DISCRETE MATHEMATICS

SUBMITTED BY
KOMAL
APPLIED SCIENCE

Introduction

- Discrete Mathematics is the part of Mathematics devoted to study of

  Discrete (Disinct or not connected objects)
- Discrete Mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous .
- As we know Discrete Mathematics is a

  backbone of mathematics and

  computer science

Scope

- It Develops our Mathematical Thinking
- It Improves our problem solving abilities
- Many Problems can be solved using Discrete mathematics
- For eg .
  - Sorting the list of Integers
  - Finding the shortest path from home to any destination
  - Drawing a garph within two conditions
    - We are not allowed to lift your pen.
    - We are not allowed to repeat edges

Algebraic Structures

- Algebraic systems Examples and general properties
- Semi groups
- Monoids
- Groups
- Sub groups

Algebraic systems

- **N = {1,2,3,4,…..$\propto$ } = Set of all natural numbers.**
  Z = { 0, ± 1, ± 2, ± 3, ± 4 , ….. $\propto$} = Set of all integers.
  Q = Set of all rational numbers.
  R = Set of all real numbers.
- **Binary Operation:** The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if
  $a * b \in A$ for all $a, b \in A$ (Closure property).
  Ex: The set N is closed with respect to addition and multiplication but not w.r.t subtraction and division.
- **Algebraic System:** A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.
  Ex: (N, +), (Z, +, $-$), (R, +, . , $-$) are algebraic systems.

Properties

- **Commutative:** Let * be a binary operation on a set A.

  The operation * is said to be commutative in A if

  $a * b = b * a$ for all a, b in A
- **Associativity:** Let * be a binary operation on a set A.

  The operation * is said to be associative in A if

  $(a * b) * c = a * (b * c)$ for all a, b, c in A
- **Identity:** For an algebraic system (A, *), an element 'e' in A is said to be an identity element of A if

  $a * e = e * a = a$ for all $a \in A$.
- **Note:** For an algebraic system (A, *), the identity element, if exists, is unique.
- **Inverse:** Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if

  $a * b = b * a = e$

Semi group

- **Semi Group:** An algebraic system (A, *) is said to be a semi group if
  1. * is closed operation on A.
  2. * is an associative operation, for all a, b, c in A.
- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.
- Ex. (N, –) is not a semi group.

- **Monoid:** An algebraic system (A, *) is said to be a **monoid** if the following conditions are satisfied.
  1) * is a closed operation in A.
  2) * is an associative operation in A.
  3) There is an identity in A.

Subsemigroup & submonoid

Subsemigroup : Let (S, *) be a semigroup and let T be a subset of S. If T is closed under operation * , then (T, *) is called a subsemigroup of (S, *).

Ex: (N, .) is semigroup and T is set of multiples of positive integer m then (T,.) is a sub semigroup.

Submonoid : Let (S, *) be a monoid with identity e, and let T be a non- empty subset of S. If T is closed under the operation * and e $\in$ T, then (T, *) is called a submonoid of (S, *).

Group

- **Group:** An algebraic system (G, *) is said to be a **group** if the following conditions are satisfied.

  1) * is a closed operation.
  2) * is an associative operation.
  3) There is an identity in G.
  4) Every element in G has inverse in G.

- **Abelian group (Commutative group):** A group (G, *) is said to be ***abelian*** (or ***commutative)*** if

  $$a * b = b * a \quad .$$

Theorem

- In a Group (G, *) the following properties hold good

1. Identity element is unique.
2. Inverse of an element is unique.
3. Cancellation laws hold good

$a * b = a * c \Rightarrow b = c$ (left cancellation law)

$a * c = b * c \Rightarrow a = b$ (Right cancellation law)

4. $(a * b)^{-1} = b^{-1} * a^{-1}$

- In a group, the identity element is its own inverse.

- ***Order of a group*** : The number of elements in a group is called order of the group.

- Finite group: If the order of a group G is finite, then G is called a finite group.

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .

- Solution: Let R^* = set of all non zero real numbers.

  Let a, b, c are any three elements of R^* .

1. Closure property : We know that, product of two nonzero real numbers is again a nonzero real number .

   i.e., $a . b \in R^*$ for all $a,b \in R^*$.

2. Associativity: We know that multiplication of real numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in R^*$.

3. Identity : We have $1 \in R^*$ and $a .1 = a$ for all $a \in R^*$.

   $\therefore$ Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in R^*$, we have $1/a \in R^*$ such that

   $a .(1/a) = 1$ i.e., Each element in R^* has an inverse.

Contd.,

- 5.Commutativity: We know that multiplication of real numbers is commutative.

  i.e., $a \cdot b = b \cdot a$ for all $a,b \in R^*$.

