Chapter 3 : Algebraic structures

W.DJELLADJ

Unit-III
Algebraic Structures

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

Algebraic systems

- **$N = \{1,2,3,4,.....\infty\}$ = Set of all natural numbers.**

  $Z = \{0, \pm 1, \pm 2, \pm 3, \pm 4, ... \infty\}$ = 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

  $a * b = b * a = e$

Exemple 1: L'addition usuelle $+$ sur sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$ est une loi associative, commutative, et elle admet 0 comme élément neutre; de plus, dans $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$ tout élément x a $-x$ comme symétrique (inverse) pour l'addition.

Dans $\mathbb{N}$, le seul élément symétrisable pour l'addition usuelle est 0.

La multiplication usuelle $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$ est une loi associative et commutative admettant 1 comme élément neutre, et dans $\mathbb{Q}^*$,$\mathbb{R}^*$ et $\mathbb{C}^*$ tout élément x a $\frac{1}{x}$ comme inverse (symétrique) pour la multiplication. L'élément 0 n'a pas d'inverse pour la multiplication usuelle $\times$.

Dans $\mathbb{Z}$, les seuls éléments inversibles pour la multiplication usuelle sont-1 et 1.

Exemple 2: L'opération $\top$ définie sur $\mathbb{Z}$ par $n \top m = -n - m$ est commutative mais non associative et n'admet pas d'élément neutre. $(0 = (1 \top 2) \top 3 \neq 1 \top (2 \top 3) = 4)$

Exemple 3: La composition $\circ$ sur $A(E, E)$, est une loi associative, admettant Id_E comme élément neutre, et les seuls éléments inversibles sont les applications bijectives. $((f \circ g) \circ h = f \circ (g \circ h)$, $f \circ Id_E = f = Id_E \circ f$, f^{-1}l'application réciproque de f est l'inverse de f pour la composition car $f \circ f^{-1} = Id_E = f^{-1} \circ f)$

La composition $\circ$ n'est pas commutative si E contient au moins deux éléments.

Exemple 4: L'intersection $\cap$ sur l'ensemble $\mathcal{P}(E)$ des parties de E est une loi associative et commutative, admettant E comme élément neutre, et le seul élément inversible est bien E. $((X \cap Y) \cap Z = X \cap (Y \cap Z)$, $X \cap E = X = E \cap X$, si $X \neq E$, on ne peut pas trouver X' vérifiant $X \cap X' = E$, ça marche seulement pour $X = E$.

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.

Monoid

- Ex. Show that the set ‘N’ is a monoid with respect to multiplication.
- Solution: Here, N = {1,2,3,4,……}

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

i.e., $a.b = b.a$ for all $a,b \in N$

$\therefore$ Multiplication is a closed operation.

2. Associativity : Multiplication of natural numbers is associative.

i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in N$

3. Identity : We have, $1 \in N$ such that

$a.1 = 1.a = a$ for all $a \in N$.

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

Hence, N is a monoid with respect to multiplication.

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

  $a * b = b * a \quad \forall a, b \in G.$

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, the set of all integers is a group with respect to addition.

- Solution: Let Z = set of all integers.

Let a, b, c are any three elements of Z.

1. Closure property : We know that, Sum of two integers is again an integer.

   i.e., $a + b \in Z$ for all $a,b \in Z$

2. Associativity: We know that addition of integers is associative.

   i.e., $(a+b)+c = a+(b+c)$ for all $a,b,c \in Z$.

3. Identity : We have $0 \in Z$ and $a + 0 = a$ for all $a \in Z$.

   $\therefore$ Identity element exists, and '0' is the identity element.

4. Inverse: To each $a \in Z$, we have $-a \in Z$ such that

   $a + (-a) = 0$

   Each element in Z has an inverse.

5. Commutativity: We know that addition of integers is commutative.

   i.e., $a + b = b + a$ for all $a,b \in Z$.

