Algebraic Structures

UNIT-2

Discrete Structures

B.Tech (CS, DS)
IIIrd Sem

ANAMIKA TIWARI
Assistant Professor
CSET

Content

- Course Objective
- Course Outcome
- CO-PO Mapping
- Syllabus
- Prerequisite and Recap
- Definition
- Operation
- Groups, Subgroups and order,
- Cyclic Groups, Cosets,
- Lagrange's theorem,
- Normal Subgroups, Permutation and Symmetric Groups, Group Homomorphisms,
- Rings, Internal Domains,
- Fields.

Content

- Video links
- Daily Quiz
- Weekly Assignment
- MCQ
- Old Question papers
- Expected Question for University Exam
- Summary
- References

Course Objective

- The subject enhances one’s ability to develop logical thinking and ability to problem solving.

- The objective of discrete structure is to enables students to formulate problems precisely, solve the problems, apply formal proofs techniques and explain their reasoning clearly.

Course Outcome

Course Outcome (CO)	At the end of course , the student will be able to	Bloom’s Knowledge Level (KL)
CO1	Apply the basic principles of sets, relations & functions and mathematical induction in computer science & engineering related problems	K3
CO2	Understand the algebraic structures and its properties to solve complex problems	K2
CO3	Describe lattices and its types and apply Boolean algebra to simplify digital circuit.	K2,K3
CO4	Infer the validity of statements and construct proofs using predicate logic formulas.	K3,K5
CO5	Design and use the non-linear data structure like tree and graphs to solve real world problems.	K3,K6

Syllabus

- **UNIT-I Set Theory, Relation, Function**

Set Theory: Introduction to Sets and Elements, Types of sets, Venn Diagrams, Set Operations, Multisets, Ordered pairs. Proofs of some general Identities on sets.

Relations: Definition, Operations on relations, Pictorial Representatives of Relations, Properties of relations, Composite Relations, Recursive definition of relation, Order of relations.

Functions: Definition, Classification of functions, Operations on functions, Growth of Functions. ***Combinatorics*****:** Introduction, basic counting Techniques, Pigeonhole Principle.

Recurrence Relation & Generating function: Recursive definition of functions, Recursive Algorithms, Method of solving Recurrences.

Proof techniques: Mathematical Induction, Proof by Contradiction, Proof by Cases, Direct Proof

- **UNIT-II Algebraic Structures**

Algebraic Structures: Definition, Operation, Groups, Subgroups and order, Cyclic Groups, Cosets, Lagrange's theorem, Normal Subgroups, Permutation and Symmetric Groups, Group Homomorphisms, Rings, Internal Domains, and Fields.

Syllabus

- **UNIT-III Lattices and Boolean Algebra**

  Ordered set, Posets, Hasse Diagram of partially ordered set, Lattices: Introduction, Isomorphic Ordered set, Well ordered set, Properties of Lattices, Bounded and Complemented Lattices, Distributive Lattices. Boolean Algebra: Introduction, Axioms and Theorems of Boolean Algebra, Algebraic Manipulation of Boolean Expressions, Simplification of Boolean Functions.

- **UNIT-IV Logics**

  Introduction, Propositions and Compound Statements, Basic Logical Operations, Wellformed formula, Truth Tables, Tautology, Satisfiability, Contradiction, Algebra of Proposition, Theory of Inference.

Syllabus

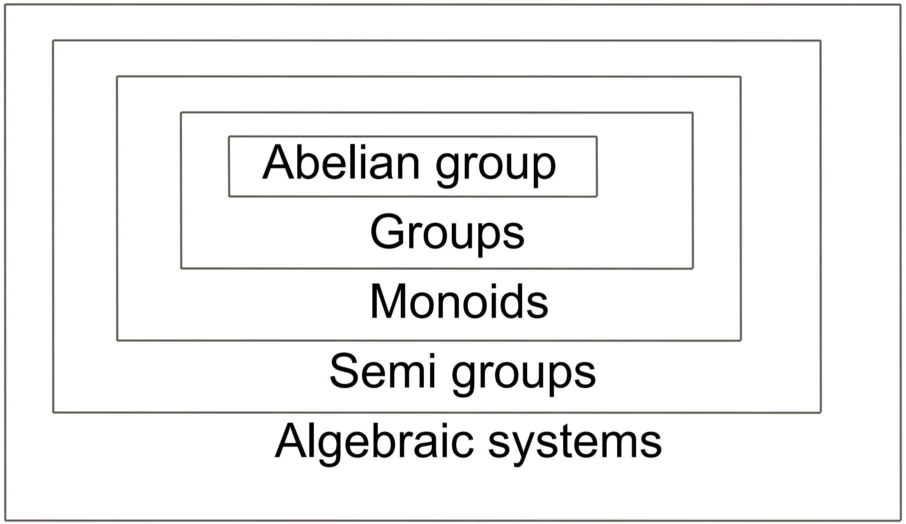
Predicate Logic: First order predicate, Well-formed formula of Predicate, Quantifiers, Inference Theory of Predicate Logic.

