Chapter 4

Homomorphism Group

Def. 4.1: (Homomorphism Group)

Let (G, *) and (G', o) be two groups and ϕ be a mapping from G into G′, then ϕ: G→G′ is said to be homomophism if

$\phi(a*b) = \phi(a) \text{ o } \phi(b)$, for each a, b $\in$ G.

Ex. 4.2: Let (G, *) be a group and ϕ: (G, *)→(G, *) defined by $\phi(x) = x$, then ϕ is homomorphism since

$\phi(x*y) = x*y = \phi(x)*\phi(y)$.

∴ Every identity map from a group G into itself is a homomorphism.

Ex. 4.3: Let H be a normal subgroup of G and $\phi: G \to G/H$ such that $\phi(a) = aH$, where a$\in$G. Is ϕ a homomorphism mapping ?

Solution: $\forall$ a, b $\in$G.

We show that $\phi(a.b) = \phi(a) \otimes \phi(b)$.

Since $\phi(a.b) = a.b.H$

$= (a.H) \otimes (b.H)$

$= \phi(a) \otimes \phi(b)$.

∴ ϕ is homomorphism.

Remark 4.3′: ϕ from **Ex. 4.3** is called the natural map.

Th. 4.4: Let $\phi: G \to G'$ be a group homomorphism and e, e′ the identity elements of G and G′, respectively, then

(1) $\phi(e) = e'$.

(2) $\phi(a^{-1}) = (\phi(a))^{-1}$, $\forall a \in G$.

Proof: (1) Let $a \in G$, $\phi(a) \in G'$.

$\phi(a).e' = \phi(a) = \phi(a.e)$

$= \phi(a).\phi(e)$ (since ϕ is homomorphism)

So, $e' = \phi(e)$ (By cancellation law)

(2) Let $a \in G$. By (1), $\phi(e) = e'$, then

$e' = \phi(e) = \phi(a.a^{-1}) = \phi(a).\phi(a^{-1})$ (since ϕ is homomorphism)

$\Rightarrow e' = \phi(a).\phi(a^{-1})$

$(\phi(a))^{-1}.e' = (\phi(a))^{-1}.\phi(a).\phi(a^{-1})$

But, $(\phi(a))^{-1}.\phi(a) = e'$.

$\therefore$ $(\phi(a))^{-1} = \phi(a^{-1})$.

$\therefore$ $\phi(a^{-1}) = (\phi(a))^{-1}$.

Th. 4.5: Let f: $(G, *) \to (G', .)$ be a group homomorphism, then

(1) If H is a subgroup of G, then f(H) is a subgroup of G′.

(2) If H′ is a subgroup of G′, then $f^{-1}(H')$ is a subgroup of G.

Proof: (1) Since H is a subgroup of G, $e \in H$, then $f(e) \in f(H)$.

Since $f(e) = e'$ (by **Th. 4.4(1)**), then

$e' \in f(H)$. Therefore, $f(H) \neq \phi$.

Let $x, y \in f(H)$.

We show that $x.y^{-1} \in f(H)$.

Since $x, y \in f(H)$, then there exist $a, b \in H$ such that $x = f(a)$ and $y = f(b)$.

Therefore, $x.y^{-1} \in f(a).(f(b))^{-1}$.

Since $(f(b))^{-1} = f(b^{-1})$ [by **Th. 4.4 (2)**]

Then, $f(a).f(b^{-1}) = f(a*b^{-1}) \in f(H)$ [since $a.b^{-1} \in H$, $H \preccurlyeq G$, then $f(a*b^{-1}) \in f(H)$].

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

$\therefore$ $f(H) \preccurlyeq G'$.

(2) **H.W.**

Def. 4.6: (Kernel of a group)

Let $(G_1, *)$, $(G_2, .)$ be two groups and $f: G_1 \to G_2$ be a homomorphism. Define $Ker(f) = \{x \in G_1: f(x) = e_2\}$, where e_2 is the identity element in G_2.

Th. 4.7: Let f be a homomorphism from a group $(G_1, *)$ into a group $(G_2, .)$ with identity elements e_1, e_2, respectively, then $Ker(f)$ is a normal subgroup of G_1.

Proof: Since we have $f(e_1) = e_2$ (by **Th. 4.4 (1)**), then $e_1 \in Ker(f)$.

So, $Ker(f) \neq \phi$.

Let $a, b \in Ker(f)$.

We show that $a*b^{-1} \in Ker(f)$, i.e.,

we show $f(a*b^{-1}) = e_2$.

Since $a \in Ker(f)$, then $f(a) = e_2$ and

$b \in Ker(f)$, then $f(b) = e_2$.

