**UNIT-V**

**HOMOMORPHISMS**

**DEFINITION:** Let (G, o) and ( \*) be two groups. Then a function f: G  is said to be homomorphism if f(aob) = f(a) \*f(b)  a, b G.

**Examples:**

1. Let G and  be two groups. Then f; G  be defined by f(a) = , where  is the identity element of  Then f is a homomorphism because f(ab) =  =  .  = f(a) f(b)  a, b G.

2. Let G be any group. Then the identity mapping IG : G G is a homomorphism because IG (ab) = ab = IG (a) IG (b)  a, b G.

3. Let G be the additive group of integers. Then f : G G defined by f(x) = 5x is a homomorphism because f(a + b) = 5 (a + b)

= 5a + 5b

= f(a) + f(b)  a, b G.

4. Let G = (R+, . ), the group of all positive reals under multiplication and let  = (R, +) the additive group of reals. Define f : G as f(a) = log a,  a, b G. Then f is a homomorphism because f(ab) = log ab

= log ab + log b

= f(a) + f(b)  abG.

5. Let G = (R, +) and  = (R+, . ). Then f : G defined by f(a) = 2a is a homomorphism because f(a + b) = 2a+b = = 2a. 2b = f(a) . f(b)  a, b G.

**ISOMORPHISM:** Let G and  be two groups. Then a function f : G  is said to be an onto isomorphism if

(i) f is homomorphism

(ii) f is one-one

(iii) f is onto

**Example:** Let G = (R, +) be the additive of reals and  = (R+, . ) be the multiplicative group of all positive reals. Then f : G defined by f(x) = ex  x G is an isomorphism.

**Solution:**

**f is homomorphism.** Let x1, x2 G.

Then f(x1 + x2) = 

=  . 

= f(x1) f(x2)

 f is a homomorphism.

**f is one-one:** Let x1, x2 G such that f(x1) = f(x2)

 

 log = log

 x1 log e = x2 log e

 x1 = x2

 f is one-one

**f is onto:** Let y. Then y is a positive real number and so log y G. Also, f(log y) = elog y = y. Thus, for each y,  log y G such that f(log y) = y.

 f is onto.

Hence, f is an isomorphism.

**Example:** Let G = (R+, . ), the multiplicative group of positive reals and  = (R, +), the additive group of reals. Then f : G defined by f(x) = log x  x G is an isomorphism.

**Solution:**

**f is a homomorphism:** Let x1, x2 G.

Then f(x1 . x2) = log x1 . x2

= log x1 + log x2

= f(x1) + f(x2)

 f is a homomorphism

**f is one-one:** Let x1, x2 G such that f(x1) = f(x2).

Then f(x1) = f(x2)

 log x1 = log x2

  = 

 x1 = x2

 f is one-one.

**f is onto:** Let y. then eyG and f(ey) = log ey = y log e = y. Thus, for each y  eyG such that f(ey) = y. Thus, f is onto. Hence f is an isomorphism.

**ISOMORPHIC GROUPS:** Two groups G and  are said to be isomorphic if there exists an isomorphism from G onto  and we write G .

**Example:** Show that the additive group of integers G = {….. – 3, – 2, – 1, 0, 1, 2, 3, …} is isomorphic to the additive group  = {….. – 3m, –2m, –m, 0, 0, 2m, 3m, ….}, where m is any fixed integer except zero. i.e. prove that Z  m Z, m is a non-zero integer.

**Solution:** Let f : G   be defined by f(x) = mx  xG.

**f is homomorphism:** Let x1, x2 G.

Then f(x1 + x2) = m(x1 + x2)

= mx1 + mx2

= f(x1) + f(x2)

 f is a homomorphism.

**f is one-one:** Let x1, x2 G such that

f(x1) = f(x2)

 mx1 = mx2

 x1 = x2 [ m  0]

 f is one-one.

**f : G is onto:** Let y. Then y/m G and f (y/m) = m(y/m) = y. Thus, for each y,  y/m G such that f(y/m) = y.

 f is onto.

Hence f : G  is an isomorphism of G onto . Thus, G  .

**ENDOMORPHISM:** Let G be a group. Then a homomorphism f : GG is called an endomorphism.

**AUTOMORPHISM:** Let G be a group. Then an isomorphism f : G  G is called an automorphism.

**Example:** Let G be the additive group of integers. Then  : GG defined by (x) = – x is an automorphism.

**Solution:**

** is a homomorphism:** Let x, y G.

Then  (x + y) = – (x + y)

= – x – y

= (–x) + (–y) = (x) + (y)

  is a homomorphism (or endomorphism).