- **UNIT-V Tree and Graph**

  Trees: Definition, Binary tree, Complete and Extended Binary Trees, Binary Tree Traversal, Binary Search Tree.

  Graphs: Definition and terminology, Representation of Graphs, Various types of Graphs, Connectivity, Isomorphism and Homeomorphism of Graphs, Euler and Hamiltonian Paths, Graph Coloring

Algebraic structure(CO2)



Algebraic Structures(CO2)

- Algebraic Structures: A non empty set S is called algebraic structure wrt binary operations *, if (a * b) S, for all a,b S.
- Here * is closure operations on S
- Ex: (N, +),
- (Z, +, –)
- (R, +, . , –) are algebraic structures

Operations(CO2)

- 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

Algebraic structures(CO2)

- **Groupoid:** Let operation * is binary operation on set G and satisfies the closure property then the algebraic structure (G,*) is called groupoid.
- **Semi Group:** An algebraic structure (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, +) ,(z,+) are semi group.

  Ex. (N, .), (z, .) are semi group.

  Ex. (N, –) , (z, -) are not semi group.
- **Monoid:** An algebraic structure (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.

Monoid Example(CO2)

Ex. Show that the set 'N' is a monoid with respect to multiplication.

<u>**Solution**</u>**:** Here, N = {1,2,3,4,……}

1. <u>Closure property</u> : We know that product of two natural numbers is again a natural number.

   i.e., a.b = b.a for all a,b belongs to N

   Multiplication is a closed operation.

2. <u>Associativity</u> : Multiplication of natural numbers is associative.

   i.e., (a.b).c = a.(b.c) for all a,b,c belongs to N

3. <u>Identity</u> : We have, 1 belongs to N such that

   a.1 = 1.a = a for all a belongs to N.

   Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Group and Abelian group(CO2)

- **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

$$a * b = b * a \qquad a, b \;\; G.$$

Example of Abelian group(CO2)

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

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

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 $1 \in G$.
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.

Example of Abelian group(CO2)

The composition table of G is

.	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

G = {1, ω, ω^2} is an abelian group under multiplication. Where 1, ω, ω^2 are cube roots of unity. (CO2)

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 $1 \in G$.
4. Inverse: From the composition table, we see that the inverse elements of 1 ω, ω^2 are 1, ω^2, ω respectively.

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication.

Sub-semigroup & Sub-monoid(CO2)

Sub-semigroup : 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 even positive integers then (T,.) is a sub semigroup.

Sub-monoid : 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, *).

Sub groups(CO2)

Definition. 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 improper or trivial sub groups ,others are called proper or non trivial sub group.

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.

Sub groups(CO2)

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.

<u>Closure property</u>: Now, $a * b$ = maximum of (a, b) belongs to Z for all a,b belongs to Z

<u>Associativity</u> : $(a * b) * c$ = maximum of {a,b,c} = $a * (b * c)$ belongs to

(Z, *) is a semi group.

<u>Identity</u> : There is no integer x such that

$a * x$ = maximum of (a, x) = a for all a belongs to Z

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

Daily Quiz (CO2)

1. This is an abelian group { – 3 n : n ε Z } under?
A. division
B. subtraction
C. addition
D. multiplication

2. What is the inverse of – ı If G = { 1, -1, ı, – ı } is group under multiplication?
A. −1 **B. ı** C. 1 D. None of Above

3. The monoid is a?
A. a non-abelian group
B. groupoid
C. A group
D. a commutative group

Daily Quiz(CO2)

4. (ba)-1 =______ If a, b are elements of a group G?
A. b-1 a B. a-1 b C. b-1 a-1 **D. a-1 b-1**

