## 6. Homomorphisms.

Definition: Let $G, H$ be two group. A mapping $\phi: G \to H$ is called a homomorphism if $\phi(xy) = \phi(x)\phi(y)$

[~~If we apply binary~~ In the notation, $xy$, binary operation on $G$ is involved, and in the notation $\phi(x)\phi(y)$, binary operation on $H$ is involved.]

Definition: Let $\phi: G \to H$ be a homomorphism.

If $\phi$ is injective, it is called a monomorphism.

If $\phi$ is surjective, it is called an epimorphism

If $\phi$ is bijective, it is called an ~~isof~~ isomorphism.

If $f$ be a homomorphism of a group $G$ into itself, i.e, if $f: G \to G$ be a homomorphism, then $f$ is called an endomorphism.

If $f: G \to G$ be an isomorphism, then $f$ is called an automorphism.

Examples: 1. Let $G$ and $H$ be groups and let $e'$ be the identity element of $H$. Then the mapping $f: G \to H$ defined by

$f(a) = e', \forall a \in G$ is a homomorphism as

$f(ab) = e' = e'.e' = f(a).f(b), \forall a, b \in G$. It is called the trivial homomorphism

2. For any group $G$, the identity mapping $i: G \to G$ defined by $i(a) = a, \forall a \in G$ is an automorphism.

3. Let $G$ be the group $(\mathbb{R}^+, \cdot)$ of positive real numbers under multiplication and $H$ be the group $(\mathbb{R}, +)$ of real numbers under addition. Then $\phi(x) = \log x$ is an ~~isomp~~ isomorphism.

$(\phi: \mathbb{R}^+ \to \mathbb{R})$

Here, $\phi(x_1) = \phi(x_2) \Rightarrow \log x_1 = \log x_2 \Rightarrow x_1 = x_2$. So, $\phi$ is injective.

For, $y \in \mathbb{R}$, $e^y \in \mathbb{R}^+$ and $\phi(e^y) = \log e^y = y$. So, $\phi$ is surjective.

Also $\phi(xy) = \log xy = \log x + \log y = \phi(x) + \phi(y)$

So, $\phi$ is a homomorphism. So, $\phi$ is an isomorphism.

4. Let $G$ be a group. For a given $a \in G$, consider the mapping

$I_a : G \to G$ given by $I_a(x) = axa^{-1}$, $\forall x \in G$.

Since, $I_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = I_a(x) I_a(y)$

$I_a$ is a homomorphism. $I_a(x) = I_a(y) \Rightarrow axa^{-1} = aya^{-1}$

$\Rightarrow x = y$ (by Cancellation laws). Hence, $I_a$ is injective. For any $x \in G$

$I_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$., Hence, $I_a$ is surjective.

Consequently, $I_a$ is an automorphism of $G$. It is called the inner automorphism of $G$ determined by $a$.

5. Consider the groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ and a mapping

$\phi : \mathbb{Z} \to 2\mathbb{Z}$ by $\phi(a) = 2a$, $a \in \mathbb{Z}$. Then $\phi$ is an isomorphism (Exercise)

6. Let $G$ be the group $(\mathbb{Z}, +)$. Let $\phi : G \to G$ be defined by $\phi(x) = x+1$, $x \in G$. Then $\phi$ is not a homomorphism as

$\phi(2) = 3$, $\phi(3) = 4$ and $\phi(2+3) = \phi(5) = 6$

So, $\phi(2+3) = 6$ and $\phi(2) + \phi(3) = 3+4 = 7$

Hence, $\phi(2+3) \neq \phi(2) + \phi(3)$

7. Let $G = S_3$ and $G' = (\{1, -1\}, \cdot)$ be two groups.

Let $\phi : G \to G'$ defined by $\phi(x) = 1$ if $x$ be an even permutation in $S_3$
$= -1$ if $x$ be an odd permutation in $S_3$

Then $\phi$ is a homomorphism

Let $x, y \in S_3$ Then $xy \in S_3$

Case 1 Let $x, y$ both be even. Then $xy$ is also even.