Hence, (Z , +) is an abelian 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., $a \cdot b \in R^*$ 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 $a \cdot 1 = a$ 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

   $a \cdot (1/a) = 1$ 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.

- 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.
- Proof:
- 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.

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: 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)

Exemple 5: $(n\mathbb{Z}, +)$ (où $n \in \mathbb{Z}$) est un sous groupe de $(\mathbb{Z}, +)$.(l'élément neutre $0 \in n\mathbb{Z}$, et pour tous $m, m' \in n\mathbb{Z}$, on $m + (-m') \in n\mathbb{Z}$).

Homomorphism and Isomorphism.

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

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

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

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

  Then we write $G \equiv G^1$

Example

- 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 $f(x) = 2^x$ for all $x \in R$ is an isomorphism.
- Solution: First, let us show that f is a homomorphism.
- Let $a , b \in R$.
- Now, $f(a+b) = 2^{a+b}$
- $= 2^a \ 2^b$
- $= f(a).f(b)$
- $\therefore$ f is an homomorphism.
- Next, let us prove that f is a Bijection.

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

  a) $f(e_1) = e_2$

- Proof: a) we have in G_2,

$$e_2 \oplus f(e_1) = f(e_1) \quad \text{(since, } e_2 \text{ is identity in } G_2\text{)}$$
$$= f(e_1 * e_1) \quad \text{(since, } e_1 \text{ is identity in } G_1\text{)}$$
$$= f(e_1) \oplus f(e_1) \quad \text{(since f is a homomorphism)}$$
$$e_2 = f(e_1) \quad \text{(By right cancellation law)}$$

Theorem 2

$f(x)' = f(x')$ *"the symmetric of a morphism is the morphism of the symmetric"*

Proof : $f(x) \circ f(x') = f(x * x') = f(e_1) = e_2$ and

$f(x') \circ f(x) = f(x' * x) = f(e_1) = e_2$

Image and Kernel of morphism

Let f be a morphism from the group $(G, *)$ to the group $(G', *')$, with e, e' their neutral element respectively.

$\rightsquigarrow$ The image of f is the subset of G' defined as :

$$Im\ f = \{f(x), x \in G\}$$

$\rightsquigarrow$ The Kernel of f is the subset of G defined as :

$$Ker\ f = \{x \in G : f(x) = e'\}$$

Image and Kernel of morphism : example

On $(\mathbb{R}, +)$ and $(\mathbb{R}_+^*, \times)$, consider the function $f : \mathbb{R} \to \mathbb{R}_+^*$, $x \mapsto e^x$.

- $\rightsquigarrow$ Since $f(x+y) = e^{x+y} = f(x) \times f(y)$, f is a morphism of the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_+^*, \times)$.
- $\rightsquigarrow$ $Im\ f = \{e^x, x \in \mathbb{R}\} = \mathbb{R}_+^*$.
- $\rightsquigarrow$ $Ker\ f = \{x \in \mathbb{R} : e^x = 1\} = \{0\}$.

Kernel and image of a group:

- ***Proposition :*** Let f : G → H be a homomorphism. Then

$$f \text{ is injective} \Longleftrightarrow Ker\, f = \{e_1\}.$$

Proof=⇒ :Suppose that f is injective.

We must show that $x \in \text{Ker } f \Longleftrightarrow x = e_1$. Note that $e_1 \in \text{Ker } f$

Conversely, suppose that $x \in \text{Ker } f$. Then by definition $f(x) = e_2 = f(e_1)$.

Since f is injective, $x = e_1$.

⇐= : Suppose that Ker f = $\{e_1\}$.