5. What is an inverse of – i in the multiplicative group if {1, – 1, i , – i} is?
A. -1 B. 1 **C. I** D. None of these

6. What is the value of (a- 1 b)- 1 is in the group (G, .)?
A. b- 1a B. ab-1 C. ba-1 D. a-1b

7. What is the inverse of an if (Z,*) is a group with a*b = a+b+1 ∀ a, b ∈Z?
A. -2 B. 0 **C. -a-2** D. a-2

Daily Quiz(CO2)

8. An algebraic structure _________ is called a semigroup.
a) (P, *)
b) (Q, +, *)
c) (P, +)
d) (+, *)

9. Condition for monoid is __________
a) (a+e)=a
b) (a*e)=(a+e)
c) a=(a*(a+e)
d) (a*e)=(e*a)=a

10. A monoid is called a group if _______
a) (a*a)=a=(a+c)
b) (a*c)=(a+c)
c) (a+c)=a
d) (a*c)=(c*a)=e

11. What is the inverse of an if (Z,*) is a group with a*b = a+b+1 ∀ a, b ∈Z?
A. -2 B. 0 **C. -a-2** D. a-2

Daily Quiz(CO2)

12. A group (M,*) is said to be abelian if ___________
a) (x+y)=(y+x)
b) (x*y)=(y*x)
c) (x+y)=x
d) (y*x)=(x+y)

13. Condition for monoid is __________
a) (a+e)=a
b) (a*e)=(a+e)
c) a=(a*(a+e)
d) (a*e)=(e*a)=a

14. How many properties can be held by a group?
a) 2
b) 3
c) 5
d) 4

Daily Quiz(CO2)

15. A cyclic group is always _________

a) abelian group

b) monoid

c) semigroup

d) subgroup

16. {1, i, -i, -1} is __________

a) semigroup

b) subgroup

c) cyclic group

d) abelian group

17. A subgroup has the properties of ________

a) Closure, associative

b) Commutative, associative, closure

c) Inverse, identity, associative

d) Closure, associative, Identity, Inverse

Daily Quiz(CO2)

18. Which sentence is true?
A. Set of all matrices forms a group under multiplication
B. Set of all rational negative numbers forms a group under multiplication
C. Set of all non-singular matrices forms a group under multiplication
D. Both (b) and (c)

19. Which statement is false?
A. The set of rational integers is an abelian group under addition
B. The set of rational numbers form an abelian group under multiplication
C. The set of rational numbers is an abelian group under addition
D. None of these

20. What is the identity element In the group G = {2, 4, 6, 8) under multiplication modulo 10?
A. 5 B. 9 **C. 6** D. 12

Theorem 1(CO2)

Theorem: 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,

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

$\Rightarrow \quad (a * b) = b * a$ (Since each element of G is its own inverse)

Hence, G is abelian.

Theorem 2 (CO2)

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, $e \in H,\ a \in H \Rightarrow e * a^{-1} \in H$

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

Continue…(CO2)

$\therefore$ 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.

Theorem 3(CO2)

Theorem :In a group (G, *), if $(a * b)^2 = a^2 * b^2$ $\forall a,b \in G$ then show that G is abelian group.

Proof: Given that $(a * b)^2 = a^2 * b^2$

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

$\Rightarrow a * (b * a) * b = a * (a * b) * b$ (By associative law)

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

$\Rightarrow (b * a) = (a * b)$ (By right cancellation law)

Hence, G is abelian group.

Note: $a^2 = a * a$

$a^3 = a * a * a$ **etc.**

Modulo systems(CO2)

Addition modulo m $(+_m)$

let m is a positive integer. For any two positive integers a and b

$a +_m b = a + b$ if $a + b < m$

$a +_m b = r$ if $a + b \geq m$ where r is the remainder obtained by dividing (a+b) with m.

Multiplication modulo p $(\times_p)$

let p is a positive integer. For any two positive integers a and b

$a \times_p b = a\,b$ if $a\,b < p$

$a \times_p b = r$ if $a\,b \geq p$ where r is the remainder obtained by dividing (ab) with p.

Ex. $3 \times_5 4 = 2$, $5 \times_5 4 = 0$, $2 \times_5 2 = 4$

The set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

The composition table of G is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

1. <u>Closure property:</u> Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Continue.. (CO2)

2. Associativity: The binary operation $+_6$ is associative in G.

for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

$2 +_6 (3 +_6 4) = 2 +_6 1 = 3$

3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 0 is the identity element.

