# Chapter II: Elementary Algebraic Structures

B. AMARI, bedrane.amari@g.enp.edu.dz

1er décembre 2024

# Teaching content

# Introduction

One of the first mathematical skills that we all learn is how to add a pair of positive integers. A young child soon recognizes that something is wrong if a sum has two values, particularly if his or her sum is different from the teacher's. In addition, it is unlikely that a child would consider assigning a non-positive value to the sum of two positive integers. In other words, at an early age we probably know that the sum of two positive integers is unique and belongs to the set of positive integers. This is what characterizes all binary operations on a set.

# Properties of Operations

## Binary Operation

Let $S$ be a non-empty set. A binary operation on $S$ is a rule that assigns to each ordered pair of elements of $S$ a unique element of $S$. In other words, a binary operation is a function from $S \times S$ into $S$.

- $\rightsquigarrow$ $+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$
- $\rightsquigarrow$ Multiplications, union, intersection, composition of functions ..., are binary operations.

# Properties of Operations

## Commutative Property

Let $*$ be a binary operation on a set $S$. We say that $*$ is commutative if and only if $a * b = b * a$ for all $a, b \in S$.

## Associative Property

Let $*$ be a binary operation on a set $S$. We say that $*$ is associative if and only if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

- $\rightsquigarrow$ The addition and multiplication are associative and commutative on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $\rightsquigarrow$ $T : xTy = \frac{x+y}{2}; x, y \in \mathbb{Q}$ is not associative $(((-1T0)T1 = \frac{1}{4})$ and $(-1T(0T1) = \frac{-1}{4})$ ). But it is commutative on $\mathbb{Q}$.
- $\rightsquigarrow$ $\circ$ is associative on $\mathcal{A}(S, S)$, but not commutative on $\mathcal{A}(S, S)$, only if $E$ is reduced to one element.

# Properties of Operations

## Identity Property

Let $*$ be a binary operation on a set $S$. We say that $*$ has an identity if and only if there exists an element $e \in S$ such that $a * e = e * a = a$ for all $a \in S$.

## Inverse Property

Let $*$ be a binary operation on a set $S$. We say that $*$ has the inverse property if and only if for each $a \in S$ there exists $b \in S$ such that $a * b = b * a = e$. We call $b$ an inverse of $a$, noted $a^{-1}$.

- $\rightsquigarrow$ On $(\mathbb{R}, \times), e = 1$ and $(\mathcal{A}(S, S), \circ), e = f_{Id}$. $e$ is called the neutral element
- $\rightsquigarrow$ $a^{-1} \in \mathbb{R}^*$ is $\frac{1}{a}$ and the inverse of $f \in (\mathcal{A}(S, S))$ is $f^{-1}$

# Properties of Operations

## Idempotent Property

Let $*$ be a binary operation on a set $S$. We say that $*$ is idempotent if and only if $a * a = a$ for all $a \in S$.

- $\rightsquigarrow$ On $((\mathcal{A}(S,S),\circ)$, $f^n = f \circ f \circ f \circ \cdots \circ f = f$ when $f = f_{Id_E}$
- $\rightsquigarrow$ ...on matrix !

# Properties of Operations

## Left Distributive Property

Let $*$ and $*'$ be binary operations on a set $S$. We say that $*'$ is left distributive over $*$ if and only if $a *' (b * c) = (a *' b) * (a *' c)$ for all $a, b, c \in S$.

## Right Distributive Property

Let $*$ and $*'$ be binary operations on a set $S$. We say that $*'$ is right distributive over $*$ if and only if $(b * c) *' a = (b *' a) * (c *' a)$ for all $a, b, c \in S$.

## Distributive Property

Let $*$ and $*'$ be binary operations on a set $S$. We say that $*'$ is distributive over $*$ if and only if $*'$ is both left and right distributive over $*$.

# Closure Property, Closed Set

## Closure Property

Let $T$ be a subset of $S$ and let $*$ be a binary operation on $S$. We say that $T$ is closed under $*$ if $a, b \in T$ implies that $a * b \in T$.

## Closed Set

$(S, *)$ is a closed set if $S$ is non-empty set and $S$ is closed under $*$.