If $f(x_1) = f((x_2)$, then

in one hand $f(x_1)\ o\ (f(x_2))' = f((x_2)\ o\ (f(x_2))' = f((x_2)\ o\ (f(x_2') = f(x_2 * x_2') = f(e_1) = e_2$

in the other hand $f(x_1 * x_2') = e_2$ Then $(x_1 * x_2') \in$ Ker f then $x_1 * x_2' = e_1$ so $x_1 = x_2$

Kernel and image of a group:

Definition 1:

Let f : $(G_1,*) \rightarrow (G_2,o)$ be a homomorphism, then Ker(f) is a sub-group

Proof: x and y $\in G1$ then $f(x) = f(y) = e_2$

$f(x*y') = f(x)\ o\ f(y') = e_2\ o\ e_2 = e_2$

Therefore $(x*y') \in$ Ker f

Definition 2: The image of f is a sub-group of the group (G_2,o)

Algebraic structures

2. Ring structure

The definition of a ring

A structure $(R, +, \cdot)$ is a ring if R is a non-empty set and + and · are binary operations such that

Addition: $(R, +)$ is an abelian group, that is

- associativity: for all $a, b, c \in R$ we have $a + (b + c) = (a + b) + c$
- there exists $0 \in R$ such that for all $a \in R$ we have $a + 0 = 0 + a = a$
- inverses: for any $a \in R$, $-a \in R$ such that $a + (-a) = (-a) + a = 0$
- commutativity: for all $a, b \in R$ we have $a + b = b + a$

Multiplication: associativity: for all $a, b, c \in R$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Addition and multiplication together : for all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

Ring

A closed set $(R, T, *)$ is a ring if :

- (R, T) is an Abelian group ;
- The operation $*$ is associative on A ;
- The operation $*$ is distributive to T ;
- A admit a neutral element for the operation $*$.

If $*$ is commutative, then we say that the ring $(R, T, *)$ is commutative.

Special types of rings:

Assume $(R; +, \cdot)$ is a ring.

- We say R is a commutative ring if its multiplication $\cdot$ is commutative, that is $a \cdot b = b \cdot a$ for all $a, b \in R$.
- We say R is a ring with 1 (or ring with identity) if there exists an identity for multiplication, that is

  identity element: there exists $1 \in R$ such that for all $a \in R$ we have a

  $a \,.\, 1 = 1 \cdot a = a.$
- Integral domain:

  The commutative ring $(R; +, \cdot)$ is an integral domain if for all a, b in R,

  $$a \cdot b = 0 \Rightarrow a=0 \text{ or } b=0.$$

Examples :

(1) All of $(Z,+,.)$, $(Q,+,.)$, $(R,+,.)$ and $(C,+,.)$ are commutative rings with identity (with the number 1 as the identity).

(2) $(N,+,.)$ is NOT a ring for the usual addition and multiplication. These are binary operations and we do have a zero element, namely 0. However existence of additive inverses fails: there is no $n \in N$ for which $1 + n = 0$, for example.

(3) (A (R; R) , +, o) is a non commutative ring with identity and without integral domain :
The identity is id_x such that $f \circ id_x = f$
$f \circ g = 0$ does not imply that f and g are zeros.

Subrings and the Subring Test :

Let (R; +, ·) be a ring and let S be a non-empty subset of R. Then (S; +, ·) is a subring of R if it is a ring with respect to the operations it inherits from R.

The Subring Test : Let (R; +, ·) be a ring and let S ⊆ R.
Then (S; +, ·) is a subring of R if (and only if) S is non-empty and the following hold:

- a + b ∈ S for any a, b ∈ S;
- a − b ∈ S for any a, b ∈ S;
- ab ∈ S for any a, b ∈ S.

Sub-ring

A nonempty subset S of a ring $(R, +, \times)$ is a subring of R if and only if :

- $(S, +)$ is a subgroup of the group $(R, +)$
- S is closed under multiplication : if $a, b \in S$ then $a \times b \in S$.
- $e_\times \in S$

$(\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Q}, +, \times)$

Homomorphism of rings

In ring theory, a branch of abstract algebra, a **ring homomorphism** is a structure-preserving function between two rings. More explicitly, if R and S are rings, then a ring homomorphism is a function $f : R \to S$ such that f is:[1][2][3][4][5][6][7][a]

addition preserving:

$$f(a + b) = f(a) + f(b) \text{ for all } a \text{ and } b \text{ in } R,$$

multiplication preserving:

$$f(ab) = f(a)f(b) \text{ for all } a \text{ and } b \text{ in } R,$$

and unit (multiplicative identity) preserving:

$$f(1_R) = 1_S.$$

Examples

(1) $(Z,+,x)$ and $(Q,+,x)$ are subrings of R;

(2) R, regarded as numbers of the form a + 0i for a $\in R$, is a subring of C.

