Group Theory

Thm 1.4.7

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

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

$$X = \{a_1, a_2, \ldots, a_r\} \amalg \{b_1, b_2, \ldots, b_s\} \amalg \{\text{the rest}\}$$

C1 — $a \in \{a_1, \ldots, a_r\}$ say a_i

$$\left.\begin{aligned} \alpha(a_i) &= a_{i+1} \\ \beta(\alpha(a)) &= \beta(a_{i+1}) = a_{i+1} \\ \\ \beta(a_i) &= a_i \\ \alpha(\beta(a_i)) &= \alpha(a_i) = a_{i+1} \end{aligned}\right\} \begin{aligned} &\alpha\beta(a) \\ &= \beta\alpha(a) \end{aligned}$$

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

(2) $X = \{a_1, \ldots, a_r\} \amalg X \setminus \{a_1, \ldots, a_r\}$

<u>C1</u> – $a \in \{a_1, \ldots, a_r\}$ say a_i

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

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

<u>1.2</u> $a = a_r$

$\alpha(a_r) = a_1$

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

<u>C2</u> – $a \in X \setminus \{a_1, \ldots, a_r\}$

$\alpha(a) = a$

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

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

<u>3.1</u> $a = a_i$ (say) $(1 < i \leqslant r)$

$$(a_1 \dots a_r)(a_r \dots a_1)(a_i) = (a_1 \dots a_r)(a_{i-1})$$
$$= a_i = Id_X(a_i)$$

If $a = a_i$,

$$(a_1 \dots a_r)(a_r \dots a_1)(a_1) = (a_1 \dots a_r)(a_r)$$
$$= a_1 = Id_X(a_1)$$

<u>3.2</u> $(a_1 \dots a_r)(a_r \dots a_1)(a) = a = Id_X(a)$

1. Not every elem of G has finite

eg – $(\mathbb{Z}, +, 0)$

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

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

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

PT $(a_1, a_2 \ldots, a_r)$ has order r.

Pf – $\sigma = (a_1, \ldots, a_r)$

we need to show

1. $\sigma^r = e$
2. $0 < i < r, \quad \sigma^i \neq e$

Ppn : $\sigma^i(\alpha_i) = \alpha_{\overline{j+i}}$,

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

Pf - BC : $\sigma(\alpha) = \alpha_{\overline{j+1}}$

IH : $\sigma^{i+1}(\alpha_j) = \sigma(\alpha_{\overline{j+i}})$

$= \alpha_{\overline{j+i+1}}$

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

1. So, for $i = r$, $\sigma^r(\alpha_j) = \alpha_{\overline{r+j}}$

$= \alpha_j \quad \forall j$

$\underline{\sigma^r = e}$

2. If $0 < i < r$, $\sigma^i(\alpha_1) = \alpha_{\overline{i+1}} \neq \alpha_1$

$1 < i+1 < r+1$

$\Rightarrow 1 < i+1 \leq r$

Ex 1.5.2

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

Pf

$\forall\ \sigma \in S_n$, $\exists\ \sigma_1, \ldots, \sigma_p \in S_n$

s.t

$\sigma = \sigma_1 \sigma_2 \ldots \sigma_p$ s.t σ_i s are disjoint cycles

Let $\sigma_i = (\alpha_{i1}, \alpha_{i2} \ldots, \alpha_{ij_i})$

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

By thm, $\forall\ \sigma_i$

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

$\therefore\ \sigma = (\alpha_{11}, \alpha_{12}) \ldots (\alpha_{1(j_1-1)}, \alpha_{1j_1})(\alpha_{21}, \alpha_{22}) \ldots$

$\ldots (\alpha_{p(j_p-1)}, \alpha_{pj_p})$

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

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

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

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

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

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

$\alpha \in \{1, i, j\}$ $\rightarrow$ $\alpha = 1$ ✓
$\rightarrow$ $\alpha = i$ ✓
$\rightarrow$ $\alpha = j$ ✓

$\square$

(2) Show that $Y = \{(12), (23) \ldots\}$ 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 $(1, 2, \ldots, n)$ & (12) generate S_n

Pf Let $(1, 2, \ldots, n)$ & (12) generate $(k-1 \; k)$

BC :

IH : $(1, 2, \ldots, n)(k-1 \; k)\overbrace{(1, 2, \ldots, n)^{-1}}^{(1, 2, \ldots, n)^{(n-1)}} = (k \; k+1)$

