Definition : Let G be a group with respect to a binary operation o and let G' be another group with respect to a binary operation o'. Let $f : G \to G'$ be a mapping such that

$$f(a \text{ o } b) = f(a) \text{ o}' f(b)$$

where, $a, b \in G$ and $f(a)$ and $f(b)$ are their images under f. Then the mapping f is said to be an *homomorphism* and we say that G is homomorhic to G'.

If the mapping f is a one-one and onto mapping, then f is said to be an *isomorphism* and we say that G is isomorphic to G'.

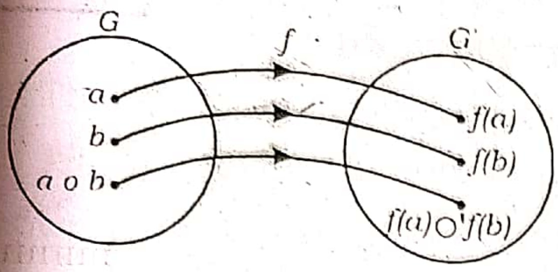
Thus if f is an isomorphism, the following conditions are satisfied.

(i) f is a homomorphism, that is $f(a \text{ o } b) = f(a) \text{ o}' f(b)$

i.e. f preserves group operation.

(ii) f is a one-one and onto mapping.

Explanation : We take any two elements a and b in the



If it so happens that $f(a)\ o'\ f(b) \in G'$ is the image of $a \circ b \in G$ under the mapping f, then we say that f is a homomorphism. Moreover if f is one-one and onto, then we say that f is an isomorphism. The above explanation can be incorporated into a picture like this.

If G is isomorphic to G', we write $G \cong G'$. If f is an isomorphism of G onto G', the group G' is called an isomorphic image of G.

There are 4 separate steps in proving that a group G is isomorphic to a group G'.

Step 1. Mapping : that is, define a function f from G to G'.

Step 2. 1-1 : Prove that f is one-one; that is, assume $f(a) = f(b)$ and prove that $a = b$.

Step 3. Onto : Prove that f is onto; that is, for any element g' in G', find an element g in G such that $f(g) = g'$.

Step 4. Prove that f is operation preserving, that is, show that $f(a\ b) = f(a)f(b)$ for all $a, b \in G$.

Ex.1. Let I be the additive group of integers and let E be the subgroup of even integers.

That is $\quad G = (I, +) \quad$ and $\quad G' = (E, \cdot)$.

Consider the mapping $f : I \to E$ given by

$$f(n) = 2n \text{ where } n \in I.$$

Show that f is an isomorphism.

Soln. f preserves operations in G and G'.

Let $m, n \in I$. Then

$$f(m + n) = 2(m + n) = 2m + 2n$$
$$= f(m) + f(n)$$

f is onto : Also, f is an onto mapping, since an even integer say $2n \in E$ is the image of an integer $n \in I$.

f is one one : Again, f is a one-one mapping, for

$$f(m) = f(n) \Rightarrow 2m = 2n$$

i.e. $\quad$,, $\quad$,, $\quad \Rightarrow m = n.$

Thus we find that (i) f is a homomorphism and (ii) f is one-one and onto mapping.

Hence f is an isomorphism.

Ex. 2. Let Z be the additive group of integers and let G' be the multiplicative group of numbers of the form 2^m, where $m = 0, \pm 1, \pm 2, \ldots$

That is, $\quad G = (Z, +)$

and $\quad G' = [\{2^m, m = 0, \pm 1, \pm 2, \ldots\}, \cdot]$

Let the mapping : $f : Z \rightarrow \{2^m\}$ be defined by

$$f(m) = 2^m; \quad m \in I.$$

Show that f is an isomorphism.

Soln. f preserves operation in G and G'.

Let $m, n \in I$. Then

$$f(m+n) = 2^{m+n} = 2^m \cdot 2^n$$
$$= f(m) \cdot f(n)$$

Therefore f is a homomorphism.

f is onto : Obviously f is an onto mapping, since the preimage-point of any element say $2^k \in G'$ is k which $\in I$.

f is one-one : Also f is one-one, since $f(m) = f(n) \Rightarrow 2^m = 2^n$, i.e. $m = n$

Hence f is an isomorphism.