(3) $(nZ , + , .)$, with n $\in Z$ are sub rings of (Z , + , .) because :

nZ contains zéro 0 and for all x,y $\in$ nZ: x - y $\in nZ$ and x . y $\in nZ$

Definition:

The element a of R the ring with unity is said to be invertible if there exists b such that

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

Example:

- In (Z,+,.), the invertible elements are 1 and -1
- In (R,+,.), all elements are invertible except 0
- In (A (R; R) , +, o), the invertible elements are the bijective applications

Exemple 2: La structure $(A(\mathbb{R},\mathbb{R}),+_A,\cdot_A)$ est un anneau commutatif unitaire non intègre.

$A(\mathbb{R},\mathbb{R})$ est l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition usuelle $+_A$et la multiplication usuelle $\cdot_A$ des applications définies par:
Pour toutes f,$g \in A(\mathbb{R},\mathbb{R})$: $f +_A g$ et $f \cdot_A g$ sont les applications de $\mathbb{R}$ dans $\mathbb{R}$ telles que: $(f +_A g)(x) = f(x) + g(x)$ et $(f \cdot_A g)(x) = f(x) \cdot g(x)$, pour tout $x \in \mathbb{R}$.

*L'élément unité 1_A est l'application constante $1_A : \mathbb{R} \to \mathbb{R}$ telle que $1_A(x) = 1$

*Dans l'anneau $(A(\mathbb{R},\mathbb{R}),+_A,\cdot_A)$, les éléments inversibles sont les applications f qui ne s'annulent pas, (C.à.d: Pour tout $x \in \mathbb{R} : f(x) \neq 0$), dans ce cas $f^{-1} = \frac{1}{f}$, avec $\frac{1}{f}(x) = \frac{1}{f(x)}$

*On peut avoir $f \cdot_A g = 0_A$ sans que f et g soient nulles. ($f(x) \neq 0$ pour $x \neq 1$ et $f(1) = 0$ et $g(x) = 0$ pour $x \neq 1$ et $g(1) \neq 0$)

The definition of a field

Definition : A structure (F, +, ·) where + and · are binary operations on F is a field if

- $0 \neq 1$ ie "$e_1 \neq e_2$"
- (F, +) is an abelian group;
- (F \ {0}, ·) is an abelian group;
- The distributive laws hold.

The field is commutative if the ring is commutative.

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are fields.
- The commutative rings $(\mathbb{Z}/2\mathbb{Z}, \overline{+}, \overline{\times})$ and $(\mathbb{Z}/3\mathbb{Z}, \overline{+}, \overline{\times})$ are commutative fields.

Remarks

- A field is a ring where each element is invertible with the second operation, excepted the zero element.
- If $(F, T, *)$ is a field then the set $F \setminus \{0_F\}$, noted F^*, provide with the second operation ; $(F^*, *)$ is a group.
- All fields are rings integral domain. The converse is false.

$(\mathbb{Z}, +, \cdot)$ is a ring with integral domain but is not a field.
$(R, +, \cdot)$, $(Q, +, \cdot)$, $(C, +, \cdot)$ are fields,

The Subfield : Let $(F; +, \cdot)$ be a field and let $L \subseteq F$.
Then $(L; +, \cdot)$ is a subfield of F if and only if:

- $a + b \in L$ for any $a, b \in L$;
- $a - b \in L$ for any $a, b \in L$;
- $a . b^{-1} \in L$ for any $a, b \in L$.

Remark that a homomorphism of field is a homomorphism of ring