  Hence, $(R^*, \cdot)$ is an abelian group.

- Ex: Show that set of all real numbers 'R' is not a group with respect to multiplication.
- Solution: We have $0 \in R$.

  The multiplicative inverse of 0 does not exist.

  Hence. R is not a group.

Example

- Ex. Let (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by $n * m$ = maximum of (n, m).

  Show that (Z, *) is a semi group.

  Is (Z, *) a monoid ?. Justify your answer.
- Solution: Let a , b and c are any three integers.

Closure property: Now, $a * b$ = maximum of (a, b) $\in Z$ for all a,b $\in Z$

Associativity : $(a * b) * c$ = maximum of {a,b,c} = $a * (b * c)$

$\therefore$ (Z, *) is a semi group.

Identity : There is no integer x such that

$a * x$ = maximum of (a, x) = a for all a $\in Z$

$\therefore$ Identity element does not exist. Hence, (Z, *) is not a monoid.

Ex. Show that the set of all positive rational numbers forms an abelian group under the composition * defined by

$a * b = (ab)/2$.

- Solution: Let A = set of all positive rational numbers.

Let a,b,c be any three elements of A.

1. Closure property: We know that, Product of two positive rational numbers is again a rational number.

i.e., $a * b \in A$ for all $a, b \in A$.

2. Associativity: $(a*b)*c = (ab/2) * c = (abc) / 4$

$a*(b*c) = a * (bc/2) = (abc) / 4$

3. Identity : Let e be the identity element.

We have $a*e = (a\,e)/2$ ...(1) , By the definition of *

again, $a*e = a$ .....(2) , Since e is the identity.

From (1)and (2), $(a\,e)/2 = a \Rightarrow e = 2$ and $2 \in A$.

$\therefore$ Identity element exists, and '2' is the identity element in A.

Contd.,

- 4. <u>Inverse:</u> Let $a \in A$

  let us suppose b is inverse of a.

  Now, $a * b = (a\ b)/2$ ….(1) (By definition of inverse.)

  Again, $a * b = e = 2$ …..(2) (By definition of inverse)

  From (1) and (2), it follows that

  $(a\ b)/2 = 2$

  $\Rightarrow$ $b = (4 / a) \in A$

$\therefore$ (A ,*) is a group.

- Commutativity: $a * b = (ab/2) = (ba/2) = b * a$
- Hence, (A,*) is an abelian group.

Theorem

- Ex. In a group $(G, *)$, Prove that the identity element is unique.
- Proof :

a) Let e_1 and e_2 are two identity elements in G.

Now, $e_1 * e_2 = e_1$ ...(1) (since e_2 is the identity)

Again, $e_1 * e_2 = e_2$ ...(2) (since e_1 is the identity)

From (1) and (2), we have $e_1 = e_2$

$\therefore$ Identity element in a group is unique.

Theorem

- Ex. In a group (G, *) , Prove that the inverse of any element is unique.
- <u>Proof</u>:
- Let a ,b,c $\in$G and e is the identity in G.
- Let us suppose, Both b and c are inverse elements of a .
- Now, a * b = e ...(1) (Since, b is inverse of a)
- Again, a * c = e ...(2) (Since, c is also inverse of a)
- From (1) and (2), we have
- a * b = a * c
- $\Rightarrow$ b = c (By left cancellation law)
- In a group, the inverse of any element is unique.

Theorem

- Ex. In a group (G, *) , Prove that
  $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a,b \in G$.
- <u>Proof :</u>
- Consider,
- $(a * b) * (b^{-1} * a^{-1})$
- $= (a * (b * b^{-1}) * a^{-1})$ (By associative property).
- $= (a * e * a^{-1})$ (By inverse property)
- $= (a * a^{-1})$ (Since, e is identity)
- $= e$ (By inverse property)
- Similarly, we can show that
- $(b^{-1} * a^{-1}) * (a * b) = e$
- Hence, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Ex. If $(G, *)$ is a group and $a \in G$ such that $a * a = a$, then show that $a = e$, where e is identity element in G.

- Proof: Given that, $a * a = a$
- $\Rightarrow a * a = a * e$ (Since, e is identity in G)
- $\Rightarrow a = e$ (By left cancellation law)
- Hence, the result follows.

Ex. If every element of a group is its own inverse, then show that the group must be abelian .

- Proof: Let (G, *) be a group.
- Let a and b are any two elements of G.
- Consider the identity,
- $(a * b)^{-1} = b^{-1} * a^{-1}$
- $\Rightarrow$ $(a * b) = b * a$ (Since each element of G is its own
- inverse)
- Hence, G is abelian.