4. . Inverse: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4. 5 are 0, 5, 4, 3, 2, 1 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.

Hence, $(G, +_6)$ is an abelian group.

Multiplication Modulo ($\times_m$) (CO2)

The set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

The composition table of G is

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. <u>Closure property:</u> Since all the entries of the composition table are the elements of the given set, the set G is closed under $\times_7$.

Continue…(CO2)

2. Associativity: The binary operation $\times_7$ is associative in G.

for ex. $(2 \times_7 3) \times_7 4 = 6 \times_7 4 = 3$ and

$2 \times_7 (3 \times_7 4) = 2 \times_7 5 = 3$

3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 1 is the identity element.

4. Inverse: From the composition table, we see that the inverse elements of 1, 2, 3, 4. 5 ,6 are 1, 4, 5, 2, 5, 6 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $\times_7$ is commutative.

Hence, $(G, \times_7)$ is an abelian group.

Order(CO2)

- **Order of an element of a group:**

  Let (G, *) be a group. Let ‘a’ be an element of G. The smallest integer n such that $a^n = e$ is called order of ‘a’. If no such number exists then the order is infinite.

- **Order of group:**

  The number of elements in a group is called order of group.

- **Cyclic group:**

  Cyclic groups are groups in which every element is a power of some fixed element. A group G is called cyclic if for some element a belongs to G, every element is of the form a^n where n is some integer.

  $G = \{a^n : n$ belongs to $Z\}$

  The element a is called a generator.

Homomorphism and Isomorphism(CO2)

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 $G \equiv G^1$

Example of Homomorphic group(CO2)

Ex. Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R^+ \to R$ defined by $f(x) = \log_{10} x$ for all $x \in R$ is an isomorphism.

<u>Solution</u>: First, let us show that f is a homomorphism.

Let $a , b \in R^+$.

Now, $f(a.b) = \log_{10} (a.b)$

$= \log_{10} a + \log_{10} b$

$= f(a) + f(b)$

$\therefore$ f is an homomorphism.

Next, let us prove that f is a Bijection.

Continue…(CO2)

For any $a, b \in R^+$, Let, $f(a) = f(b)$

$$\Rightarrow \log_{10} a = \log_{10} b$$

$$\Rightarrow a = b$$

$\therefore$ f is one.to-one.

Next, take any $c \in R$.

Then $10^c \in R$ and $f(10^c) = \log_{10} 10^c = c$.

$\Rightarrow$ Every element in R has a pre image in R^+.

i.e., f is onto.

$\therefore$ f is a bijection.

Hence, f is an isomorphism.

Theorem for Homomorphism(CO2)

Theorem: Consider the groups $(G_1, *)$ and $(G_2, \oplus)$ with identity elements e_1 and e_2 respectively. If $f : G_1 \rightarrow G_2$ is a group homomorphism, then prove that

a) $f(e_1) = e_2$

b) $f(a^{-1}) = [f(a)]^{-1}$

c) If H_1 is a sub group of G_1 and $H_2 = f(H_1)$, then H_2 is a sub group of G_2.

d) If f is an isomorphism from G_1 onto G_2, then f^{-1} is an isomorphism from G_2 onto G_1.

Proof(CO2)

- a) we have in G_2,

  $e_2 \oplus f(e_1) = f(e_1)$ (since, e_2 is identity in G_2)

  $= f(e_1 * e_1)$ (since, e_1 is identity in G_1)

  $= f(e_1) \oplus f(e_1)$ (since f is a homomorphism)

  $e_2 = f(e_1)$ (By right cancellation law)

- b) For any $a \in G_1$, we have

  $f(a) \oplus f(a^{-1}) = f(a * a^{-1}) = f(e_1) = e_2$

  and $f(a^{-1}) \oplus f(a) = f(a^{-1} * a) = f(e_1) = e_2$

  $\therefore$ $f(a^{-1})$ is the inverse of $f(a)$ in G_2

  i.e., $[f(a)]^{-1} = f(a^{-1})$

Continue…(CO2)

- c) $H_2 = f(H_1)$ is the image of H_1 under f; this is a subset of G_2.

  Let $x, y \in H_2$.

