GROUP HOMOMORPHISM

$f : (G, \circ) \longrightarrow (H, *)$ is group homomorphism

if $\forall a, b \in G$ $\quad f(a \circ b) = f(a) * f(b)$

Ex: $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_4, +)$

is an homomorphism

$$f(x) = [x] = \{x + 4k \mid k \in \mathbb{Z}\}$$

$$f(x+y) = [x+y] = [x] + [y] = f(x) + f(y)$$

(Homomorphism in general) $g : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +)$ $\quad [n \in \mathbb{Z}^+]$

Properties: $f:(G,\circ) \to (H,*)$

$e_H \leftarrow id(H)$

$e_G \leftarrow id(G)$

① $e_H = f(e_G)$

$e_H * f(e_G) = f(e_G) = f(e_G) * f(e_G)$

② $f(a^{-1}) = [f(a)]^{-1}$

$$\left.\begin{aligned} f(a) * f(a^{-1}) &= f(a \circ a^{-1}) = f(e_G) = e_H \\ f(a^{-1}) * f(a) &= f(e_G) = e_H \end{aligned}\right\}$$

③ $f(a^n) = [f(a)]^n$

$[n \in \mathbb{Z}]$

$f(a^{n+1}) = f(a^n \circ a)$

$= f(a^n) * f(a) = [f(a)]^n * f(a)$

$= [f(a)]^{n+1}$

④ $\forall$ subgroups S of G, $f(S)$ is a subgroup of H.

$\forall a, b \in S \qquad x = f(a) \in f(S)$

$y = f(b) \in f(S)$

(i) $x * y = f(a) * f(b) = f(a \circ b) \in f(S)$

↳ Closure Property

(ii) $f(a^{-1}) = [f(a)]^{-1} \in f(S)$

↳ Existance of Inverse

$\therefore f(S)$ is a subgroup of H. ✓

GROUP ISOMORPHISM

$f : (G, \circ) \to (H, *)$ is a homomorphism and f is bijective (one-to-one + onto)

Ex: $G = \{1, -1, i, -i\}$ under $*$ (mult.)

$H = (\mathbb{Z}_4, +)$

$f : (G, *) \to (\mathbb{Z}_4, +)$ such that
$$\begin{cases} f(1) = [0] \\ f(-1) = [2] \\ f(i) = [1] \\ f(-i) = [3] \end{cases}$$

bijective

f isomorphism

$f(1 * -1) = f(-1) = [2] = [0] + [2]$
$= f(1) + f(-1)$

$f(i * -i) = f(1) = [0] = [1] + [3] = f(i) + f(-i)$

$G = \{1, -1, i, -i\}$ group under $*$

Generated by $\langle i \rangle$ or $\langle -i \rangle$

CYCLIC GROUPS

$\exists\, a \in G$ such that $\forall x \in G \quad x = a^n \quad (n \in \mathbb{Z})$

Ex: ① $H = (\mathbb{Z}_4, +)$ is a cyclic group $\langle [3] \rangle, \langle [1] \rangle$

$[3]^1 = [3], \quad [3]^2 = [2], \quad [3]^3 = [1], \quad [3^4] = [0]$

② $(\mathbb{Z}_9, +, *)$ Ring $\quad (U_9, *)$ cyclic group

$$\left.\begin{array}{lll} [2]^1 = [2], & [2]^2 = [4], & [2]^3 = [8] \\ [2]^4 = [7], & [2]^5 = [5], & [2]^6 = [1] \end{array}\right\} \text{generator: } \langle [2] \rangle, \langle [5] \rangle$$

$U_9 = \{[1], [2], [4], [5], [7], [8]\}$

Ex: $U_9 = \langle [2] \rangle, \langle [5] \rangle$

$\langle [4] \rangle = \{[1], [4], [7]\}$

$\langle [1] \rangle = \{[1]\}$

$\langle [8] \rangle = \{[1], [8]\}$

$\rightarrow$ SUBGROUPS generated by $\langle x \rangle$ in $(G, \circ)$

Ex: $G = \{1, -1, i, -i\}$ group/cyclic with $*$

$G = \langle i \rangle = \langle -i \rangle$

$\langle -1 \rangle = \{1, -1\}$

$\langle 1 \rangle = \{1\}$

▷ ORDER of cyclic Groups:

$o(G) = |\langle a \rangle|$ → finite → infinite

$|\langle a\rangle| =$ finite.