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

Ex 1.5.1

$$\beta = (a_1, \ldots, a_r), \quad \gamma \in S_n$$

PT $\gamma\beta\gamma^{-1} = (\gamma(a_1), \ldots, \gamma(a_r))$

Pf - $\beta(a_i) = a_{i+1}, \quad i \leq r$
$\beta(x) = x$ if $x \neq a_i \ \forall\, i \leq r$

We need to show

$$\gamma\beta\gamma^{-1}(\gamma(a_i)) = \gamma(a_{i+1})$$
$\gamma\beta\gamma^{-1}(x) = x$ if $x \neq \gamma(a_i)$ for any $i \leq r$

1. $(\gamma\beta\gamma^{-1})(\gamma(a_i)) = \gamma\beta(\underbrace{\gamma^{-1}\gamma}_{e})(a_i) = \gamma\beta(a_i)$
$= \gamma(a_{i+1})$

2.
If $x \neq \gamma(a_i)$ for any $i \leq r$
$\Rightarrow \gamma^{-1}(x) \neq \gamma^{-1}\gamma(a_i) = a_i$ ($\because \gamma$ is an injection)

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

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

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

$(b_{11}, b_{12} \cdots b_{1n_1})$ $\quad$ $(b_{l1}, b_{l2}, \cdots, b_{ln_l})$

$$\begin{aligned}
\gamma \beta \gamma^{-1} &= \gamma \beta_1 \beta_2 \cdots \beta_l \gamma^{-1} \\
&= \gamma \beta_1 \gamma^{-1} \gamma \beta_2 \cdots \gamma \beta_l \gamma^{-1} \\
&= (\gamma \beta_1 \gamma^{-1})(\gamma \beta_2 \gamma^{-1}) \cdots (\gamma \beta_l \gamma^{-1})
\end{aligned}$$

$(\gamma(b_{11}), \gamma(b_{12}), \cdots, \gamma(b_{1n_1}))$ $\quad$ $(\gamma(b_{l1}), \cdots, \gamma(b_{ln_l}))$

Ch 2 : SubGps

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

1. $\forall\, a, b \in H, \quad a \cdot b \in H$
2. $a \in H \Rightarrow a^{-1} \in H$

Then H is a group.

Pf 1. H is a non-empty set

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

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

$\Rightarrow e \in H$

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

$m_H : H \times H \longrightarrow G$

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

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

So, $m_H : H \times H \longrightarrow H$

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

Associativity follows from def^n 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.
(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. $m \mid n \Rightarrow m\mathbb{Z} \subset n\mathbb{Z}$ subgp.

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

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

Pf

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

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

3. $$\left.\begin{aligned} e^{-1} &= e \\ (13)^{-1} &= (13) \\ (24)^{-1} &= (24) \\ ((13)(24))^{-1} &= (13)(24) \end{aligned}\right\} \in H$$

$\therefore\; H \subseteq S_4$ is a subgp.

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

$\because\; (13)(14) \notin H$

Ex - $Y \subseteq X$

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

Show that $\mathrm{Aut}(X, Y)$ is a subgp. of $\mathrm{Aut}(X)$

Pf 1. $Id_X(Y) = Y$

$\because$ $Id_X \in \mathrm{Aut}(X, Y)$

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

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

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

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

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

$$\varphi(Y) = Y \Rightarrow (\varphi^{-1} \circ \varphi)(Y) = \varphi^{-1}(Y)$$
$$\Rightarrow Y = \varphi^{-1}(Y)$$

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

$\because \quad \varphi \circ \varphi^{-1} = Id_X = \varphi^{-1} \circ \varphi$

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

Hence, $Aut(X, Y)$ is a subgp.

eg – $X = \{1, 2, 3, 4\}$, $Y = \{1, 3\}$

find $Aut(X, Y)$

$$Aut(X, Y) = \{\underbrace{e, (24)}, \underbrace{(13), (13)(24)}\}$$

$1 \to 1$ $\quad$ $1 \to 3$

$3 \to 3$ $\quad$ $3 \to 1$

Note – 1. If $Y_1 \subseteq Y_2 \subseteq X$,

then $Aut(X, Y_1) \subseteq Aut(X, Y_2) \subseteq Aut(X)$

2. If X is finite,

$$Aut(X, Y) = Aut(X, X - Y)$$

Let $S \subseteq G$ be a subset.