  Then $x = f(a)$, $y = f(b)$ for some $a,b \in H_1$

  Since, H_1 is a subgroup of G_1, we have $a * b^{-1} \in H_1$.

  Consequently,

  $$\begin{aligned} x \oplus y^{-1} &= f(a) \oplus [f(b)]^{-1} \\ &= f(a) \oplus f(b^{-1}) \\ &= f(a * b^{-1}) \in f(H_1) = H_2 \end{aligned}$$

  Hence, H_2 is a subgroup of G_2.

Continue…(CO2)

- d) Since $f : G_1 \to G_2$ is an isomorphism, f is a bijection.

  $\therefore f^{-1} : G_2 \to G_1$ exists and is a bijection.

  Let $x, y \in G_2$. Then $x \oplus y \in G_2$

  and there exists $a, b \in G_1$ such that $x = f(a)$ and $y = f(b)$.

  $$\begin{aligned} \therefore f^{-1}(x \oplus y) &= f^{-1}(f(a) \oplus f(b)) \\ &= f^{-1}(f(a * b)) \\ &= a * b \\ &= f^{-1}(x) * f^{-1}(y) \end{aligned}$$

  This shows that $f^{-1} : G_2 \to G_1$ is an homomorphism as well.

  $\therefore f^{-1}$ is an isomorphism.

Cosets(CO2)

If H is a sub group of(G, *) and a $\in$ G then the set

$Ha = \{ h * a \mid h \in H\}$ is called a right coset of H in G.

Similarly, $aH = \{a * h \mid h \in H\}$ 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(CO2)

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, $O(Ha_1) = O(Ha_2) = \ldots\ldots = O(Ha_r) = O(H)$

$\therefore O(G) = O(H) + O(H) \ldots + O(H)$. (r terms)

$= r \cdot O(H)$

This shows that O(H) divides O(G).

Ring(CO2)

Let <R, +, .> be an algebraic structure for a nonempty set R and two binary operations + and . defined on it.

An algebraic structure (R, +, .) is called ring if the following conditions are satisfied.

- (R,+) is an abelian group
- (R, .) is a semigroup
- The operation . is *distributive* over the operation + in R.

  $a . (b + c) = (a . b) + (a . c)$

  $(a + b) . c = (a . c) + (b . c)$ for all $a, b, c \in R$.
- The operation + is *commutative* and *associative*.

  $a + b = b + a$, for all $a, b \in R$.

  $a + (b + c) = (a + b) + c$, for all $a, b, c \in R$.
- There exists the *identity element* 0 in R w.r.t. +.

  $a + 0 = 0 + a = a$, for every $a \in R$.
- Every element in R is *invertible* w.r.t. +.

  With every $a \in R$ there exists in R its inverse element, denoted by $(–a)$.

  $a + (–a) = (–a) + a = 0$.

Ring(CO2)

- The operation . is associative

  $a . (b. c) = (a . b) . c$ for all $a, b, c \in R$.

- The operation . is *distributive* over the operation + in R.

  $a . (b + c) = (a . b) + (a . c)$

  $(a + b) . c = (a . c) + (b . c)$ for all $a, b, c \in R$.

Zero ring(CO2)

The zero ring is the unique ring in which the additive identity 0 and multiplicative identity 1 coincide

- The zero ring is commutative.
- The element 0 in the zero ring is a unit, serving as its own multiplicative inverse.
- The unit group of the zero ring is the trivial group {0}.
- The element 0 in the zero ring is not a zero divisor.

Ring with Unity(CO2)

If in a ring there exist an element denoted by 1 such that $1.a=a.1$ for all $a \in R$ then R is called Ring with unity element

Examples

1. <Z, +, x>, Z is a set of integers and binary operations + and x.
2. <Q, +, x>, Q is a set of rational nos. and binary operations + and x.
3. <R, +, x>, R is a set of real nos. and binary operations + and x.

Commutative Ring(CO2)

If the operation . Is *commutative* in a ring <R, +, .>.

Examples

1. <Z, +, x>, Z is a set of integers and binary operations + and x.

2. <Q, +, x>, Q is a set of rational nos. and binary operations + and x.

3. <R, +, x>, R is a set of real nos. and binary operations + and x.

Ring without Unity(CO2)

A ring R which does not contain multiplicative identity is called a ring without unity.

