G) = e_H$

- Kernel :

$$\text{ker}(f) = \{ g \in G \mid f(g) = e_H \}$$

L: $\text{ker}(f)$ is a sg. of G

Pf : O. $f(e_G) = e_H$

$$\Rightarrow e_G \in \text{ker}(f)$$

I. Consider $a, b \in \text{ker}(f)$

$$\Rightarrow f(a) = e_H \quad \& \quad f(b) = e_H$$

$$\begin{aligned} \Rightarrow f(ab) &= f(a)f(b) \\ &= e_H \cdot e_H \\ &= e_H \end{aligned}$$

$$\Rightarrow f(ab) \in \text{ker}(f)$$

2. Consider $a \in \text{ker}(f)$

$$\Rightarrow f(a) = e_H$$

$$aa^{-1} = e_G \Rightarrow f(aa^{-1}) = f(e_G) \Rightarrow f(a)f(a^{-1}) = e_H$$

$$\begin{aligned}\Rightarrow & e_H f(a^{-1}) = e_H \\ \Rightarrow & f(a^{-1}) = e_H \\ \Rightarrow & a^{-1} \in \text{Ker}(f)\end{aligned}$$

L: $f(g)^{-1} = f(g^{-1})$

Pf: $g \cdot g^{-1} = e_Q \Rightarrow f(g \cdot g^{-1}) = f(e_Q)$
 $\Rightarrow f(g) \cdot f(g^{-1}) = e_H$
 $\Rightarrow f(g)^{-1} f(g) f(g^{-1}) = f(g)^{-1} \cdot e_H$
 $\Rightarrow \underline{f(g^{-1}) = f(g)^{-1}}$

We'll drop the subscript for identity now.

L: $f: G \rightarrow G'$ be a gp. h'mn.

Let $H \subseteq G'$.

Then the set

$$f^{-1}(H) = \{x \in G \mid f(x) \in H\} \subseteq G$$

Pf - Consider $x, y \in f^{-1}(H)$

1. We need to show that $xy \in f^{-1}(H)$

$$x, y \in f^{-1}(H) \Rightarrow f(x), f(y) \in H$$

$$\Rightarrow f(xy) \in H$$

$$\Rightarrow xy \in f^{-1}(H)$$

2. $x \in f^{-1}(H) \Rightarrow f(x) \in H$

$$\Rightarrow f(x)^{-1} \in H$$

$$\Rightarrow f(x^{-1}) \in H$$

$$\Rightarrow x^{-1} \in f^{-1}(H)$$

□

L: Let $K = \text{ker}(f)$. Then $gK = Kg$

Pf - we will show that $gKg^{-1} \subset K$

Consider $k \in K$.

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g^{-1}) = e$$

$$\Rightarrow gkg^{-1} \in K$$

$$\therefore gKg^{-1} \subset K$$

$$gkg^{-1} = k_1, \quad k_1 \in K$$

$$\Rightarrow gk = k_1g \Rightarrow gk \in Kg$$

$$\therefore gK \subset Kg$$

since, $gKg^{-1} \subset K$ holds $\forall g \in G$
it also holds for g^{-1} .

$$\therefore g^{-1}Kg \subset K$$

By similar argument, we can show
that $Kg \subset gK$

$$\therefore gK = Kg$$

L: If $K \leq G$ s.t $gK = Kg \quad \forall g \in G$,
then $\exists f: G \rightarrow G$ gp h.s.m s.t
 $K = \text{ker}(f)$

Pf — Let $P(G)$ be the power set of G .