<u>Centralizer of S in G</u>

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

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

<u>0</u>. $e \in C_G(S)$ $\because$ $e \cdot x = x \cdot e$ $\forall x \in S$

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

<u>1</u>. $a, b \in C_G(S)$ $\Rightarrow$ $ax = xa$ $\forall x \in S$

$bx = xb$

$$(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$$

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

<u>2</u>. $a \in C_G(S)$ $\Rightarrow$ $ax = xa$ $\forall x \in S$

$\Rightarrow$ $a^{-1}axa^{-1} = a^{-1}xaa^{-1}$

$\Rightarrow$ $xa^{-1} = a^{-1}x$

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

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

eg - 1. $G = S_3$, $S = \{(1\,2)\}$

$$C_S(G) = \{ g \in S_3 : g \cdot (1\,2) = (1\,2) g \}$$

g	$g(1\,2)$	$(1\,2)g$	$=?$
e	$(1\,2)$	$(1\,2)$	✓
$(1\,2)$	e	e	✓
$(2\,3)$	$(1\,3)$	$(1\,2\,3)$	✗
$(1\,3)$	.	.	✗
$(1\,2\,3)$	.	.	✗
$(1\,3\,2)$	.	.	✗

2 If $G = S_4$,

$(3\,4) \in C_S(G)$ for $S = \{(1\,2)\}$

└ cycle disjoint with $(1\,2)$

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> — Abelian — Non-abelian

Abelian	Non-abelian
$(\mathbb{Z}, +, 0)$	$S_n \quad (n > 2)$
$(M_n(\mathbb{R}), +, 0)$	$(GL(n, \mathbb{R}), \cdot, Id_n)$

<u>Ex</u> — Let $g \in G$
$H_{\langle g \rangle} = \{ g^i : i \in \mathbb{Z} \}$
Show that $H_{\langle g \rangle}$ is a subgp.

<u>Pf</u> — <u>0</u>. $g = g^1 \Rightarrow g \in H_{\langle g \rangle}$
$\therefore H_{\langle g \rangle} \neq \emptyset$

<u>1</u>. $a, b \in H_{\langle g \rangle}$. $\exists\, i, j$ s.t $a = g^i$ & $b = g^j$
$a \cdot b = g^{(i+j)} \in H_{\langle g \rangle}$

<u>2</u>. $a \in H_{\langle g \rangle}$ $\exists\, i$ s.t $a = g^i$

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

eg – 1. $n \in \mathbb{Z}$, $H_{\langle n \rangle} = \{an : a \in \mathbb{Z}\} = n\mathbb{Z}$

2. S_3

$H_{\langle (12) \rangle} = \{e, (1\,2)\}$

$H_{\langle (123) \rangle} = \{e, (1\,2\,3), (1\,3\,2)\}$

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

Pf – 1. $O(g)$ is infinite

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

$\therefore \exists\ i, j \in \mathbb{Z}$ s.t $i \neq j$ & $g^i = g^j$

$$\Rightarrow g^i g^{-j} = g^j g^{-j}$$

$$\Rightarrow g^{(i-j)} = e$$

$\Rightarrow O(g)$ is finite.

which is a contd^n.

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, $\exists\, k, r \in \mathbb{Z}$
s.t $a = km + r$, $0 \leq r < m$

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

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

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

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

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

Pf – Let $O(a) = k \Rightarrow ka \equiv 0 \pmod{n}$

$\because \gcd(a, n) = 1$, $\therefore k \equiv 0 \pmod{n}$

$\Rightarrow k = n$

Hence, $O(a) = n$

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

Given a gp. G & a sg. $H \subset G$.
We want to define an eq. rel^n on G.

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

Checking ER

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

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. rel^n.

This eq. rel^n breaks G into disjoint eq. classes.

What are the eq. classses?

<u>Pp^n</u> : For any $g \in G$, the eq. class of g is precisely the set

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

ie $x \in G$ s.t $x \sim g \iff x \in Hg$

<u>Pf</u> – ① <u>$EC(g) \subset Hg$</u>

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

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

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

$\implies x = hg$

$\implies x \in Hg$

$\therefore EC(g) \subset Hg$

② $\underline{Hg \subset EC(g)}$

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, $EC(g) = Hg$.

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

$$R_g : G \to G$$
$$x \mapsto xg$$

Claim : R_g is a bijection.

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

$$R_g \circ R_{g^{-1}} = Id_G = R_{g^{-1}} \circ R_g$$

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

$$R_{g^{-1}} \circ R_g(x) = R_{g^{-1}}(xg) = xgg^{-1} = x$$

$\Rightarrow$ R_g is a bijection.

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

Clearly, $Hg = R_g(H)$

A bijective map preserves 'size' of sets.