Consider,

$e_2 = (f(b))^{-1}.(f(b)) = (f(b))^{-1}.e_2 = (f(b))^{-1}$.

$\therefore (f(b))^{-1} = e_2$.

Since f is a homomorphism, then

$f(a*b^{-1}) = f(a).f(b^{-1})$.

But, $f(b^{-1}) = (f(b))^{-1}$ [by **Th. 4.4 (2)**]

Then, $f(a*b^{-1}) = e_2.e_2 = e_2$.

So, $a*b^{-1} \in Ker(f)$.

$\therefore Ker(f) \preccurlyeq G_1$.

It remains to show that, $Ker(f) \nabla G_1$ **(H.W.)**.

Let (G, *) and (G′, .) be two groups.

Def. 4.8: (epimorphism mapping)

A homomorphism $\phi: G \to G'$ is said to be epimorphism if ϕ is onto **or** $\phi(G) = G'$.

Def. 4.9: (monomorphism mapping)

A homomorphism $\phi: G \to G'$ is said to be a monomorphism if ϕ is 1-1.

Def. 4.10: (isomorphism mapping)

A homomorphism $\phi: G \to G'$ is said to be an isomorphism if ϕ is 1-1 and onto.

Def. 4.11: (isomorphic between two groups)

Two groups (G, *) and (G′, .) are said to be isomorphic if there exists an isomorphism between G and G′.

It is denoted by $G \cong G'$.

Th. 4.12:

A homomorphism $\phi: G \to G'$ is 1-1 **iff** $Ker(\phi) = \{e\}$, where e is the identity element of G.

Proof: Suppose $Ker(\phi) = \{e\}$, then we show that ϕ is 1-1, i.e.,

we show that $\forall$ x, y$\in$G, $\phi(x) = \phi(y) \Rightarrow x = y$.

Since $x \in G, y \in G \Rightarrow y^{-1} \in G$ (since G is a group)

Then, $x.y^{-1} \in G$ (by closure law)

$\phi(x.y^{-1}) = \phi(x).\phi(y^{-1})$ (since ϕ is homomorphism)

$= \phi(x).(\phi(y))^{-1}$ (by **Th. 4.4 (2)**)

$= \phi(y).(\phi(y))^{-1}$ (since $\phi(x) = \phi(y)$)

$= e'$

$\therefore \phi(x.y^{-1}) = e'$.

$\Rightarrow x.y^{-1} \in Ker(\phi) = \{e\}$.

$\Rightarrow x.y^{-1} = e \Rightarrow x.y^{-1}.y = e.y$

$\Rightarrow x.(y^{-1}.y) = y \Rightarrow x.e = y \Rightarrow x = y$.

$\therefore \phi$ is 1-1.

Conversely, suppose ϕ is 1-1, then we want to show that $Ker(\phi) = \{e\}$; this means to show that

$\{e\} \subseteq Ker(\phi)$ (it is obvious) and

$Ker(\phi) \subseteq \{e\}$ **(H.W.)**

Ex. 4.13: Let $\phi: (\mathbb{Z}, +) \to (\mathbb{Z}_e, +)$ defined by $\phi(n) = 2n$, then show that ϕ is isomorphism.

Or, (Show that $(\mathbb{Z}, +) \cong (\mathbb{Z}_e, +)$)

Solution: Let n, m $\in \mathbb{Z}$, we show that $\phi(n+m) = \phi(n)+\phi(m)$.

Now, $\phi(n+m) = 2(n+m) = 2n+2m = \phi(n)+\phi(m)$.

$\therefore \phi$ is homomorphism.

Let $\phi(n) = \phi(m)$, we show that n = m.

Let $\phi(n) = \phi(m)$, then 2n = 2m. Therefore, n = m.

Hence ϕ is 1-1.

Since $\phi(n) = 2n$, i.e., $\phi(\mathbb{Z}) = \mathbb{Z}_e$.

or,

$\forall 2n \in \mathbb{Z}_e, \exists\ n \in \mathbb{Z}$ such that $\phi(n) = 2n$.

So, ϕ is onto.

$\therefore \phi$ is an isomorphism.

$\therefore \mathbb{Z} \cong \mathbb{Z}_e$.

Def. 4.14: (Automorphism group)

The set of all mapping from a group G into itself such that f is isomorphism is said to be automorphism and denoted by Auto(G) or Aut(G), i.e,

Aut(G) = $\{f: G\to G,\ f$ is isomorphism$\}$.

Def. 4.14′: (Endomorphism group)

The set of all homomorphism f from (G, *) into itself is called endomorphism and denoted by End(G) **or** E(G), i.e,

End(G) = $\{f: G\to G,\ f$ is homomorphism$\}$.