Let $C \subseteq P(G)$ be the collection of
right cosets of K .

$$C = \{Kg \mid g \in G\}$$

$$\text{Aut}(C) = \{ \theta: C \rightarrow C \mid \theta \text{ is a bijection}\}$$

We will define a map of sets

$$\varphi: G \rightarrow \text{Aut}(C)$$

$$\varphi(x) = \tilde{l}_x$$

Recall the map $l_x: G \rightarrow G$, $l_x(y) = xy$

Claim: $l_x(kg) = kxg$

$$l_x(kg) = xkg$$

Consider $xkg \in l_x(kg)$

$$xkg = k'ng \in Kng \Rightarrow xkg \subset Kng$$

Similarly, we can show $Kng \subset xkg$

$$\text{Hence, } xkg = Kng \Rightarrow l_x(kg) = Kng$$

$\ell_n: G \rightarrow G$ defines a map

$$\tilde{\ell}_n: P(G) \rightarrow P(G)$$

$$\tilde{\ell}_n(S) = \ell_n(S)$$

our claim shows that $\tilde{\ell}_n(S)$ preserves

$$\begin{array}{ccc} P(G) & \xrightarrow{\tilde{\ell}_n} & P(G) \\ \cup & & \cup \\ C & \xrightarrow{\tilde{\ell}_n} & C \end{array}$$

It is clear that $\tilde{\ell}_n$ is a bijection
as its inverse is $\tilde{\ell}_n^{-1}$.

$$\begin{aligned} \tilde{\ell}_n^{-1}(\tilde{\ell}_n(S)) &= \tilde{\ell}_n^{-1}(\ell_n(S)) = \ell_n^{-1}(\ell_n(S)) \\ &= n^{-1}n S = S \end{aligned}$$

So, indeed $\tilde{\ell}_n: C \rightarrow C$ is a bijection
& hence $\tilde{\ell}_n \in \text{Aut}(C)$

we need to check that

$$\varphi(xy) = \varphi(x)\varphi(y)$$

iff

$$\tilde{\iota}_{xy} = \tilde{\iota}_x \circ \tilde{\iota}_y$$

If $s \in G$, then

$$\begin{aligned}\tilde{\iota}_x \circ \tilde{\iota}_y(s) &= \tilde{\iota}_x(\tilde{\iota}_y(s)) = \tilde{\iota}_x(y s) = xy s \\ &= \tilde{\iota}_{xy}(s)\end{aligned}$$

Hence, φ is a gp. hom

What is $\text{Ker}(\varphi)$?

$$\text{Ker}(\varphi) = \{ x \in G \mid \tilde{\iota}_x = \text{Id}_C \}$$

$$\tilde{\iota}_x = \text{Id}_C \Leftrightarrow \forall g \in G, \text{ we have}$$

$$\tilde{\iota}_x(kg) = \text{Id}_C(kg) = kg$$

1. $K \subset \text{Ker}(\varphi)$

$$k \in K, \quad \tilde{\iota}_k(kg) = \iota_k(kg) = Kkg = kg$$

2. $\text{Ker}(\varphi) \subset K$

Suppose $\tilde{\ell}_n = gdc$, then

$$\tilde{\ell}_n(K) = K$$

$$\Rightarrow \ell_n(K) = K$$

$$\Rightarrow nK = K$$

$$\Rightarrow x \in K$$

$$\Rightarrow \text{Ker}(\varphi) = K$$

- Normal sg : $H \leq G$ s.t $gHg^{-1} \in H \quad \forall g \in G$
 $(gH = Hg \quad \forall g \in G)$

P: Sg is normal \Leftrightarrow It is kernel of
a gp hom

L: $f: G \rightarrow H$ gp. h'sm

Then the subset $f(G) \subseteq H$

Pf : $f(x), f(y) \in f(G)$

$$\Rightarrow f(x)f(y) = f(xy) \in f(G)$$

$$f^{-1}(x) = f(x^{-1}) \in f(G)$$

Given any two gps. $G \& H$, we
always have at least 1 gp. h'sm

$f_{\text{trivial}} : G \rightarrow H$

$$f_{\text{trivial}}(g) = e \quad \forall g \in G$$

Note - $\#f(G) \# \text{ker}(f) = \# G$

&

$$\# f(G) \mid \# H$$

If $\# G$ & $\# H$ are coprime, then $\# f(G) = 1$
or $f = f_{\text{trivial}}$

Hence, there does not always exist
a non-t'vl gp. h'sm