DISCRETE STRUCTURE

LECTURE-19

HOMOMORPHISM, ISOMORPHISM & AUTOMORPHISM

Topics covered

- Homomorphism
- Isomorphism
- Automorphism

Isomorphism

- Two groups are isomorphic if there is a bijection of one onto the other which preserves the group operations i.e.

if $\langle G_1, \bullet \rangle$ and $\langle G_2, * \rangle$ are groups then a bijection $f : G_1 \to G_2$ is an isomorphism provided

$$\forall x, y \in G_1 \; f(x \bullet y) = f(x) * f(y)$$

Example: Consider the group of matrices of the form $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ where $t \in R$ under matrix multiplication. This is isomorphic to the group $\langle R, + \rangle$

The mapping is $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \to t$

An isomorphism from a group onto itself is called an automorphism.

HOMOMORPHISMS

The idea of isomorphic algebraic structures can be readily generalised by dropping the requirement that the functional mapping be a bijection.

Let $\langle A, \bullet \rangle$ and $\langle B, * \rangle$ be two algebraic systems then a *homomorphism* from $\langle A, \bullet \rangle$ to $\langle B, * \rangle$ is a functional mapping $f : A \to B$ such that

$$\forall x, y \in A \; f(x \bullet y) = f(x) * f(y)$$

Example: consider the two structures

$\bullet$	α	β	γ	δ	ε	ζ
α	α	β	α	α	γ	δ
β	β	α	γ	β	γ	ε
γ	α	γ	α	β	γ	ε
δ	α	β	β	δ	ε	ζ
ε	γ	γ	γ	ε	ε	ζ
ζ	δ	ε	ε	ζ	ζ	ζ

$*$	1	0	–1
1	1	1	0
0	1	0	–1
–1	0	–1	–1

then f such that $f(\alpha) = 1, f(\beta) = 1, f(\gamma) = 1, f(\delta) = 0$ $f(\varepsilon) = 0, f(\zeta) = -1$ is a homomorphism between $\langle \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}, \bullet \rangle$ and $\langle \{1, 0, -1\}, * \rangle$

HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF SEMIGROUPS

- **6 Homomorphism :** Let (S, .) and (T, . ’) be two semigroups. An everywhere defined function
- f : S□T is called a homomorphism from (S, .) to (T, . ’) if
- f(a .b) = f(a) . ’f(b) a, b . S
- **Isomorphism :** Let (S, .) and (T, .’) be two semigroups. A function
- f : S . T is called a isomorphism from (S, ..) to (T, .’) if
- (i) it is one-to-one correspondence from S to T (ii) f(a .b) = f (a)
- .’f (b) . a, b . S
- (S, .) and (T, . ’) are isomorphic’ is denoted by s…T .
- **Automorphism :** An isomorphism from a semigroup to itself is called an automorphism of the semigoup. An isonorptism f:.s…s is called automorphism.

HOMOMORPHISM, LSOMORPHISM AND AUTOMORNHISM OF MONOIDS

- **Homomorphism :** Let (M, .) and (M', .') be two monoids. An everywhere defined function f : M ..M' is called a homomorphism from
- (M, .) to (M', .) if
- f (a .b) = f(a) . 'f(b) . a, b . M
- **Isomorphism :** Let (M, .) and (M', . ') be two monoids. A function
- f : M . M' is called a isomorphism from (M, □.) to (M', .') if
- (i) it is one-to-one correspondence from M to M' (ii) f is onto.
- (iii) f(a .b = f (a) . 'f (b) . a, b.M
- '(M .) and (M', . ') are isomorphic is denoted by M .M'.
- **Automorphism :** An isomorphism from a monoid to itself is called an automorphism of the monoid. An isomorphism f:.M…M is called Automorphism of monoid.

HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF GROUPS

- **Homomorphism :** Let (G, .) and (G’, . ’) be two groups. An everywhere
- defined function f : G . G’ is called a homomorphism from (G, .) to (G’,.’) if
- f (a .b) = f (a) . ’f (b) . a, b .G
- **Isomorphism :** Let (G, .) and (G’, . ’) be two groups. A function
- f : G.G’ is called a isomorphism from (G, .) to (G’, .’) if
- (i) it is one-to-one correspondence from G to G’ (ii) f is onto.
- (iii) f(a .b) = f (a) . ’f (b) . a, b.G
- ‘(G, .) and (G’, .’) are isomorphic’ is denoted by G .G’.
- **Automorahism:** An isomorphism from a group to itself is called an automorphism of the group. An isomorphism f:.G…G is called Automorphism.

- **Theorem 1 :** Let (S, .) and (T, .') be monoids with identity e and e',
- respectively. Let f : S . T be an isomorphism. Then f(e) = e'.
- **Proof :** Let b be any element of T. Since f is on to, there is an element a in
- S such that f(a) = b
- Then *a . a . e*
- *b* . *f* (*a*) . *f* (*a* . *e*) .*f* (*a*) . *f* (*e*) . *b* .' *f* (*e*) (f is isomorphism)
- Similarly, since *a* . *e* . *a* ,
- *b* . *f* (*a*) . *f* (*e* . *a*) *f* (*e** *a*)… *f* (*e*) . '..*a*.
- Thus for any ,b.T,
- *b* . *b* . ' *f* (*e*) . *f* (*e*) . '*b*
- which means that f(e) is an identity for T.
- Thus since the identity is unique, it follows that f(e)=e'

- **Theorem 6.6 :** Let f be a homomorphism from a semigroup (S, .) to a
- semigroup (T, .’). If S’ is a subsemigroup of (S, .), then
- F(S’) = {t . T | t = f (s) for some s . S},
- The image of S’ under f, is subsemigroup of (T, . ’).
- **Proof :** If t1, and t2 are any elements of F(S’), then there exist s1 and s2 in
- S’ with
- t l= f(s1) and t2 = f(s2).
- Therefore,
- *t*1 .*t*2 . *f* (*s*1) .*f* (*s*2) . *f* (*s*1 . *s*2) . *f* (*s*2 . *s*1) . *f* (*s*2) . *f* (*s*1) . *t*2 .*t*1
- Hence (T, . ') is also commutative.

Application & Scope of research

- Theoretical Computer Science