- $\rightsquigarrow$ $(\mathbb{N}, +), (\mathbb{N}, .)$ and $(\mathcal{P}(\mathcal{E}), \cup), (\mathcal{P}(\mathcal{E}), \cap)$ are closed sets.
- $\rightsquigarrow$ $(\mathbb{N}, -)$ is not a closed set, ....

# Morphism, isomorphism and endomorphism

## Morphism, isomorphism and endomorphism

Lets $(S,*)$ and $(S',*')$ be two closed set.

- ▷ A morphism from $(S,*)$ to $(S',*')$ is every application $f : S \to S'$ such that :

$$\forall (x,x') \in E^2 : f(x * x') = f(x) *' f(x')$$

- ▷ If $f$ is bijective then $f$ is an isomorphism $(S,*)$ to $(S',*')$.
- ▷ An endomorphism is a morphism $(S,*)$ on itself.
- ▷ An automorphism is an endomorphism $(S,*)$ bijective.

# Group

## Group

Let $(G, *)$ be a closed set. $(G, *)$ is a group if :

1. $*$ is associative on G :$(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. There exists an identity element, $e \in G$, such that $a * e = e * a = a$ for all $a \in G$.
3. For all $a \in G$, there exists an inverse; that is, there exists $b \in G$ such that $a * b = b * a = e$.

If $*$ is commutative then $(G, *)$ is Abelian group (commutative group).

# Group example

- $(\mathbb{R},+),(\mathbb{Z},+),(\mathbb{R}^*,\times),(\mathbb{Q}^*,\times)$ are Abelian groups.
- $(\mathbb{N},+)$ and $(\mathbb{Z},\times)$ are not groups.
- Let $E \neq \emptyset$. $(\mathcal{P}(E),\cup)$ is not a group, because if $A \neq \emptyset$ then, there is no $A' \in \mathcal{P}(E)$ such that $A \cup A' = \emptyset$.
- Let $E \neq \emptyset$. $(\mathcal{P}(E),\cap)$ is not a group, because if $A \neq E$ then, there is no $A' \in \mathcal{P}(E)$ such that $A \cap A' = E$.

# Subgroup

## Subgroup definition

Let $(G, *)$ be a group. A non empty subset $H$ of $G$ is a subgroup if and only if it satisfies the following conditions.

1. The identity $e$ of $G$ is in $H$.
2. If $x, y \in H$, then $x * y \in H$.
3. If $x \in H$, then $x^{-1} \in H$.

## Proposition

Let $H$ be a subset of a group G. Then $H$ is a subgroup of $G$ if and only if $H \neq \emptyset$, and whenever $x, y \in H$ then $x * y^{-1} \in H$ is in H.

# Subgroup example

Consider the group $G = (\mathbb{R}^*, \times)$. $H = \{2^n, n \in \mathbb{Z}\}$ is a subgroup of $G$.

- $H \subset G$;
- $e = 1$ is in $H$;
- Let $a = 2^n, n \in \mathbb{Z}$ and $b = 2^m, m \in \mathbb{Z}$.
  $a \times b = 2^n \times 2^m = 2^{n+m} \in H$
- Let $a = 2^n, n \in \mathbb{Z}$, $a^{-1} = 2^{-n}, -n \in \mathbb{Z}$, so $a^{-1} \in H$.

# Image and Kernel of morphism

## 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

## 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 $(\mathbb{R}_+^*,\times)$.
- $\rightsquigarrow$ $Im\ f=\{e^x, x\in\mathbb{R}\}=\mathbb{R}_+^*$.
- $\rightsquigarrow$ $Ker\ f=\{x\in\mathbb{R}: e^x=1\}=\{0\}$.

# Some results

## Propositions

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

$P_1$ : The neutral element of a group $(G, *)$, $e$, is unique.

$P_2$ : The symmetrical element of a group $(G, *)$, $x^{-1}$, is unique.

$P_3$ : $f(e) = e'$ and $f(x^{-1}) = (f(x))^{-1}$.

$P_4$ : $f$ is injective if and only if $Ker\ f = \{e\}$.

$P_5$ : Let $K$ be the kernel of $f$. $\forall k \in K$, and $\forall x \in G$, we have $x * k * x^{-1} \in K$

$\rightsquigarrow$ Proofs !

