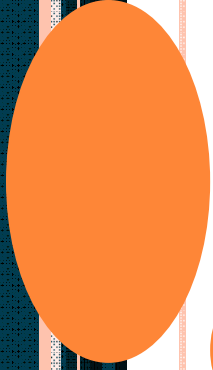
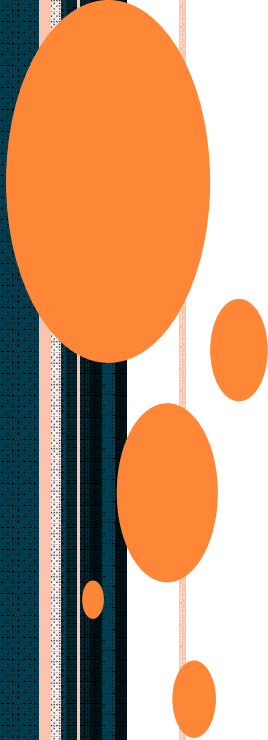


DISCRETE STRUCTURE



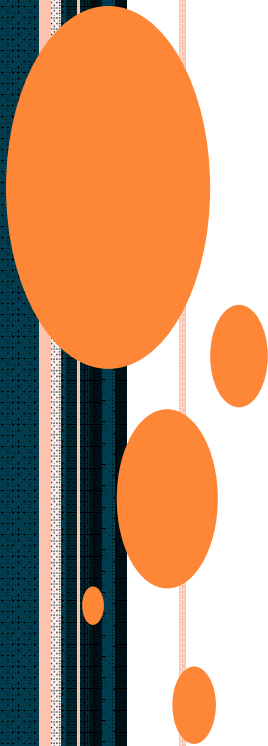
LECTURE-19

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 $f : G_1 \rightarrow G_2$ is an isomorphism provided

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

Example: Consider the group of matrices of the form $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ where $t \in \mathbb{R}$ under matrix

multiplication. This is isomorphic to the group $\langle \mathbb{R}, + \rangle$

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

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 $f : A \rightarrow B$ such that

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

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, \cdot) and (T, \cdot') be two semigroups. An everywhere defined function
- $f : S \rightarrow T$ is called a homomorphism from (S, \cdot) to (T, \cdot') if
- $f(a \cdot b) = f(a) \cdot' f(b) \quad a, b \in S$
- **Isomorphism** : Let (S, \cdot) and (T, \cdot') be two semigroups. A function
- $f : S \rightarrow T$ is called a isomorphism from (S, \cdot) to (T, \cdot') if
- (i) it is one-to-one correspondence from S to T (ii)
- $f(a \cdot b) = f(a) \cdot' f(b) \quad a, b \in S$
- (S, \cdot) and (T, \cdot') are isomorphic' is denoted by $S \cong T$.
- **Automorphism** : An isomorphism from a semigroup to itself is called an automorphism of the semigroup. An isomorphism $f : S \rightarrow S$ is called automorphism.



HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF MONOIDS

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



HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF GROUPS

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



- **Theorem 1** : Let (S, \cdot) and (T, \cdot') be monoids with identity e and e' ,
- respectively. Let $f : S \rightarrow T$ be an isomorphism. Then $f(e) = e'$.
- **Proof** : Let b be any element of T . Since f is onto, there is an element a in
- S such that $f(a) = b$
- Then $a \cdot a \cdot e$
- $b \cdot f(a) \cdot f(a \cdot e) \cdot f(a) \cdot f(e) \cdot b \cdot f(e)$ (f is isomorphism)
- Similarly, since $a \cdot e \cdot a$,
- $b \cdot f(a) \cdot f(e \cdot a) \cdot f(e \cdot a) \dots f(e) \cdot f(a)$.
- Thus for any $b \in T$,
- $b \cdot f(e) \cdot f(e) \cdot b$
- 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, \cdot) to a
- semigroup (T, \cdot') . If S' is a subsemigroup of (S, \cdot) , then
- $F(S') = \{t \in T \mid t = f(s) \text{ for some } s \in S'\}$,
- The image of S' under f , is subsemigroup of (T, \cdot') .
- **Proof** : If t_1 , and t_2 are any elements of $F(S')$, then there exist s_1 and s_2 in
- S' with
- $t_1 = f(s_1)$ and $t_2 = f(s_2)$.
- Therefore,
- $t_1 \cdot' t_2 = f(s_1) \cdot' f(s_2) = f(s_1 \cdot s_2) = f(s_2 \cdot s_1) = f(s_2) \cdot' f(s_1) = t_2 \cdot' t_1$
- Hence (T, \cdot') is also commutative.



APPLICATION & SCOPE OF RESEARCH

- Theoretical Computer Science