So $\phi(x) = 1$, $\phi(y) = 1$ and $\phi(xy) = 1$, So $\phi(xy) = \phi(x)\phi(y) = 1$

Case 2 Let $x, y$ both be odd. Then $\phi(x) = -1$ $\phi(y) = -1$

and $xy$ is even (as sum of odd integer is even). So, $\phi(xy) = 1$

So, $\phi(xy) = \phi(x)\phi(y) = 1$

Case 3: Let one of $x, y$ be odd and the other is even. Without any loss of generality, let $x$ be odd and $y$ be even. Then $xy$ is odd

So, $\phi(xy) = -1$ and $\phi(x) = -1$, $\phi(y) = 1$

So $\phi(xy) = \phi(x)\phi(y) = -1$

Hence $\phi(xy) = \phi(x)\phi(y)$, $\forall\, x, y \in S_3$.

So $\phi$ is a homomorphism.

It is surjective but not injective. So $\phi$ is an epimorphism.

Theorem 6.1 Let $G$ and $H$ be be groups with identities $e$ and $e'$, respectively, and let $\phi : G \to H$ be a homomorphism. Then

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

(ii) $\phi(x^{-1}) = (\phi(x))^{-1}$ for each $x \in G$.

(iii) if $x \in G$ then $\phi(x^n) = (\phi(x))^n$, $n$ being an integer.

(iv) if $x \in G$ and $o(x)$ is finite then $o(\phi(x))$ is a divisor of $o(x)$.

Proof: (i) $\phi(e)\phi(e) = \phi(ee) = \phi(e) = e'\phi(e)$. Hence, by the Cancellation Law, $\phi(e) = e'$

(ii) Let $x \in G$. Then $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$ --- (a)

Also $e' = \phi(e) = \phi(x^{-1}x) = \phi(x^{-1})\phi(x)$ --- (b)

So, from (a) and (b) ~~$\phi(x) \cdot \phi$~~ $\phi(x)\phi(x^{-1}) = \phi(x^{-1})\phi(x) = e'$

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

(iii) Case 1, $n = 0$. In this case, the statement reduces to (i) and so it holds.

Case 2 $n$ is a positive integer.

The statement is true for $n=1$. Let us assume that the statement is true for $n = m$, $m$ being a positive integer.

Then $\phi(x^m) = (\phi(x))^m$

Now $\phi(x^{m+1}) = \phi(x^m x) = \phi(x^m)\phi(x) = (\phi(x))^m \phi(x)$
$= (\phi(x))^{m+1}$

This shows that the statement is true for $n = m+1$. By the principle of mathematical induction, $\phi(x^n) = (\phi(x))^n$.

<u>case 3</u> $n$ is a negative integer.

Let $n = -m$, $m$ is a positive integer.

$$\phi(x^n) = \phi(x^{-m}) = \phi((x^{-1})^m) = (\phi(x^{-1}))^m \text{ by case 2}$$

$$= ((\phi(x))^{-1})^m \text{ by (ii)}$$

$$= (\phi(x))^{-m} = (\phi(x))^n$$

So, $\phi(x^n) = (\phi(x))^n$ for any integer $n$

(iv) If $x \in G$ and $o(x) = n$, then $x^n = e$

So, $\phi(x^n) = \phi(e) = e'$. But $\phi(x^n) = (\phi(x))^n$

So, $(\phi(x))^n = e'$ Hence $\phi(x)$ is of finite order

and $o(\phi(x))$ divides $o(x)$.

Let $G$ and $G'$ be two groups. Let $\phi : G \to G'$ be a homomorphism

The image of $\phi$, denoted by $\text{Im}\phi$, is a subset of $H$ defined by

$\text{Im}\phi = \{\phi(x) : x \in G\}$. $\text{Im}\phi$ is also called the homomorphic

image of $\phi$ and is also denoted by $\phi(G)$

The Kernel of $\phi$, denoted by $\text{Ker}\phi$, is a subset of $G$ defined by

$\text{Ker}\phi = \{x \in G : \phi(x) = e'\}$ where $e'$ is the identity in $G'$.