** is one-one:** Let x, y G such that (x) = (y)

Then, (x) = (y)

 – x = – y  x = y

  is one-one.

** : G****G is onto:** Let yG. Then – yG and  (– y) = – (– y) = y.

Thus,  is onto. Hence  is an automorphism.

**Example:** Let G be the multiplicative group of positive reals. Define : GG by (x) = x2 for all xG. Then  is an automorphism.

**Solution:**

** is a homomorphism:** Let x, yG.

Then, (xy) = (xy)2

= x2 y2

= (x) (y)

  is a homomorphism (or endomorphism)

** is one-one:** Let x, yG such that (x) = (y).

Then (x) = (y)

x2 = y2

 x = y [ x > 0, y > 0]

  is one-one.

** is onto:** Let yG. Then G and  () = ()2 = y

  is onto.

Hence  is an automorphism.

**THEOREM:** Let  : G  be a homomorphism. Then

(i) (e) = , where e and  are the identities of G and  respectively.

(ii)  (x–1) = [ (x)]–1  x G.

**Proof:** (i) Let xG. Then

(x) .  = (x)

= (xe)

= (x) (e) [ is a homomorphism]

  (x) .  = (x) (e)

  = (e) [By left cancellation law]

 (e) = .

(ii) Let x G be any element. Than x–1G.

 (x) (x –1) = (x x–1) [ is a homomorphism]

= (e)

= 

and (x–1) (x) = (x–1x) = (e) = 

Thus, (x) (x–1) =  = (x–1) (x)

 (x–1) is the inverse of (x) in 

(x–1) = [(x)]–1

**KERNEL OF A HOMOMORPHISM:** Let G and  be two groups and let  : G  be a homomorphism. Then kernel of  denoted ker (or k) is defined as ker = {xG:(x) =}, where  is the identity of .

**THEOREM:**Let  : G be a homomorphism. Then ker is a normal subgroup of G.

**Proof:** We have ker = {xG : (x) = }. Since (e) =  so e  ker. Thus, ker is a non-empty subset of G.

**Ker is a subgroup of G:** Let x, y  ker. Then (x) =  and (y) = .

Now, (xy–1) = (x) (y–1) [ is a homomorphism]

= (x) [(y)]–1

=  []–1

=  .  =

 x y–1  ker  x, y  ker

Thus, ker is a subgroup of G.

**Ker is a normal subgroup of G:** Let k ker and xG.

Then (x k x–1) = (x) (k) (x–1)

= (x) (x–1) [ k ker  (k) = ]

= (x) (x–1)

= (x) [(x)]–1

= 

 xkx–1  ker  xG and  kker. Thus, ker is a normal subgroup of G.

**THEOREM:** Let  : G be a homomorphism. Then  is one-one if and only if ker = {e}..

**Proof:** First suppose  : G is one-one homomorphism.

Then we have to show that ker = {e}

Let x ker. Then (x) = 

(x) = (e) [(e) = ]

 x = e [ is one-one]

Thus, x ker  x = e

Hence, ker = {e}.

Conversely, suppose ker = {e}.

Then we have show that  is one-one.

Let x1 yG such that

(x) = (y)

 (x) [(y)]–1 = (y) [(y)]–1

 (x) (y–1) = 

 (xy–1) = 

 xy–1  ker

 xy–1 = e [ ker = {e}]

 xy–1y = ey

 xe = y

 x = y

Thus, f is one-one.

**THEOREM:** Let  : Gbe an onto homomorphism. Then  is an isomorphism if and only if ker = {e}.

**Proof:** Same as above theorem.

**THEOREM:** Let N be a normal subgroup of a group G. Let f : G  G/N be defined by f(x) = Nx  x G. Then f is an onto homomorphism and kerf = N.

**Proof:**

**f : G  G/N is homomorphism**: Let x, y  G.

Then f(xy) = Nxy

= Nx Ny

= f(x) f(y)

Thus, f is a homomorphism.

**f : G  G/N is onto:** Let NxG/N. Then xG and f(x) = Nx. Thus f is onto.

Hence f : G  G/N is an onto homomorphism.

Next, we have to prove that kerf = N. Let x Kerf. Then xkerf

 f(x) = N [ Identity of G/N is N]

 Nx = N

 x  N

Thus, kerf = N.