Ex. 3. Let R^+ be the multiplicative group of positive real numbers and let R be the additive group of real numbers. Consider the mapping $f : R^+ \rightarrow R$ given by $f(x) = \log x$, where $x \in R^+$. Show that f is an isomorphism.

Soln. f preserves operations in R^+ and R.

Let $x, y \in R^+$ in which the operation is multiplication.

We observe that

$$f(xy) = \log(xy) = \log x + \log y$$
$$= f(x) + f(y)$$

Therefore f is a homomorphism.

f is onto : Also, f is onto; to prove this, it has to be shown that there is not a single element in R which is not the image of an element of R^+. In particular, let $a \in R$ and let this be image of u i.e. $f(u) = a$. From the definition of the given function $f(u) = \log u$.

Thus $\log u = a$ i.e. $u = e^a$ and $e^a \in R^+$.

Hence f is an onto-mapping.

f is one-one : We have now to show that f is one-one.

For this, let $u, v \in R^+$. Then

$f(u) = f(v) \Rightarrow \log u = \log v$ i.e. $u = v$.

Thus we find that

(i) f is a homomorphism and (ii) f is one-one and onto.

Hence f is an isomorphism.

Ex.4. Let $G = \{1, -1, i, -i\}$ be a multiplicative group and let Z_4 (= $I/(4)$) be the additive group of residue classes modulo 4 i.e. $Z_4 = \{\{0\}, \{1\}, \{2\}, \{3\}\}$.

Consider the mapping $f : G \to Z_4$ defined in either of the two ways :

$f : G \to Z_4$	$f : G \to Z_4$
$1 \to \{0\}$	$1 \to \{0\}$
$-1 \to \{2\}$	$-1 \to \{2\}$
$1 \to \{3\}$	$i \to \{1\}$
$-i \to \{1\}$	$-i \to \{3\}$

We will take up the first mapping and show that it is an isomorphism.

Soln. The multiplication table for G and Z_4 are as follows :

$(G, \times)$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$(Z_4, +_4)$

+	0	2	3	1
0	0	2	3	1
2	2	0	1	3
3	3	1	2	0
1	1	3	0	2

The guide lines in the preparation of the table are as follows. We first of all make the multiplication table for G in the usual way. To write down the table for Z_4 we notice that since $1 \to \{0\}$, $-1 \to \{2\}$, $i \to \{3\}$, $-i \in \{1\}$. therefore the guiding numbers in the table for Z_4 row-wise and column-wise will be 0, 2, 3, 1 respectively corresponding to their pre-image points in G. The computation work in Z_4 is done as usual. To read the table, we take any point in the table for Z_4, say the element 2 (i.e.) $\{2\}$ which occurs in the third row and third column and wish to know its preimage point in G. For this we have to take that point in the table of G which is at the point of intersection of the third row and third column. That point is -1 which is $i \cdot i$. Thus it follows that

$$f\{(i) \cdot (i)\} = f(-1) = \{2\} = \{3\} + \{3\} = f(i) + f(i)$$

This is true for any two points $\in G$.

In other words, if we replace $1 \in G$ by $\{0\}$, -1 by $\{2\}$, i by $\{3\}$ and $-i$ by $\{1\}$, the multiplication table for G is transformed exactly into the table for Z_4. These two groups show one-to-one correspondence between their elements.

Thus f is an homomorphism. Again f is onto, since every point of Z_4 is the image of some point in G.

Also f is one-one.

Hence f is an isomorphism between $\{1, -1, i, -i\}$ and $\{(0, 2, 3, 1) \pmod 4\}$.

Note : Similarly it can be verifed that there is an isomorphism between $\{1, -1, i, -i\}$ and $\{0, 2, 1, 3, \text{mod } (4)\}$.

Thus there may exist more than one isomorphic mappings of a group G to a group G'.

6.2 Example of a homomorphism which is not isomorphism [M.U. 90H, Dumka 96H]

Ex.1. Let $(Z, +)$ be the additive group of integers. Let m be a fixed integer. Show that the map $f: Z \to Z$ given by $f(a) = ma$, $a \in Z$ is a homomorphism.

Soln. Let $a, b \in Z$. Then

$$f(a + b) = m(a + b) = ma + mb = f(a) + f(b).$$

Hence f is a homomorphism.

But this homomorphism is one-one but not onto if $m \neq \pm 1$.