<u>Theorem 6.2</u> (i) $\text{Im}\phi$ is a subgroup of $G'$

(ii) $\text{Ker}\phi$ is a normal subgroup of $G$

Proof: $e' = \phi(e) \in \text{Im}\phi$. So, $\text{Im}\phi \neq \phi$

Let $a', b' \in \text{Im}\phi$. So $a' = \phi(a)$, $b' = \phi(b)$, $a, b \in G$

Now $a'b' = \phi(a)\phi(b) = \phi(ab) \in \text{Im}\phi$. Let $a' \in \text{Im}\phi$. So $a' = \phi(a)$,

$a \in G$. Now, $a'^{-1} = (\phi(a))^{-1} = \phi(a^{-1}) \in \text{Im}\phi$. So $\text{Im}\phi$ is a

subgroup of $G'$

(ii) As $\phi(e) = e'$, $e \in \text{Ker}\phi$ So $\text{Ker}\phi \neq \phi$.

Let $a, b \in \mathrm{Ker}\phi \Rightarrow \phi(a) = e', \phi(b) = e'$

Now $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e'e'^{-1} = e'e' = e'$

So, $ab^{-1} \in \mathrm{Ker}\phi$. So, $\mathrm{Ker}\phi$ is a subgroup of $G$.

Let $x \in G$ and $h \in \mathrm{Ker}\phi$. So $\phi(h) = e'$

Now
$$\phi(xhx^{-1}) = \phi(x)\phi(h)\phi(x^{-1})$$
$$= \phi(x)e'(\phi(x))^{-1} \text{ as } \phi(h) = e' \text{ and } \phi(x^{-1}) = (\phi(x))^{-1}$$
$$= \phi(x)(\phi(x))^{-1}$$
$$= e'$$

So $xhx^{-1} \in \mathrm{Ker}\phi$. So $\mathrm{Ker}\phi$ is a normal subgroup of $G$.

Theorem 6.3 A homomorphism $\phi: G \to G'$, $G$ and $G'$ are two groups, is injective if and only if $\mathrm{Ker}\phi = \{e\}$

Proof : Suppose $\phi$ is injective. Let $x \in \mathrm{Ker}\phi$. Then $\phi(x) = e'$

or, $\phi(x) = \phi(e) \Rightarrow x = e$, as $\phi$ is injective

So, $\mathrm{Ker}\phi = \{e\}$

Conversely, let $\mathrm{Ker}\phi = \{e\}$. Then $\phi(x) = \phi(y) \Rightarrow$

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

$\Rightarrow xy^{-1} \in \mathrm{Ker}\phi \Rightarrow xy^{-1} = e \Rightarrow x = y$

Hence $\phi$ is injective.

Theorem 6.4 Let $G, G'$ be two groups and $\phi: G \to G'$ be an epimorphism. Then

(i) if $G$ is commutative then $G'$ is commutative

(ii) if $G$ is cyclic then $G'$ is cyclic

Also, The converse of (i) and (ii) are not true.

Proof Let $a', b' \in G'$. Then $\exists\, a, b \in G$ such that $\phi(a) = a', \phi(b) = b'$ as $\phi$ is surjective.

Now
$$a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) \text{ (as } G \text{ is commutative)}$$
$$= \phi(b)\phi(a) = b'a'$$

So, $G'$ is commutative.

(ii) Let $G = \langle a \rangle$.

Let $b' \in G'$. Since $\phi$ is surjective, $\exists\ b \in G$ such that $\phi(b) = b'$

As $b \in G$, so $b = a^m$, for some integer $m$

So, $b' = \phi(b) = \phi(a^m) = (\phi(a))^m$

This shows that $G' = \langle \phi(a) \rangle$. So, $G'$ is cyclic

Converse of (i) and (ii) are not true follows from example 7 where $G = S_3$ and $G' = (\{\{1, -1\}, \cdot\})$ and the epimorphism $\phi : G \to G'$, defined by

$$\phi(x) = 1 \text{ if } x \text{ is even permutation}$$
$$= -1 \text{ if } x \text{ is odd permutation}$$

Here $G'$ is commutative but $G$ is not. Here $G'$ is cyclic but $G$ is not.