**Note:** The mapping f : G  G/N defined by f(x) = Nx  xG is called a natural mapping of G onto G/N.

**FUNDAMENTAL THEOREM OF HOMOMORPHISMS (FIRST ISOMORPHISM THEOREM):** Let f : G be an onto homomorphism with kerf = K. Then G/K  .

**Proof:** Since K = kerf is a normal subgroup of G so G/K exists.

Define  : G/K  by  (Kx) = f(x)  xG. Then

** is well-defined:** Let x, yG such that Kx = Ky.

Then Kx = Ky  Kxy–1 = Kyy–1

 Kxy–1 = Ke

 Kxy–1 = K

 xy–1  K

 f(xy–1) = 

 f(x) f(y–1) = 

 f(x) [f(y)]–1 f(y) = . f(y)

 f(x) .  = f(y)

 f(x) = f(y)

  (kx) =  (ky)

  is well-defined.

** is a homomorphism:** Let Kx, Ky  G/K.

Then  (Kx. Ky) =  (Kxy)

= f(xy)

= f(x) . f(y). [ f is homomorphism]

=  (Kx) (Ky)

  is a homomorphism.

** is one-one:** Let Kx, Ky G/K such that  (Kx) = (Ky)

 f(x) = f(y)

 f(x) [f(y)]–1 = f(y) [f(y)]–1

 f(x) f(y–1) = 

 xy–1 K

 Kxy–1 = K

 Kxy–1y = Ky

 Kxe = Ky

 Kx = Ky

  is one-one.

** is onto:** Let . Since f : G  is onto so there exists x G such that f(x) = . Now, x G  Kx G/K and  (Kx) = f(x) = 

  is onto.

Hence  : G/K  is an onto isomorphism. Thus G/K  .

**An application of fundamental theorem of homomorphism:** Let G = (R, +) be the additive group of reals and  = {z  C : |z| = 1} be the multiplicative group. Then prove that G/Z .

**Solution:** Define f : G  by f(t) = e2it  t G. Then

**f is a homomorphism:** Let t1, t2 G.

Then f(t1 + t2) = 

= 

= , 

= f(t1) . f(t2)

Thus, f is a homomorphism.

**f is onto:** Let z  . Then |z| = 1 and so z = ei,   R.

Now, R   R   G.

Also, f  = 

= ei

= z

Thus f is onto.

Hence by fundamental theorem of homomorphism  - (1)

Next, we show that kerf = Z. Let t  kerf.

Then t  kerf  f(t) = 1 + i 0

 e2 i t = 1

 cos 2 t + i sin 2 t = 1

 t  Z

Thus, kerf = Z.

From (1), we get G/Z  .

**THEOREM:** Let f : G  be an onto homomorphism with kernel H. For each subgroup  of , let K = {x G : f(x)  }

Then,

(i) K is a subgroup of G containing H.

(ii)  is a normal subgroup of  iff K is a normal subgroup of G.

**Proof:** (i) K is a subgroup of G

Let x, y K. Then f(x), f(y)   .

 f(x). [f(y)]–1 [ is a subgroup of ]

 f(x). f(y–1) 

 xy–1  K

Thus, x y–1 K  x, y K. Hence, K is a subgroup of G.

Next, we show that HK.

Let h  H (= kerf)

 h  kerf

 f(h) = 

 f(h)   [ ]

 h K

Thus, HK.

Hence K is a subgroup of G containing H.

(ii) First suppose  is normal in  Then we have to prove that K is normal in G. Let x G and k K.

Then f(x k x–1) = f(x) f(k) f(x–1)

= f(x) f(k) [f(x)]–1 -(1)

Since f(x)  f(k)  and  is normal in  so f(x) f(k) [f(x)]–1  

 f(x k x–1)  [using (1)]

 x k x–1 K

 K is normal in G.

Conversely, suppose K is normal in G. Then we have to prove that  is normal in 

Let y  and . Then y = f(x) for some x G and  == f(k) for some k K.

Now, y  y –1 = f(x) f(k) [f(x)]–1

= f(x) f(k) f(x–1)

= f(x k x–1) -(2)

Since K is normal in G so x k x–1 K.

 f(x k x–1) 

 y y–1  [using (2)]

  is a normal subgroup of .

**THEOREM (SECOND ISOMORPHISM THEOREM):** Let f : G  be an onto homomorphism. For each normal subgroup  of , let K = {x G: f(x) }.