Ex.2 Let $(R, +)$ be the additive group of real numbers and $K = \{e^{i\theta},\ \theta$ is real$\}$ be the multiplicative group of complex numbers with absolute value 1. Show that the map $f: R \to K$ given by $f(\theta) = e^{i\theta}$, $\theta \in R$ is a homomorphism.

Soln. Let $\theta_1, \theta_2 \in R$. Then

$$f(\theta_1 + \theta_2) = e^{i(\theta_1 + \theta_2)} = e^{i\theta_1} \cdot e^{i\theta_2} = f(\theta_1) \cdot f(\theta_2)$$

Hence f is a homomorphism.

But this homomorphism is onto but not one-one, because

$$f(\theta + 2n\pi) = e^{i(\theta+2n\pi)} = e^{i\theta} \cdot e^{i2n\pi}$$

$$= e^{i\theta} \cdot 1 \text{ for } n = 0, 1, 2, 3...$$

In fact, if we take $\theta_1 = 2\pi$ and $\theta_2 = 4\pi$ then $\theta_1 \neq \theta_2$.

But $f(\theta_1) = e^{i2\pi} = 1$ and also $f(\theta_2) = e^{i4\pi} = 1$.

Thus $f(\theta_1) = f(\theta_2)$ although $\theta_1 \neq \theta_2$.

Hence f is not an isomorphism.

6.3 Theorem : The composition of two homomorphisms is a homomorphism.

Proof : Let $f: G \to G'$ and $g: G' \to G''$ be two homomorphisms.

If $a, b \in G$, then

$$(g o f)(ab) = g\{f(ab)\}$$

$= g\{f(a)\, f(b)\}$; since f is a homomorphism

$= g\{f(a)\}\, g\{f(b)\}$; since g is a homomorphism.

$= (g \circ f)\,(a)\,(g \circ f)\,(b)$

Hence $g \circ f : G \to G''$ is also a homomorphism.

Cor. Composition of two isomorphism is an isomorphism.

The proof follows from the fact that the composition of two bijections (one-one-onto functions) is a bijection.

6.4 Theorem : To show that the relation '$\cong$' of being isomorphic is an equivalence relation on any set S of groups.

[P.U. 83H; B.U. 78H, 2003H; Bhag 90H, 2003H; R.U. 92H; Haz. 2003H]

Proof : We shall prove that the relation of isomorphism denoted by $\cong$ in the set S of all groups is reflexive, symmetric and transitive. Let $G, H, K \in S$.

Relexive : $G \cong G$,

Let f be the identity mapping on G i.e. $f : G \to G$

such that $f(x) = x$ for all $x \in G$.

Obviously f is one-one onto.

Also, Let $x, y \in G$, then $f(x) = x$ and $f(y) = y$.

$\therefore \quad f(xy) = xy$

$\qquad\qquad = f(x)\, f(y)$.

Hence f preserves operations in G and G. Thus f is an isomorphism of G onto G. Hence $G \cong G$.

Symmetric : i.e. $G \cong H \Rightarrow H \cong G$.

Let $G \cong H$. Let f be an isomorphism of G onto H. Then f is one-one onto and preserves operations in G and H.

Since f is one-one onto, therefore it is invertible, i.e. f^{-1} exists. Also we know that the inverse function f^{-1} is one-one onto.

Now we shall show that $f^{-1} : H \to G$ also preserves operation.

Let $x', y' \in H$. Then there exist elements $x, y \in G$ such that $f^{-1}(x') = x$ and $f^{-1}(y') = y$

$$\Rightarrow f(x) = x', f(y) = y' \quad \dots (1)$$

Now, $f^{-1}(x'y') = f^{-1}[f(x) f(y)]$; from (1)

$= f^{-1}[f(xy)]$; since $f(xy) = f(x) f(y)$

$= xy$; from definition of f^{-1}

$= f^{-1}(x') f^{-1}(y')$ from (1)

$\therefore f^{-1}$ preserves operation in H and G.

Hence $H \cong G$.

Transitive : i.e. $G \cong H$, $H \cong K \Rightarrow G \cong K$.

Suppose G is isomorphic to H and H is isomorphic to K.

Further suppose that $f : G \to H$ and $g : H \to K$ are the respective isomorphic mappings.

Then $g \circ f : G \to K$.