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

$$\therefore \quad \underset{\underset{\#H}{=}}{\#R_g(H)} = \#Hg$$

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

Since,

$$G = EC(g_1) \amalg EC(g_2) \dots \amalg EC(g_l)$$
$$= Hg_1 \amalg Hg_2 \dots \amalg Hg_l$$

$$\#G = (\#H)\, l$$
$$\Rightarrow \#H \mid \#G$$

$\square$

(Lagrange's Thm)

Structure of Pf

1. Put eq. relⁿ on G
2. Checked that eq. classes are of the form $EC(x) = Hx$
3. Showed $R_g : G \to G$, $R_g(x) = xg$ is a bijection $\Rightarrow$ $\#(Hg) = \#H$

$\Rightarrow$ $\#G = \#H$ (# eq. classes)

L: $\#G = p$ (prime). 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, $\# \langle g \rangle \mid \#G = p$

$\Rightarrow$ $\# \langle g \rangle = \cancel{1}, p$ $\because g \neq e$

$\Rightarrow$ $\# \langle g \rangle = p = \#G$

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

$\square$

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

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

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

$$\left\{ \because O(g) = \underbrace{\#\langle g \rangle \mid \#G}_{LT} \right\}$$

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

No!

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

If yes, let g be such elem.

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

But, $\langle g\rangle$ is Abelian, while G may <u>not</u> be Abelian

<u>eg</u> – S_3

Now, consider $d \mid \#G$ & $d < \#G$.
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,

Assoc
$$(g_1, g_2)\cdot\left((g_1', g_2')\cdot(g_1'', g_2'')\right)$$
$$= \left((g_1, g_2)\cdot(g_1', g_2')\right)\cdot(g_1'', g_2'')$$

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 $H \subset \mathbb{Z}$, the $\exists\, n$ s.t $H = \langle n \rangle$

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 (+ve)

$\therefore$ H contains a (+ve) integer

Consider the smallest (+ve) int $n_0 \in H$

Claim $H = \langle n_0 \rangle$

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

Consider $h \in H$.

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

If $r = 0$, $h = qn_0 \Rightarrow h \in \langle n_0 \rangle$

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

& $0 < r < n_0$

which is a contd^n since we assumed n_0 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 $m | n$.

Then $g^{n/m}$ has order m.

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

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

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

$g^{nk/m} = e$

But, $\frac{nk}{m} < n$ which is a contd^n

$\because\ O(g) = n$

Ex 3:

Pf - $H_a = \{e, a, \ldots, a^{n-1}\}$
$H_b = \{e, b, \ldots, b^{m-1}\}$

Consider $g \in H_a \cap H_b$

$\because g \in H_a \quad \therefore O(g) \mid \# H_a \Rightarrow O(g) \mid n$

$\because g \in H_b \quad \therefore O(g) \mid \# H_b \Rightarrow O(g) \mid m$

coprime

$\Rightarrow O(g) = 1$

$\Rightarrow \underline{g = e}$

Ex 4:

1. $(ab)^{mn} = a^{mn} b^{mn}$ ($\because G$ is abelian)

$= (a^m)^n (b^n)^m$

$= e$

Let $O(ab) = k$, $(ab)^k = e$

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

Then $\quad g \in H_a \cap H_b$

$\Rightarrow \quad g = e$

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

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

$\Rightarrow \quad m \mid k \qquad \Rightarrow n \mid k$

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

To prove k is smallest,

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

$$\left\{ \begin{array}{l} \underline{L}: \quad O(g) = n \quad \& \quad g^m = e \quad \Rightarrow \quad n \mid m \\ \underline{Pf} - \quad m = nq + r \quad \Rightarrow \quad g^r = e \\ \qquad\quad 0 \leq r < n \qquad\qquad \underline{\quad} \\ \qquad\qquad\qquad\qquad\qquad \text{contd}^n \end{array} \right\}$$

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

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
$l_i, s_i, a_i, d_i > 0$

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

Pf – Let $d|n$ & $d|m$.
Consider a prime p s.t $p|d$
$\Rightarrow p = p_i$, $1 \leq i \leq r$

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

$$\left.\begin{array}{l} d|n \Rightarrow \alpha_i \leq l_i \\ d|m \Rightarrow \alpha_i \leq s_i \end{array}\right\} \Rightarrow \alpha_i \leq \min\{l_i, s_i\} \quad \forall i$$

$$\Rightarrow d \mid \prod p_i^{\min\{l_i, s_i\}}$$

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

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

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.