Def. 4.15:

Let (G, .) be a group and a be a fixed element in G. Define a mapping f_a: G→G by $f_a(x) = a.x$.

Th. 4.16:

Show that f_a is 1-1 and onto, but not homomorphism.

Proof: Let x, y $\in$ G.

Let $f_a(x) = f_a(y)$. We show that x = y.

Let $f_a(x) = f_a(y) \Rightarrow a.x = a.y$.

Since a is a fixed element in G and G is a group, then $\exists\ a^{-1} \in G$ such that

$a^{-1}.(a.x) = a^{-1}.(a.y) \Rightarrow (a^{-1}.a).x = (a^{-1}.a).y \Rightarrow e.x = e.y \Rightarrow x = y$.

So, f_a is 1-1.

$\forall\ x \in G, \exists\ a^{-1}.x \in G$ (since $a \in G$ and G is a group, then $\exists\ a^{-1} \in G$) such that $f_a(a^{-1}.x) = a.(a^{-1}.x) = (a.a^{-1}).x = e.x = x$.

$\therefore f_a$ is onto.

Let x, y $\in$ G, we show that $f_a(x.y) \neq f_a(x).f_a(y)$.

Now, $f_a(x.y) = a.x.y = (a.x).y = f_a(x).y$

$\therefore f_a(x.y) \neq f_a(x).f_a(y)$.

$\therefore f_a$ is not homomorphism.

Q. 4.16′: Let (G, .) be any group, then show that (F_G, o) is group, where

$F_G = \{f_a : a \in G\}$ and $f_a(x) = a.x$.

Solution:

(1) Let $f_a, f_b \in F_G$ such that

$f_a: G \to G$ and , $f_b: G \to G$, where $f_a(x) = a.x$ and $f_b(x) = b.x$.

Now, $(f_a \text{ o } f_b)(x) = f_a(f_b(x))$

$= f_a(b.x)$

$(f_a \circ f_b)(x) = a.(b.x)$

$= a.b.x$

$= f_{ab}(x) \in F_G.$

$\therefore f_a \circ f_b \in F_G.$

(2) Let $f_a, f_b, f_c \in F_G$.

We show that $((f_a \circ f_b) \circ f_c)(x) = (f_a \circ (f_b \circ f_c))(x)$

Now, $((f_a \circ f_b) \circ f_c)(x) = (f_a \circ f_b)(f_c(x))$

$= (f_a \circ f_b)(c.x)$

$= f_a(f_b(c.x))$

$= f_a(b.c.x)$

$= a.b.c.(x)$

$= a.(b.c).(x)$

$= f_a \circ (f_b \circ f_c))(x)$ [How ? write step by step]

So, $((f_a \circ f_b) \circ f_c)(x) = (f_a \circ (f_b \circ f_c))(x)$.

(3) **H.W.** (identity)

(4) **H.W.** (inverse)

Th. 4.17: (Cayley's Theorem)

If $(G, *)$ is an arbitrary group, then $(G, *) \cong (F_G, o)$.

(**Q:** State and prove Cayley's Theorem).

Proof: Define a mapping $\phi: (G, *) \to (F_G, o)$ by $\phi(a) = f_a$, $\forall\, a \in G$.

First we show that ϕ is well-defined.

Let $a, b \in G$ such that $a = b$.

Let $x \in G \Rightarrow a*x = b*x \Rightarrow f_a(x) = f_a(y) \Rightarrow \phi(a) = \phi(b)$.

Second we show that ϕ is homomorphism.

Let a, b $\in$G such that

$\phi(a*b) = f_{a*b} = f_{a*b}(x) = (a*b)*x = a*(b*x) = f_a(b*x) = f_a(f_b(x)) =$

$(f_a \circ f_b)(x) = \phi(a) \circ \phi(b)$.

$\therefore \phi$ is homomorphism.

Now, we show that ϕ is 1-1.

Let $\phi(a) = \phi(b)$, $\forall$ a, b$\in$G.

$\Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow a*x = b*x$.

Since $x \in G$, then $\exists\ x^{-1} \in G$ (since G is a group)

$\Rightarrow a*(x*x^{-1}) = b*(x*x^{-1}) \Rightarrow a = b \Rightarrow \phi$ is 1-1.

Now, $\forall\ f_a \in F_G$, $\exists$ a $\in$G such that $\phi(a) = f_a$.

$\therefore \phi$ is onto.

$\therefore \phi$ is an isomorphism.

$(G, *) \cong (F_G, \circ)$ [by First Isomorphism Group Theorem].

Q 4.17′: Give an example on Cayley's Theorem.