Example

A = { …....-6,-4 -2,0,2,4,6……}

Finite and Infinite ring:

If number of elements in the ring R is finite then (R,+,.) is called finite ring otherwise it is called an infinite ring.

Order of ring : The number of elements in a finite ring R is called order of ring R .It is denoted by 0(R)

Invertible ring : Let (R,+,.) be ring with unity ,an element a $\in$ R is said to be invertible , if there exist an element b is called the inverse of a such that

$$a.b = b.a = 1$$

Ring with Zero divisor(CO2)

Ring with zero divisor:

If the product of non zero elements of R is zero.

a.b= 0 $\Rightarrow$ a and b are not zero

R={0,1,2,3,4,5}

$(R, +_{6,} \times_{6})$

Ring without zero divisor:

a.b= 0 $\Rightarrow$ a=0 or b=0

(z,+,x)

Example of Rings(CO2)

1) Let S = {0, 1} and the operations + and . on s be defined by the following tables:

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Show that <S, +, .> is a *commutative ring with unity*.

Example of Rings(CO2)

2) Let S = {a, b, c, d} and the operations + and . on s be defined by the following tables:

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

.	a	b	c	d
a	a	a	a	a
b	a	a	b	a
c	a	b	c	d
d	a	a	d	a

Show that <S, +, .> is a *ring*.

Field(CO2)

A **field** is a set with the two binary operations of addition and multiplication, both of which operations are :

1. commutative
2. associative
3. contain identity elements
4. contain inverse elements.

The identity element for addition is 0, and the identity element for multiplication is 1. Given x, the inverse element for addition is -x, and the multiplicative inverse element for multiplication is 1/x ($x \neq 0$). Furthermore, multiplication distributes over addition.

One example is the field of rational numbers Q, that is all numbers q such that for integers a and b, $q=a/b$ where $b \neq 0$. The definition of a field applies to this number set. We also note that the set of real numbers R is also a field (see Example 1). Since $Q \subset R$ (the rational numbers are a subset of the real numbers), we can say that Q is a ***subfield*** of R. Alternatively we can say that R is an ***extension*** of Q.

MCQs(CO2)

1. In a group there must be only __________ element.
a) 1
b) 2
c) 3
d) 5

2. _____ is the multiplicative identity of natural numbers.
a) 0
b) -1
c) 1
d) 2

3. The set of even natural numbers, {6, 8, 10, 12,..,} is closed under addition operation. Which of the following properties will it satisfy?
a) closure property
b) associative property
c) symmetric property
d) identity property

4. If (M, *) is a cyclic group of order 73, then number of generator of G is equal to ______
a) 89 b) 23 **c) 72** d) 17

MCQs(CO2)

5. A group G, ({0}, +) under addition operation satisfies which of the following properties?
a) identity, multiplicity and inverse
b) closure, associativity, inverse and identity
c) multiplicity, associativity and closure
d) inverse and closure

6. Let G be a finite group with two sub groups M & N such that |M|=56 and |N|=123. Determine the value of $|M \cap N|$.
a) 1
b) 56
c) 14
d) 78

7. Let * be the binary operation on the rational number given by a*b=a+b+ab. Which of the following property does not exist for the group?
a) closure property
b) identity property
c) symmetric property
d) associative property

MCQs(CO2)

8. Consider the binary operations on X, a*b = a+b+4, for a, b $\in$ X. It satisfies the properties of _______

a) abelian group

b) semigroup

c) multiplicative group

d) isomorphic group

9. If x * y = x + y + xy then (G, *) is _____________

a) Monoid

b) Abelian group

c) Commutative semigroup

d) Cyclic group

10. A function defined by f(x)=2*x such that f(x+y)=2x+y under the group of real numbers, then ________

a) Isomorphism exists

b) Homomorphism exists

c) Heteromorphic exists

d) Association exists

MCQs(CO2)

11. A function f:(M, $*$)→(N,×) is a homomorphism if ______

a) f(a, b) = a*b

b) f(a, b) = a/b

c) f(a, b) = f(a)+f(b)

d) f(a, b) = f(a)*f(a)

12. Condition of semigroup homomorphism should be ____________

a) f(x * x) = f(x * y)

b) f(x) = f(y)

c) f(x) * f(y) = f(y)

d) f(x * y) = f(x) * f(y)