Ex. Show that G = {1, –1, i, –i } is an abelian group under multiplication.

- Solution: The composition table of G is

.	1	–1	i	-i
1	1	-1	i	- i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.
3. Identity : Here, 1 is the identity element and $1 \in G$.

Contd.,

- 4. Inverse: From the composition table, we see that the inverse elements of

  1 -1, i, -i are 1, -1, -i, i respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative. Hence, (G, .) is an abelian group.

Sub groups

- Def. A non empty sub set H of a group (G, *) is a sub group of G,
- if (H, *) is a group.

Note: For any group {G, *}, {e, * } and (G, *) are trivial sub groups.

- Ex. G = {1, -1, i, -i } is a group w.r.t multiplication.

  H_1 = { 1, -1 } is a subgroup of G .

  H_2 = { 1 } is a trivial subgroup of G.
- Ex. (Z , +) and (Q , +) are sub groups of the group (R +).
- Theorem: A non empty sub set H of a group (G, *) is a sub group of G iff
- i) $a * b \in H \quad \forall\, a, b \in H$
- ii) $a^{-1} \in H \quad \forall\, a \in H$

Theorem

- Theorem: A necessary and sufficient condition for a non empty subset H of a group (G, *) to be a sub group is that

  $a \in H,\ b \in H \Rightarrow a * b^{-1} \in H.$
- Proof: Case1: Let (G, *) be a group and H is a subgroup of G

  Let $a,b \in H \Rightarrow b^{-1} \in H$ (since H is is a group)

  $\Rightarrow a * b^{-1} \in H.$ (By closure property in H)
- Case2: Let H be a non empty set of a group (G, *).

  Let $a * b^{-1} \in H \quad \forall\, a, b \in H$
- Now, $a * a^{-1} \in H$ (Taking $b = a$)

  $\Rightarrow e \in H$ i.e., identity exists in H.
- Now, $e \in H,\ a \in H \Rightarrow e * a^{-1} \in H$

  $\Rightarrow a^{-1} \in H$

Contd.,

- $\therefore$ Each element of H has inverse in H.

  Further, $a \in H,\ b \in H \Rightarrow a \in H,\ b^{-1} \in H$

  $\Rightarrow a * (b^{-1})^{-1} \in H.$

  $\Rightarrow a * b \in H.$

  $\therefore$ H is closed w.r.t $*$.
- Finally, Let $a,b,c \in H$

  $\Rightarrow a,b,c \in G$ (since $H \subseteq G$)

  $\Rightarrow (a * b) * c = a * (b * c)$

  $\therefore$ $*$ is associative in H
- Hence, H is a subgroup of G.

Homomorphism and Isomorphism.

- **Homomorphism :** Consider the groups $(G, *)$ and $(G^1, \oplus)$

  A function $f : G \rightarrow G^1$ is called a homomorphism if

  $$f(a * b) = f(a) \oplus f(b)$$

- **Isomorphism** : If a homomorphism $f : G \rightarrow G^1$ is a bijection then f is called isomorphism between G and G^1 .

  Then we write $G \equiv G^1$

Cosets

- If H is a sub group of(G, *) and a $\in$ G then the set
  Ha = { h * a | h $\in$ H}is called a right coset of H in G.

Similarly aH = {a * h | h $\in$ H}is called a left coset of H is G.

- ***Note:-*** 1) Any two left (right) cosets of H in G are either identical or disjoint.
- 2) Let H be a sub group of G. Then the right cosets of H form a partition of G. i.e., the union of all right cosets of a sub group H is equal to G.

  3) <u>Lagrange's theorem</u>: The order of each sub group of a finite group is a divisor of the order of the group.
- 4) The order of every element of a finite group is a divisor of the order of the group.
- 5) The converse of the lagrange's theorem need not be true.

State and prove Lagrange's Theorem

- Lagrange's theorem: The order of each sub group H of a finite group G is a divisor of the order of the group.
- Proof: Since G is finite group, H is finite.
- Therefore, the number of cosets of H in G is finite.
- Let $Ha_1, Ha_2, \ldots, Ha_r$ be the distinct right cosets of H in G.
- Then, $G = Ha_1 \cup Ha_2 \cup \ldots, \cup Ha_r$
- So that $O(G) = O(Ha_1)+O(Ha_2) \ldots + O(Ha_r)$.
- But, $O(Ha_1) = O(Ha_2) = \ldots.. = O(Ha_r) = O(H)$
- $\therefore$ $O(G) = O(H)+O(H) \ldots + O(H)$. (r terms)
- $= r \, . \, O(H)$
- This shows that O(H) divides O(G).

THANK YOU