# Example

$$\mathcal{A}_{aff}(\mathbb{R},\mathbb{R}) = \{\forall (a,b) \in \mathbb{R}^* \times \mathbb{R} \ \ and \ \ \forall\, x \in \mathbb{R} : \varphi_{(a,b)}(x) = ax+b\}$$

## $(\mathcal{A}_{aff}(\mathbb{R},\mathbb{R}), \circ)$ is not a commutative group

- Let $f_1, f_2, f_3 \in \mathcal{A}_{aff}$, we have $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3 \cdots$
- $\forall f \in \mathcal{A}_{aff}, \exists f_{Id} \in \mathcal{A}_{aff} : f \circ f_{Id} = f_{Id} \circ f = f; f_{Id}(x) = x$ for $a = 1$ and $b = 0$.
- $\forall f \in \mathcal{A}_{aff}, \exists f^{-1} \in \mathcal{A}_{aff} : f \circ f^{-1} = f^{-1} \circ f = f_{Id};$ $f^{-1}_{(a,b)}(x) = \frac{1}{a}x - \frac{b}{a}$.
- Let $f_1, f_2 \in \mathcal{A}_{aff}$, we have $f_1 \circ f_2 \neq f_2 \circ f_1$.

$\rightsquigarrow$ $(\mathcal{A}_{aff}(\mathbb{R},\mathbb{R}), \circ)$ is not a commutative group.

# Example

$$\mathcal{A}_{aff}(\mathbb{R},\mathbb{R}) = \{\forall (a,b) \in \mathbb{R}^* \times \mathbb{R} \ \ and \ \ \forall\, x \in \mathbb{R} : \varphi_{(a,b)}(x) = ax+b\}$$

**$T(\mathbb{R}) = \{\varphi_{(1,b)} : b \in \mathbb{R}\}$ is a subgroup of $(\mathcal{A}_{aff}(\mathbb{R},\mathbb{R}), \circ)$.**

- $\rightsquigarrow$ $T(\mathbb{R}) \subset \mathcal{A}_{aff}(\mathbb{R},\mathbb{R})$;
- $\rightsquigarrow$ $f_{Id}$ is in $T(\mathbb{R})$;$(a = 1, b = 0)$
- $\rightsquigarrow$ Let $f_1 \in T(\mathbb{R})$ and $f_2 \in T(\mathbb{R})$. $f_1 \circ f_2 \in T(\mathbb{R})$
- $\rightsquigarrow$ Let $f \in T(\mathbb{R})$, $f^{-1}(x) = 1 - b \in T(\mathbb{R})$.

# Ring

## 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.

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are rings.
- $(\mathcal{P}(E), \cup, \cap)$ is not a ring.
- Let $X \neq \emptyset$, $(\mathcal{A}(X, \mathbb{R}), +, \times)$ is a ring, with $x \in X \mapsto 0 \in \mathbb{R}$ and $x \in X \mapsto 1 \in \mathbb{R}$

# The ring $(R, +, \times)$

## Unity of a Ring

A ring $(R, +, \times)$ that has a multiplicative identity is called a ring with unity. More formally, if $\exists 1_\times \in R : \forall a \in R$, $a \times 1_\times = 1_\times \times a = a$ then $R$ is called a ring with unity.

## 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 $(\mathbb{Q}, +, \times)$

# Integral domain and zero divisors

## Zero Divisor

Let $(R, +, \times)$ be a ring. If $a$ and $b$ are two non-zero elements of $R$ such that $a \times b = 0$, then $a$ and $b$ are called zero divisors.

## Integral Domain

A commutative ring with unity containing no zero divisors is called an integral domain.