$n \mid d \Rightarrow \alpha_i \geq l_i$ & $\beta_i \geq a_i$

$m \mid d \Rightarrow \alpha_i \geq s_i$ & $\gamma_i \geq d_i$

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

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

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

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

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

Pf - $l_i = \delta_i = 0$

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

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

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

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

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 H'sm — Let G & H be gps.

$$f : G \to H \quad \text{s.t}$$
$$f(xy) = f(x)f(y) \quad \forall\, x, y \in G$$

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

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

$\therefore h^2 = h$

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

$\underline{h = e_H}$

Hence, $f(e_G) = e_H$

- <u>Kernel</u> :

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

<u>L</u>: $\ker(f)$ is a sg. of G

<u>Pf</u> : <u>0.</u> $f(e_G) = e_H$

$\Rightarrow e_G \in \ker(f)$

<u>1.</u> Consider $a, b \in \ker(f)$

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

$\Rightarrow f(ab) = f(a) f(b)$

$= e_H \cdot e_H$

$= e_H$

$\Rightarrow f(ab) \in \ker(f)$

<u>2.</u> Consider $a \in \ker(f)$

$\Rightarrow f(a) = e_H$

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

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

$$\Rightarrow \quad e_H\, f(a^{-1}) = e_H$$
$$\Rightarrow \quad f(a^{-1}) = e_H$$
$$\Rightarrow \quad a^{-1} \in \ker(f)$$

<u>L</u>: $\quad f(g)^{-1} = f(g^{-1})$

~~Pf~~: $\quad g \cdot g^{-1} = e_G \quad \Rightarrow \quad f(g \cdot g^{-1}) = f(e_G)$

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

We'll drop the subscript for identity now.

L: $f : G \to G'$ be a gp. h'sm.

Let $H \leqslant G'$.

Then the set

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

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

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

$\square$

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

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

Consider $k \in K$.

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

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

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

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

$\Rightarrow gk = k_1 g \Rightarrow gk \in Kg$

$\therefore gK \subset Kg$

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 $Kg \subset gK$

$\therefore \; gK = Kg$

<u>L</u>: If $K \leq G$ s.t $gK = Kg \;\; \forall g \in G$, then $\exists f : G \to G$ gp h'sm s.t $K = \ker(f)$

<u>Pf</u> — Let $P(G)$ be the power set of G.

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

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

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

We will define a map of sets

$$\varphi : G \to Aut(C)$$

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

Recall the map $L_x : G \to G$, $L_x(y) = xy$

<u>Claim</u> : $L_x(Kg) = Kxg$

$$L_x(Kg) = xKg$$

Consider $xkg \in L_x(Kg)$

$xkg = k'xg \in Kxg \Rightarrow xKg \subset Kxg$

Similarly, we can show $Kxg \subset xKg$

Hence, $xKg = Kxg \Rightarrow L_x(Kg) = Kxg$

$l_x : G \to G$ defines a map

$\tilde{l}_x : P(G) \to P(G)$

$\tilde{l}_x(S) = l_x(S)$

Our claim shows that $\tilde{l}_x(S)$ preserves

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

It is clear that $\tilde{l}_x$ is a bijection as its inverse is $\tilde{l}_{x^{-1}}$.

$$\tilde{l}_{x^{-1}}(\tilde{l}_x(S)) = \tilde{l}_{x^{-1}}(l_x(S)) = l_{x^{-1}}(l_x(S))$$
$$= x^{-1}x S = S$$

So, indeed $\tilde{l}_x : C \to C$ is a bijection & hence $\tilde{l}_x \in Aut(C)$

We need to check that

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

$$\Updownarrow$$

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

If $S \subset G$, then

$$\tilde{\iota}_x \circ \tilde{\iota}_y(S) = \tilde{\iota}_x(\tilde{\iota}_y(S)) = \tilde{\iota}_x(yS) = xyS$$

$$= \tilde{\iota}_{xy}(S)$$

Hence, φ is a gp. h'sm

What is $\ker(\varphi)$?

$$\ker(\varphi) = \{ x \in G \mid \tilde{\iota}_x = Id_C \}$$

$\tilde{\iota}_x = Id_C \iff \forall g \in G$, we have

$$\tilde{\iota}_x(Kg) = Id_C(Kg) = Kg$$

1. $K \subset \ker(\varphi)$

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

2. $\ker(\varphi) \subset K$

Suppose $\tilde{i}_x = Id_C$, then

$\tilde{i}_x(K) = K$

$\Rightarrow \quad i_x(K) = K$

$\Rightarrow \quad xK = K$

$\Rightarrow \quad x \in K$

$\Rightarrow \quad \ker(\varphi) = K$

- 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 h'sm

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

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

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

$f_{trivial} : G \to H$

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

<u>Note</u> - $\#f(G)\,\#\ker(f) = \#G$

&

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

If $\#G$ & $\#H$ are coprime, then $\#f(G) = 1$

or $f = f_{\text{trivial}}$

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