Chapter 3 : Algebraic structures

A. Djehiche

29 novembre 2024

1 Binary operations

1.1 Definition

The binary operation $*$ on a set A is a function defined by :

$$A \times A \longrightarrow A$$
$$(a, b) \longrightarrow a * b$$

This means that for any elements $a, b \in A$ the operation $*$ is said to be a binary operation if and only if $(a * b) \in A$.

Example 1.

Let $A = \{1, 2, 3\}$ be a set and let $\diamond$ be a relation on A defined by :

$$A \times A \longrightarrow A$$
$$(a, b) \longrightarrow a \diamond b = \frac{a+b}{2}$$

Then, we have

$$(1, 1) \longrightarrow 1 \diamond 1 = \frac{1+1}{2} = 1 \in A$$
$$(1, 2) \longrightarrow 1 \diamond 2 = \frac{1+2}{2} = \frac{3}{2} \notin A$$

and this imply that the operation $\diamond$ is not a binary operation on A.

Example 2.

Addition $(+)$ on $\mathbb{N}$ is a binary operation

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$
$$(k_1, k_2) \longrightarrow k_1 + k_2$$

The sum of two natural numbers is always a natural number

1.2 Properties of binary operations :

Let $*$ be a binary operation on a set A.

a) Closure property :

The binary operation $*$ is said to be closure if

$$(a, b) \in A^2 \Rightarrow (a * b) \in A$$

b) Associative property :

The binary operation $*$ is associative if

$$\forall a, b, c \in A \Rightarrow a * (b * c) = (a * b) * c$$

c) Commutative property :

Comutativity means $\forall a, b \in A,\ a * b = b * a$

d) Destributive property :

Let $\#$ be another relation on A, we say that the binary operations $*$ and $\#$ are distributive if

$$a * (b\#c) = (a * b)\#(a * c) \text{ for all } a, b, c \in A$$

As an example the additin ($+$) and multiplication ($\cdot$) on R^* are destributive.

e) Identity :

Identity element is denoted by e and defined by

$$\forall a \in A \text{ there is only one element } e \in A \text{ such that } a * e = e * a = a$$

f) Inverse property :

We say that a is the inverse of b under $*$ or b is the inverse of a under $*$ if $a * b = b * a = e$, with $a, b \in A$.

Example

Let $\diamond$ be an operation on $\mathbb{R}$ defined by :

$$\forall (x, y) \in \mathbb{R}^2 \longrightarrow x \diamond y = x + y + xy$$

1. Closure property of $\diamond$:

   For all $a, b \in \mathbb{R} : a + b + ab \in \mathbb{R}$ because the addition and multiplication of real numbers are real.

2. Associative property of $\diamond$:

   We have
   $a\diamond(b\diamond c)=a+(b\diamond c)+a\,(b\diamond c)=a+b+c+bc+ab+ac+abc$, and
   $(a\diamond b)\diamond c=(a\diamond b)+c+(a\diamond b)\,c=a+b+ab+c+abc+ac+bc$
   Thus, $a\diamond(b\diamond c)=(a\diamond b)\diamond c\Longrightarrow\diamond$is assiciative binary operation.

3. Commutative property of $\diamond$:

   $a*b=a+b+ab=b*a\Rightarrow\diamond$is commutative binary operation.

4. Identity :

   $a*e=e*a=a+e+ea=a\Rightarrow e=0$

5. Inverse :

   $a*b=b*a=a+b+ab=e\Rightarrow b=\dfrac{-a}{1+a}=a^{-1}$

   It is obvious that the element -1 does not have an inverse element . This is because $a^{-1}=\dfrac{-a}{1+a}$ is undefined at $a=-1$.

2 Introduction to groups

2.1 Group

Definition 1.

We say that the operation $*$ on a set G forms a group if the following properties are satisfied :

1. Closure : $\forall a,b\in G:a*b\in G$.
2. Associativity : $\forall a,b,c\in G:a*(b*c)=(a*b)*c$
3. Identity element :$\forall a\in G,\exists e\in G:a*e=e*a=a$
4. Inverse element :$\forall a\in G,\exists b\in G:a*b=b*a=e$

Definition 2.

The group $(G,*)$ is said to be commutative (or abelian) if satisfies , in addition to the group conditions, the commutativity property.

Example 1 : Addition on the set of integer numbers $(\mathbb{Z},+)$

1. Closure : $\forall a,b\in\mathbb{Z}:a+b$ is also an integer ($a+b\in\mathbb{Z}$).
2. Associativity : $\forall a,b,c\in\mathbb{Z}:a+(b+c)=(a+b)+c$
3. Identity element :$\forall a\in\mathbb{Z},\exists e\in\mathbb{Z}:a+e=e+a=a\Rightarrow e=0$
4. Inverse element :$\forall a\in\mathbb{Z},\exists b\in\mathbb{Z}:a+b=b+a=e=0\Rightarrow b=a^{-1}=-a$

Example 2 : Multiplication on the set of non-zero real numbers $(\mathbb{R}^*, \cdot)$

1. Closure : $\forall a, b \in \mathbb{R}^* : a \cdot b$ is also an integer ($a \cdot b \in \mathbb{R}^*$).
2. Associativity : $\forall a, b, c \in \mathbb{R}^* : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Identity element :$\forall a \in \mathbb{R}^*, \exists e \in \mathbb{R}^* : a \cdot e = e \cdot a = a \Rightarrow e = 1$
4. Inverse element :$\forall a \in \mathbb{R}^*, \exists b \in \mathbb{R}^* : a \cdot b = b \cdot a = e = 1 \Rightarrow b = a^{-1} = \frac{1}{a}$

Example 3 :

The combination $(\mathbb{R}, \diamond)$, where $\diamond$ is defined by $a \diamond b = a + b + ab$, is not a group, instead $\left(\mathbb{R}^{-\{-1\}}, \diamond\right)$ is a group.