Then G/K .

**Proof:** Since  is a normal subgroup of  so K is a normal subgroup of G. Thus, G/K and  exist. Define  : G by (x) =  f(x)  xG. Then

** is a homomorphism:** Let a, b G.

Then (ab) = f(ab)

= f(a) f(b)

= [f(a)] [f(b)]

= (a) (b)

Thus  is a homomorphism.

** : G is onto:** Let . Then . Since f : G is onto so there exist xG such that f(x) = . Thus (x) = f(x) = 

Hence  is onto. Thus, by fundamental theorem of homomorphism.

 -(1)

Next, we show that ker = K.

Let x  ker.

Then x  ker  (x) =  [  is the identity of ]

 f(x) = 

 f(x) 

 x K

Thus, ker = K.

From (1), we have G/K  /

**Theorem:** Any finite cyclic group of order n is isomorphic to the additive group of integers molulo-n.

**Proof:** Let G = {a0, a1, a2, …. an – 1} be a finite cyclic group of order n-generated by a.

Let  = {0, 1, 2, 3, …., n – 1} be the group of integers under addition modulo-n.

Define  : G by

 (ak) = k  ak G.

** is a homomorphism:** Let ar, as G.

Then  (ar, as) =  (ar + s)

= 

= 

= [(an) = (e) = 0]

=

 is a homomorphism.

** is one-one:** Let ar, as G.

Then 

 r = s

 ar = as   is one-one.

** is onto:** Let m.

Then am  G and  (am) = m

  is onto.

Thus,  G  is an onto isomorphism.

Hence G .

**Theorem:** Any cyclic group of order n is isomorphic to the additive group of residue class modulo n.

**Solution:** Let G = (a) be a finite cyclic group of order n generated by a and  = {[0], [1], [2], …, [n – 1]} be the group of residue class molulo n.

Define f : G  by f(ai) = [i]  ai  G, 0  i < n

**f is a homomorphism:** Let x, y  G. Then x = ai and y = aj

 f(xy) = f(ai aj) = f(ai + j)

= [i + j] = [i] + [j]

= f(ai) + f(aj) = f(x) + f(y)

 f is a homomorphism.

**f is one-one:** Let x, y G.

Then x = ai and y = aj

 f(x) = f(y)

 f(ai) = f(aj)

 [i] = [j]

 i = j (mod n)

 n divides i – j

But 0  i, j < n

 i - j = 0  i = j

 ai = aj  x = y  f is one-one

f is onto: Let [i]  . Then there exists ai G such that f(ai) = [i]  f is onto.

Hence f : G is an onto isomorphism. Thus G .

**THEOREM:** Any finite cyclic group of order n is isomorphic to the quotient group Z/<n>.

**Proof:** Let G = <a> be a finite cyclic group of order n generated by a.

Then o (a) = n.

Define a function f : Z  G by f(n) = an nZ

**f is homomorphism:** Let n1, n2 Z. Then f(n1 + n2) =  =   = f(n1) f(n2).

 f is a homomorphism.

**f is onto:** Let an G. Then nZ and f(n) = an.

 f is onto.

Thus f : Z G is an onto isomorphism and so by fundamental theorem of homomorphism

G Z/kerf

Now mkerf  f(m) = e

 am = e

 n/m [ o (a) = n]

 m = nq for some integer q

 m  <n>

Thus kerf = <n> and so G  Z/<n>

**EXERCISE**

1. Let Z be the group of all integers under addition and let G = {2n : n Z} be group under multiplication. Define a map f : Z  G by f(x) = 2n for all n Z. Then show that f is an onto isomorphism and kerf = {0}.

2. Prove that every homomorphic image of an abelian group is an abelian group but the converse may not be true.

3. Let f : G be a homomorphism and let H be a subgroup of G. Then show that f(H) is a subgroup of .

4. Let f : G be a group homomorphism. Then show that f(G) is a subgroup of .

5. Let G be a group and a be a fixed element of G. Define fa : G  G by fa (x) = ax a–1 for all x  G. Then prove that f is an isomorphism of G onto itself.

6. Prove that the relation of “being isomorphic to” on a collection of groups is an equivalence relation.

7. Let f : G  be an isomorphism. Then show that the order of an element a  G is equal to the order of its image f(a).

8. Prove that any infinite cyclic group is isomorphic to the group Z of integers under addition.