If both f and g are one -one onto, we know that the composite mapping

$g \circ f : G \to K$ defined by

$$g \circ f(x) = g[f(x)] \text{ for all } x \in G$$

is also one-one onto.

Further, if $x, y \in G$, then

$(g \circ f)(xy) = g[f(xy)]$

$= g[f(x)f(y)]$, $\because f$ is an isomorphism

$= g[f(x)]g[f(y)]$; g is an isomorphism

$= [(g \circ f)(x)][(g \circ f)(y)]$

Hence $g \circ f$ preserves operations in G and K.

$\therefore g \circ f$ is an isomorphism of G on K and $\therefore G \cong K$.

Hence the relation of isomorphism in the set of groups is an equivalence relation.

6.5 THEOREM

Let $f : G \to G'$ be a homomorphism of groups.

(i) If e and e' be the identities in G and G' respectively then $f(e) = e'$.

(ii) If $f(a) = a'$, then $f(a^{-1}) = (a')^{-1}$.

i.e. $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

In other words, if $f: G \to G'$ be a homomorphism, then their identities correspond and their inverses correspond.

(iii) If the order of $a \in G$ is finite, then the order of $f(a)$ is a divisor of the order of a.

[P.U.80H; Bhag.95H; B.U.98H; 2002H; Mithila 98H, 200H; Dumka 95H; Haz. 96H, 97H, 2004H]

Proof : (i) Let $f(e) = e'$ where e is the identity of G and $e' \in G'$.

If f is a homomorphism, we have to prove that e' is the identity of G'.

Take $\quad x \in G$ and let $f(x) = x'$ $(x' \in G')$.

Now $\quad x = ex,$

$\therefore \quad f(x) = f(ex)$

$= f(e) \cdot f(x)$; since f is a homomorphism

$\Rightarrow \quad x' = e'x'$

which means that e' (i.e. $f(e)$) is the identity in G'.

(ii) Given $f(a) = a'$.

Now $\quad aa^{-1} = e$ (the identity in G)

$\therefore \quad f(aa^{-1}) = f(e) = e'$; from (i)

That is, $\quad f(a) \cdot f(a^{-1}) = e'$ since f is a homomorphism

i.e. $\quad a'f(a^{-1}) = e'$

which means that the inverse of a' is $f(a^{-1})$.

That is, $\quad f(a^{-1}) = (a')^{-1} = [f(a)]^{-1}$.

(iii) Let $a \in G$ and $o(a) = m$.

Thus, we have $o(a) = m \Rightarrow a^m = e$.

$\therefore \quad f(a^m) = f(e)$

$\Rightarrow f(aaa \ldots \text{ to } m \text{ factors}) = e'$

$\Rightarrow f(a)\, f(a) \ldots m \text{ times} = e' \Rightarrow [f(a)]^m = e'.$

Hence if n is the order of $f(a)$ in G', then n must be a divisor of m; i.e. $o(f(a))$ is a divisor of $o(a)$.

6.6 Theorem : Show that every isomorphic image of a cyclic group is again cyclic. **[Bhag. 2001H]**

Proof: Let $G = <a>$ be a cyclic group generated by a. Let G' be an isomorphic image of G under the isomorphism f i.e. $f: G \to G'$.

The elements of G' are the images of the elements of G under the mapping f.

Let $f(a^n) \in G'$ be the image of the element $a^n \in G$.

We have,

$f(a^n) = f(a\, a\, a \ldots \text{ to } n \text{ factors})$

$= f(a)\, f(a)\, f(a) \ldots$ to n factors, since f is an isomorphism.

$= [f(a)]^n$

Thus we see that every element of G' can be expressed as an integral power of $f(a)$.

Hence G' is cyclic and $f(a)$ is a generator of G'.

6.7 Theorem : Show that every homomorphic image of an Abelian group is Abelian. **[R.U. 2000H]**

Soln. : Let G be an Abelian group. Let f be a homomorphic mapping of G onto G'. Then G' is a homomorphic image of G.

It is to prove that G' is Abelian.

Let a', b' be any two elements of G'.

Then $f(a) = a'$ and $f(b) = b'$ for some $a, b \in G$.

We have, $a'b' = f(a)\, f(b) = f(ab)$

$\because f$ is homomorphic mapping

$= f(ba)$; $\because G$ is Abelian

$= f(b)\, f(a) = b'a'$

Hence G' is Abelian.