① $a^1 = e = a^0$ $\qquad |\langle a\rangle| = 1$

② When $a \neq e$ $\qquad \langle a\rangle = \{a, a^2, \dots, a^k\}$

$a^t = a^s \quad 1 \leq s < t$ $\qquad = \{a^m \mid m \in \mathbb{Z}\}$

$\Rightarrow a^{t-s} = e$ $\qquad$ Let, smallest n such that $a^n = e$

(i) $\langle a\rangle = \{a, a^2, a^3, \dots, a^n (= e)\}$ $\qquad |\langle a\rangle| \geq n$

otherwise $a^u = a^v \ (1 \leq u < v \leq n) \Rightarrow a^{v-u} = e$

$[v-u < n]$

CONTRADICTS n is minimal.

(ii) If $|\langle a\rangle| > n$ $\qquad k = qn + r \quad (0 \leq r < n)$

$a^k = a^{qn+r} = (a^n)^q \cdot a^r = a^r$ where $r < n$

Order of cyclic groups: $o(\langle a\rangle) = |\langle a\rangle| = n$ when $a^n = e$ (smallest n)

▨ $\langle a \rangle$ is cyclic group with $o(\langle a \rangle) = n$.
If $k \in \mathbb{Z}$ such that $a^k = e$ then $n \mid k$

Proof: $k = qn + r \quad (0 \le r < n)$

$$a^k = a^{qn+r} = (a^n)^q . a^r = e^q . a^r$$
$$= e . a^r = a^r$$

(because $r < n$)
if $a^k = e = a^r$

CONTRADICT the MINIMALITY of n

So, $r = 0 \Rightarrow k = qn \Rightarrow n \mid k$ ✓

Cyclic Group with Homomorphisms

Ex: $f : (U_9, *) \to (\mathbb{Z}_6, +)$ where $f(2^i) = [i]$

$U_9 = \langle [2] \rangle = \langle [5] \rangle$

$f(2^1) = [1] = f([2])$

$f(2^2) = [2] = f([4])$

$f(2^3) = [3] = f([8])$

$f(2^4) = [4] = f([7])$

$f(2^5) = [5] = f([5])$

$f(2^6) = [6] = f([1])$

$$f(2^m * 2^n) = f(2^{m+n})$$
$$= [m+n] = [m] + [n]$$
$$= f(2^m) + f(2^n)$$

Homomorphism ✓

Isomorphism ✓

Verify : $\langle [5] \rangle$ $\quad f(5^1) = [1]$

- - - - - so on

Theorem: G is Cyclic Group

① $|G| =$ infinite, then $f:(G,\circ) \to (\mathbb{Z},+)$

② $|G| =$ finite $= n > 1$, then $f:(G,\circ) \to (\mathbb{Z}_n,+)$

Here, f as an **ISOMORPHISM** ✓

Proof: ① $f(a^k) = k \in \mathbb{Z}$

② $f(a^k) = [k] \in \mathbb{Z}_n$

$\Big\}$ one-to-one & Onto

Homomorphism with

- Every cyclic Group is Abelian

Proof: $G = \langle a \rangle$ under $*$

$$a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m$$

↳ Commutative Property

- Is every Abelian Group Cyclic ??