13. The set of rational numbers form an abelian group under _________

a) Association

b) Closure

c) Multiplication

d) Addition

MCQs(CO2)

14. If F is a free semigroup on a set S, then the concatenation of two even words is ________

a) a semigroup of F
b) a subgroup of F
c) monoid of F
d) cyclic group of F

15. The set of odd and even positive integers closed under multiplication is ________
a) a free semigroup of (M, ×)
b) a subsemigroup of (M, ×)
c) a semigroup of (M, ×)
d) a subgroup of (M, ×)

16. If a * b = a such that a ∗ (b ∗ c) = a ∗ b = a and (a * b) * c = a * b = a then ________
a) * is associative
b) * is commutative
c) * is closure
d) * is abelian

Weekly Assignment

1. Let (G, *) be a group, where * is usual multiplication operation on G. Then show that for any x, y $\in$ G following equations holds: $(x^{-1})^{-1} = x$ $(xy)^{-1} = y^{-1}x^{-1}$
2. Define rings and write its properties.
3. Write the properties of Group. Show that the set(1,2,3,4,5)is not group under addition and multiplication modulo 6.
4. Define rings and fields
5. Show that (R – {1}, *) where the operation is defined as a*b = a +b –ab is an abelian group.
6. Let G = $(Z^2, +)$ be a group and let H be a subgroup of G where H = {(x, y) | x = y}. Find the left cosets of H in G. Here Z is the set of integers
7. Let u_8 = {1, 3, 5, 7} be a group with binary operation multiplication modulo 8. Find all proper subgroups of u_8.
8. Prove that (R, +, *) is a ring with zero divisors, where R is 2×2 matrix and + and * are usual addition and multiplication operations.

Faculty Video Links, Youtube & NPTEL Video Links and Online Courses Details (CO2)

Youtube/other Video Links

- https://www.youtube.com/watch?v=dQ4wU0k7JKI&list=PL0862D1A947252D20&index=35
- https://www.youtube.com/watch?v=urd468CJCcU&list=PL0862D1A947252D20&index=36
- https://www.youtube.com/watch?v=YB6CP1RUvgk&list=PL0862D1A947252D20&index=37

NEPTEL video link:

- https://nptel.ac.in/courses/111/105/111105112/

Old Question Papers

1. Define rings and write its properties.
2. Write the properties of Group. Show that the set(1,2,3,4,5)is not group under addition and multiplication modulo 6.
3. Define rings and fields.
4. Show that (R – {1}, *) where the operation is defined as a*b = a +b –ab is an abelian group.
5. Let G = (Z^2, +) be a group and let H be a subgroup of G where H = {(x, y) | x = y}. Find the left cosets of H in G. Here Z is the set of integers
6. Let (G, *) be a group, where * is usual multiplication operation on G. Then show that for any x, y $\in$ G following equations holds:$(x^{-1})^{-1} = x$ and $(xy)^{-1} = y^{-1}x^{-1}$
7. Let u_8 = {1, 3, 5, 7} be a group with binary operation multiplication modulo 8. Find all proper subgroups of u_8.
8. Prove that (R, +, *) is a ring with zero divisors, where R is 2×2 matrix and + and * are usual addition and multiplication operations.

For more Previous year Question papers:

https://drive.google.com/drive/folders/1xmt08wjuxu71WAmO9Gxj2iDQ0lQf-so1

Expected Questions for University Exam

1. Write the properties of Group. Show that the set(1,2,3,4,5)is not group under addition and multiplication modulo 6.
2. Define rings and fields.
3. Show that (R – {1}, *) where the operation is defined as a*b = a +b –ab is an abelian group.
4. Let G = (Z^2, +) be a group and let H be a subgroup of G where H = {(x, y) | x = y}. Find the left cosets of H in G. Here Z is the set of integers.
5. Show that every cyclic group is abelian.
6. Show that $G = \{1, -1, i, -i\}$ is an abelian group under multiplication.
7. If every element of a group is its own inverse, then show that the group must be abelian .
8. Show that G = {1, ω, ω^2} is an abelian group under multiplication. Where 1, ω, ω^2 are cube roots of unity.
9. If A has 4 elements B has 8 then find minimum amd maximum elements in AUB.
10. Prove that (R, +, *) is a ring with zero divisors, where R is 2×2 matrix and + and * are usual addition and multiplication operations.

Thank You