Let $G$ and $G'$ be two groups. Let $H$ be a subgroup of $G$ and $K'$ be a subgroup of $G'$. ~~we define~~ Let $\phi : G \to G'$ be a homomorphism.

We define $\phi(H) = \{\phi(x) : x \in H\}$ and $\phi^{-1}(K') = \{x \in G : \phi(x) \in K'\}$

Theorem 6.5 Let $G$ and $G'$ be two groups and $\phi : G \to G'$ be a homomorphism. Let $H$ and $K'$ be two subgroups of $G$ and $G'$ respectively. Then $\phi(H)$ and $\phi^{-1}(K')$ are subgroups of $G'$ and $G$ respectively

Proof $\phi(e) = e' \in \phi(H)$ as $e \in H$; $e, e'$ be the identities in $G$ and $G'$ respectively. So, $\phi(H)$ is non-empty.

Let $a', b' \in \phi(H) \Rightarrow \exists\ a, b \in G$ such that $\phi(a) = a'$, $\phi(b) = b'$

Now $a'^{-1} b' = (\phi(a))^{-1} \phi(b) = \phi(a^{-1}) \phi(b) = \phi(a^{-1} b) \in \phi(H)$

as $a^{-1} b \in H$, $H$ is a subgroup of $G$. So, $\phi(H)$ is a subgroup of $G'$. As $\phi(e) = e' \in K'$, so, $e \in \phi^{-1}(K')$

So, $\phi^{-1}(K')$ is non-empty. Let $a, b \in \phi^{-1}(K')$. So,
$\phi(a), \phi(b) \in K'$. As $K'$ is a subgroup, $(\phi(a))^{-1}\phi(b) \in K'$
or, $\phi(a^{-1})\phi(b) \in K' \Rightarrow \phi(a^{-1}b) \in K' \Rightarrow a^{-1}b \in \phi^{-1}(K')$
So, $\phi^{-1}(K')$ is a subgroup of $G$.

Theorem 6.6. Let $G$ and $G'$ be two groups and $H$ and $K'$ are two subgroups of $G$ and $G'$ respectively and let $\phi: G \to G'$ be an epimorphism. Then
(i) if $H$ is a normal subgroup of $G$, then $\phi(H)$ is a normal subgroup of $G'$
(ii) if $K'$ is a normal subgroup of $G'$, then $\phi^{-1}(K')$ is a normal subgroup of $G$.

Proof: (i) Since $H$ is a subgroup, $\phi(H)$ is a subgroup by Theorem 6.5. Let $x' \in G'$ and $h' \in \phi(H)$. So $\exists\, h \in H$ such that $\phi(h) = h'$. Since $\phi$ is surjective, $\exists\, x \in G$ such that $\phi(x) = x'$. So, $x'h'x'^{-1} = \phi(x)\phi(h)(\phi(x))^{-1}$
$= \phi(x)\phi(h)\phi(x^{-1}) = \phi(xhx^{-1}) \in \phi(H)$ as $xhx^{-1} \in H$ since $H$ is a normal subgroup of $G$. $\phi(H)$ is a normal subgroup of $G'$

(ii) As $K'$ is a subgroup of $G'$, $\phi^{-1}(K')$ is a subgroup of $G$, by Theorem 6.5. Let $x \in G$, $k \in \phi^{-1}(K')$
~~As $\phi$ is surjective, $\exists\, x \in G$, such that~~ Then $\phi(k) \in K'$
Now as $K'$ is a normal subgroup of $G'$,
$\phi(x)\phi(k)(\phi(x))^{-1} \in K' \Rightarrow \phi(x)\phi(k)\phi(x^{-1}) \in K'$
$\Rightarrow \phi(xkx^{-1}) \in K' \Rightarrow xkx^{-1} \in \phi^{-1}(K')$ as $xkx^{-1} \in K'$ and $K'$ is a normal subgroup of $G'$. So, $\phi^{-1}(K')$ is a normal subgroup of $G$.