$\boxed{\text{NO}}$

$H = \{e, a, b, c\}$

$a \circ b = c = b \circ a$

$o(\langle e \rangle) = 1 \quad o(\langle a \rangle) = o(\langle b \rangle) = o(\langle c \rangle) = 2$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

KLEIN'S GROUP of ORDER = 4

Theorem: Every Subgroup of cyclic group is also cyclic

Proof: H is a subgroup of $G = \langle a \rangle$

$a^t \in H$ where t ~~is~~ minimum

Claim: $H = \langle a^t \rangle$ $\qquad \langle a^t \rangle \subseteq H$

$\boxed{\text{H is also cyclic}}$

$\langle a^t \rangle^i \neq b = a^s \in H \qquad a^s = a^{qt+r} \qquad (0 \leq r < t)$

$(s > t \geq 1)$

$$\Rightarrow a^r = (a^t)^{-q} \cdot a^s = \underbrace{(a^t)^{-q}}_{\in H} \cdot \underbrace{b}_{\in H} \in H$$

$\uparrow r < t$

If $a^r \in H$ where $(r < t)$

CONTRADICTS minimality of t s.t $a^t \in H$

COSETS : H is a subgroup of G (under $*$)

$\forall a \in G$ $aH = \{ah \mid h \in H\}$ ← Left Coset of H in G

$Ha = \{ha \mid h \in H\}$ ← Right Coset of H in G.

(Additive Groups)

$\forall a \in G$ $a + H = \{a + h \mid h \in H\}$ ← Left Coset

$H + a = \{h + a \mid h \in H\}$ ← Right coset

Ex: $G = (\mathbb{Z}_{12}, +)$ $H = \{[0], [4], [8]\}$

$[0] + H = \{[0], [4], [8]\} = [4] + H = [8] + H = H$

$[2] + H = ?$

$[1] + H = \{[1], [5], [9]\} = [5] + H = [9] + H$

$[3] + H = ?$

Partition of $G = H \cup ([1] + H) \cup ([2] + H) \cup ([3] + H)$ ✓

H is subgroup of G (finite)

1. $\forall a \in G \quad |aH| = |H|$
2. $\forall a, b \in G \quad aH \cap bH = \phi$ or $aH = bH$ ✓

Proof: $aH = \{ah \mid h \in H\} \Rightarrow |aH| \leq |H|$

1. $ah_1 = ah_2$ if $|aH| < |H|$
$\Rightarrow h_1 = h_2$ (as $h_1, h_2, a \in G$) $\Big\}$ $|aH| = |H|$

2. $aH \cap bH \neq \phi \Rightarrow c \in aH \cap bH$

$c = ah_1 = bh_2$
$\Rightarrow a = bh_2h_1^{-1}$

$x \in aH \rightarrow x = ah \ (h \in H) = (bh_2h_1^{-1})h$
$= b(h_2h_1^{-1}h) \in bH$
$\Rightarrow aH \subseteq bH$

$y \in bH \rightarrow y = bh = (ah_1h_2^{-1})h = a(h_1h_2^{-1}h) \in aH$
$\Rightarrow bH \subseteq aH$

$b = ah_1h_2^{-1}$

LAGRANGE'S THEOREM :

If G finite group of $o(G) = n$
H is a subgroup of G, $o(H) = m$ $\Big\}$ $m \mid n$ ✓

Proof : $G = H$ ✓ otherwise $G \neq H$
$\Rightarrow a \in G - H$

$a \notin H \Rightarrow aH \neq H$

i.e $aH \cap H = \emptyset \longrightarrow G = aH \cup H$ then $|G| = 2|H|$

otherwise, $b \in G - (aH \cup H)$

$b \notin aH \cup H \Rightarrow bH \neq H$ i.e. $bH \cap H = \emptyset = bH \cap aH$

If $G = aH \cup bH \cup H$ then $|G| = 3|H|$

Otherwise, $c \in G - (aH \cup bH \cup H)$ .... so on ...

$\hookrightarrow G = a_1 H \cup a_2 H \cup \ldots \cup a_k H \Rightarrow |G| = k|H|$

COROLLARY :

① G is finite group and $\forall a \in G$

$$o(\langle a \rangle) \mid o(G) \Rightarrow |\langle a \rangle| \,\Big|\, |G|$$

② Every finite group of Prime Order is Cyclic

Proof: $|G| = p \leftarrow$ prime

Every subgroup $\underset{\text{"e"}}{\underline{1}}$ or $\underset{\text{"G"}}{\underline{p}}$ elements

(Extension from Lagrange's Theorem)