2.2 Sub-group

Subgroup $(H, *)$of a group $(G, *)$ is a subset of G manifests the same properties as $(G, *)$.

Definition

The group $(H, *)$ is said to be a subgroup of $(G, *)$ if the following have been checked

1. Closure : $\forall a, b \in H : a * b \in H$.
2. Identity element :$\forall a \in H, \exists e \in H \mid a * e = e * a = a$. ($e_H = e_G$)
3. Inverse element :$\forall a \in H, \exists a^{-1} \in H \mid a * a^{-1} = e$.

Examples :

1. $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$
2. $(\mathbb{R}^+, \cdot)$is a subgroup of $(\mathbb{R}^*, \cdot)$

2.3 Homomorphisms and isomorphisms

1. The groups $(G, *)$ and $(H, \diamond)$ are homomorphic if there exist a function $\phi : G \longrightarrow H$ such that
$$\forall a, b \in G, \phi(a * b) = \phi(a) \diamond \phi(b)$$
In this case ϕ is called Homomorphism.
2. The groups $(G, *)$ and $(H, \diamond)$ are isomorphic if there exist a $\overline{\underline{bijective}}$ function $\phi : G \longrightarrow H$ such that
$$\forall a, b \in G, \phi(a * b) = \phi(a) \diamond \phi(b)$$

In this case ϕ is called isomorphism. It is worth noting that the isomorphism is a special case of homomrphism and thus

$$\phi \ is \ isomorphism \Rightarrow \phi \ is \ homomorphism$$

2.4 Properties

Let $\phi : G \longrightarrow H$ be a function (may be bijective). ϕ is said to be homorphism (or isomorphism), then the following hold true :

1. Identity preservation : $\phi(e_G) = e_H$, where $e_G$is the identity element of G, and $e_H$is the identity element of H.
2. Inverse preservation : $\forall a \in \phi(a^{-1}) = (\phi(a))^{-1}$, where $a^{-1}$is the inverse element of a under the binary operation of the group G, and where $(\phi(a))^{-1}$is the inverse element of $\phi(a)$ under the binary operation of the group H.
3. Kernel of homomorphism : $Ker(\phi) = \{a \in G \mid \phi(a) = e_H\}$
4. Image of homomorphism : $Im(\phi) = \{\phi(a) \mid a \in G\}$

Example

Let $f(x)$ be a function defined by :

$$\begin{aligned} f : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \cdot) \\ x &\longrightarrow f(x) = e^x \end{aligned}$$

- We have $f(a+b) = e^{a+b} = e^a \cdot e^b = f(a)f(b) \Rightarrow f(x)$ is a group homomorphism
- We know that the function $e^x$is bijective$\Rightarrow f(x)$ is a group isomorphism
- $Ker(f) = \left\{a \in \mathbb{R} \mid \phi(a) = e^a = e_{(\mathbb{R}^+,\cdot)} = 1\right\} = \{0\}$

Exercise

Let $(G, \circ)$ be a group and let h be a function defined by

$$\begin{aligned} h : (G, \circ) &\longrightarrow (G, \circ) \\ x &\longrightarrow h(x) = a^{-1} \circ x \circ a \end{aligned}$$

3 Rings

3.1 Definition

A ring is an algebraic structure represented by a set with two operations called addition and multiplication. Thus, the combination $(A, \oplus, *)$ is a ring if :

1. $(A, \oplus)$ is a commutative group
2. $*$ is associative
3. $*$ is distributive over $\oplus$

3.2 Properties

- If $*$ is commutative, then $(A, \oplus, *)$ is said to be commutative ring.
- If $*$ satisfies the Identity property, then $(A, \oplus, *)$ is said to be Identity ring.

Examples :

- All of the following form a ring :
  $(\mathbb{C},+,\cdot),\ (\mathbb{R},+,\cdot),\ (\mathbb{Q},+,\cdot),\ (\mathbb{Z},+,\cdot)$.Where $+$ and $\cdot$ are the ordinary addition and multiplication·
- Addition and multiplication of polynomials $R[x]$ with real coeffecients forms a commutative ring.

4 Fields

4.1 Definition

The combination $(A,\oplus,*)$ forms a field if :

1. $(A,\oplus,*)$ is and Identity ring
2. $(A^{-\{e_\oplus\}},*)$ is a group.

Examples

All of the following form a ring :
$(\mathbb{C},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{Q},+,\cdot)$.Where $+$ and $\cdot$ are the ordinary addition and multiplication·