UNIT–2 : Algebraic Structures

Discrete Structure (CSIT-302) Notes

Easy Language + RGPV Exam Oriented Notes

---

1. Algebraic Structure

Definition

An **algebraic structure** is a non-empty set together with one or more operations defined on it.

It is written as:

(A,∗)(A,*)(A,∗)

Where:

- AAA = non-empty set
- ∗*∗ = binary operation

Example

(Z,+)(\mathbb{Z},+)(Z,+)

Integers with addition operation.

Binary Operation

A binary operation combines two elements of a set and gives another element of same set.

Example:

2+3=52+3=52+3=5

Properties of Algebraic Structures

---

1. Closure Property

If:

a,b∈Aa,b\in Aa,b∈A

then:

a∗b∈Aa*b\in Aa∗b∈A

Example

Integers under addition:

2+3=52+3=52+3=5

5 is also integer.

Hence closed.

---

2. Associative Property

(a∗b)∗c=a∗(b∗c)(a*b)*c=a*(b*c)(a∗b)∗c=a∗(b∗c)

Example

(2+3)+4=2+(3+4)(2+3)+4=2+(3+4)(2+3)+4=2+(3+4)

---

3. Identity Element

An element eee such that:

a∗e=e∗a=aa*e=e*a=aa∗e=e∗a=a

Example

For addition:

a+0=aa+0=aa+0=a

Hence 0 is identity.

---

4. Inverse Element

For every aaa, there exists a−1a^{-1}a−1 such that:

a∗a−1=ea*a^{-1}=ea∗a−1=e

Example

For addition:

a+(−a)=0a+(-a)=0a+(−a)=0

---

5. Commutative Property

a∗b=b∗aa*b=b*aa∗b=b∗a

Example

2+3=3+22+3=3+22+3=3+2

---

2. Semi Group

Definition

A non-empty set SSS with binary operation ∗*∗ is called semigroup if:

1. Closure property holds
2. Associative property holds

Mathematical Form

(S,∗)(S,*)(S,∗)

Example

(N,+)(\mathbb{N},+)(N,+)

Natural numbers under addition.

Verification

Closure

2+3=5∈N2+3=5\in\mathbb{N}2+3=5∈N

Associative

(2+3)+4=2+(3+4)(2+3)+4=2+(3+4)(2+3)+4=2+(3+4)

Hence semigroup.

---

3. Monoid

Definition

A semigroup with identity element is called monoid.

Conditions

1. Closure
2. Associative
3. Identity exists

Example

(Z,+)(\mathbb{Z},+)(Z,+)

Identity element:

000

Hence monoid.

---

4. Group

Definition

A non-empty set GGG with binary operation ∗*∗ is called group if:

1. Closure
2. Associative
3. Identity exists
4. Inverse exists

Example

(Z,+)(\mathbb{Z},+)(Z,+)

Verification

Closure

2+3=52+3=52+3=5

Associative

(2+3)+4=2+(3+4)(2+3)+4=2+(3+4)(2+3)+4=2+(3+4)

Identity

000

Inverse

For every aaa,

−a-a−a

exists.

Hence group.

---

5. Abelian Group

Definition

A group is called abelian if commutative property holds.

a∗b=b∗aa*b=b*aa∗b=b∗a

Example

(Z,+)(\mathbb{Z},+)(Z,+)

Since:

a+b=b+aa+b=b+aa+b=b+a

Hence abelian group.

---

6. Properties of Groups

---

1. Identity Element is Unique

A group has only one identity element.

---

2. Inverse is Unique

Each element has unique inverse.

---

3. Cancellation Law

If:

ab=acab=acab=ac

then:

b=cb=cb=c

---

7. Subgroup

Definition

A subset HHH of group GGG is subgroup if it itself forms group under same operation.

Conditions

1. Closed
2. Associative
3. Identity exists
4. Inverse exists

Example

$2\mathbb{Z}$

(even integers)

is subgroup of integers.

---

8. Cyclic Group

Definition

A group generated by single element.

Mathematical Form

$G=\langle a\rangle$

Example

$(\mathbb{Z},+)$

generated by 1.

Important Point

Every cyclic group is abelian.

---

9. Cosets

Definition

Let H be subgroup of G.

For $a\in G$,

Left coset:

$aH=\{ah:h\in H\}$

Right coset:

$Ha=\{ha:h\in H\}$

Example

Let:

$G=\mathbb{Z}$ $H=2\mathbb{Z}$

Then:

$1+H=\{\dots,-3,-1,1,3,\dots\}$

---

10. Factor Group (Quotient Group)

Definition

Set of all cosets forms factor group.

Written as:

G/HG/HG/H

Example

Integers modulo 2.

---

11. Permutation Group

Definition

A permutation is arrangement of elements.

Set of all permutations forms permutation group.

Example

For set:

{1,2}\{1,2\}{1,2}

Permutations:

(1,2),(2,1)(1,2),(2,1)(1,2),(2,1)

Symmetric Group

Group of all permutations of nnn elements.

Written:

SnS_nSn

---

12. Normal Subgroup

Definition

A subgroup NNN is normal if:

aN=NaaN=NaaN=Na

for every a∈Ga\in Ga∈G

Symbol

N◃GN\triangleleft GN◃G

Example

Every subgroup of abelian group is normal.

---

13. Homomorphism

Definition

A mapping between two groups preserving operation.

Mathematical Form

f(a∗b)=f(a)∘f(b)f(a*b)=f(a)\circ f(b)f(a∗b)=f(a)∘f(b)

Example

$f(x)=2x$

from integers to integers.

Important Properties

- Identity maps to identity
- Inverse maps to inverse

---

14. Isomorphism

Definition

A bijective homomorphism is called isomorphism.

Meaning

Two groups having same structure.

Symbol

$G \cong H$

Example

$(\mathbb{R}^+, \times) \cong (\mathbb{R},+)$

---

15. Rings

Definition

A non-empty set with two operations:

1. Addition
2. Multiplication

is called ring if:

Conditions

Under addition:

- Abelian group

Under multiplication:

- Semigroup

Distributive laws hold.

Example

$(\mathbb{Z},+,\times)$

Types of Rings

---

1. Commutative Ring

If:

ab=baab=baab=ba

---

2. Ring with Unity

Has multiplicative identity.

---

3. Integral Domain

Commutative ring with unity and no zero divisors.

---

16. Fields

Definition

A commutative ring in which every non-zero element has multiplicative inverse.

Example

(Q,+,×)(\mathbb{Q},+,\times)(Q,+,×)

Properties of Field

1. Addition forms abelian group

2. Non-zero elements form abelian group under multiplication
3. Distributive law holds

Difference Between Ring and Field

Ring	**Field**
Multiplicative inverse may not exist	Inverse exists
Example: Integers	Example: Rational numbers