## Remarks

- The ring must be commutative because of the right and the left of the zero divisors.
- $(R, +, \times)$ is a ring integral domain if $R \neq \{0_R\}$ and if $\forall (a, b) \in R^2 (a \times b = 0_R \Rightarrow (a = 0_R \quad or \quad b = 0_R))$

# Integral domain and zero divisors examples

1. In $(\mathcal{A}(\mathbb{R}, \mathbb{R}), +, \times)$, the two functions
$f : x \mapsto \{0 \textit{ if } x \leqslant 0; \textit{ and } \sqrt{x} \textit{ if } x > 0\}$ and
$g : x \mapsto \{x \textit{ if } x \leqslant 0; \textit{ and } 0 \textit{ if } x > 0\}$ are zero divisor.
2. The closed set $(\mathbb{Z}, +, \times)$ don't have a zero divisor, so it is a commutative ring integral domain.
3. The commutative rings $(\mathbb{Z}/2\mathbb{Z}, \overline{+}, \overline{\times})$ and $(\mathbb{Z}/3\mathbb{Z}, \overline{+}, \overline{\times})$ are integral domain. But, $(\mathbb{Z}/4\mathbb{Z}, \overline{+}, \overline{\times})$ is not integral domain, because, $\overline{2}\overline{\times}\overline{2} = \overline{0}$. So,$\overline{2}$ is a zero divisor in $\mathbb{Z}/4\mathbb{Z}$.
4. In $(\mathbb{Z}/8\mathbb{Z}, \overline{+}, \overline{\times})$, $\overline{4}$ and $\overline{2}$ are zero divisors since since $\overline{4}\overline{\times}\overline{2} = \overline{0}$.
And $\overline{6}$ is a zero divisor because $\overline{6}\overline{\times}\overline{4} = \overline{0}$

# Fields

## Field

A closed set $(F, T, *)$ is a field if :

- $(F, T, *)$ is a ring ;
- $\forall x \in F, x \neq e_T, \exists x^{-1} \in F : \; x * x^{-1} = x^{-1} * x = e_*$.

If $*$ is commutative, then we say that the Field $(F, T, *)$ 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.
- $(\mathbb{Z}/13\mathbb{Z}, \overline{+}, \overline{\times})$ is a field but $(\mathbb{Z}/4\mathbb{Z}, \overline{+}, \overline{\times})$ is not a field.
- In the general case, $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\times})$ is field if $n \in \mathbb{N}$ is prime.

# Fields remarks, example

## 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.

## $(\mathbb{Q}[\sqrt{2}], +, \times)$ is a field ; $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : (a, b) \in \mathbb{Q}^2\}$

- $(\mathbb{Q}[\sqrt{2}], +, \times)$ is a commutative ring ;
- $\forall x \in \mathbb{Q}[\sqrt{2}], x \neq 0, \exists x^{-1} \in \mathbb{Q}[\sqrt{2}] : \; x \times x^{-1} = x^{-1} \times x = 1.$
  Where $x^{-1} = a' + b'\sqrt{2} : a' = \frac{a}{a^2 - 2b^2}, b' = \frac{-b}{a^2 - 2b^2}.$

# Morphism of ring, morphism of field

## Morphism of ring, morphism of field

Lets $(R, T, *)$ and $(R', T', *')$ be two rings.

- A morphism of rings from $(R, T, *)$ to $(R', T', *')$ is every application $f : R \to R'$ such that :
  $\forall (x, x') \in R^2 : f(xTx') = f(x)T'f(x')$ ,
  $\forall (x, x') \in R^2 : f(x * x') = f(x) *' f(x')$ and $f(e_*) = e_{*'}$
- If $f$ is bijective then $f$ is an isomorphism of ring $(R, T, *)$ to $(R', T', *')$.
- If $(R, T, *)$ and $(R', T', *')$ are field, then $f$ is a field morphism.

# Example

We define on $\mathbb{R}$ the operations $\oplus$ and $\otimes$ as follow :
$x \oplus y = x + y - 1, \quad x \otimes y = x + y - xy$

1. $(\mathbb{R}, \oplus)$ is an Abelian group.
   - $x \oplus y = x + y - 1 = y \oplus x$ ;
   - $x \oplus (y \oplus x) = (x \oplus y) \oplus x$ ;
   - $e_{\oplus} = 1$ and $x^{-1} = 2 - x$.
2. $\otimes$ is associative and commutative.
   - $x \times y = y \otimes x$ ;
   - $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$ ;
   - $e_{\otimes} =?$ and $x^{-1} =?$.
3. Is $(\mathbb{R}, \oplus, \otimes)$ a ring ? field ?

# Example

$\rightsquigarrow$

$\rightsquigarrow$

## Proposition

$\rightsquigarrow$

$\rightsquigarrow$

## Proposition