University of Batna 2

Faculty of Mathematics and Computer Science

Departement of Mathematics

Chapter 04: Algebraic structures

By : Brahimi Mahmoud

$$a \times (b + c) = a \times b + a \times c$$

Academic year 2024/2025

1 Internal composition law

Definition

Let E be a set, an internal composition law on E in a map of $E \times E$ on E, we denote the internal composition law by: $*, \Delta, \mathrm{T}, \ldots$And we write

$$*: E \times E \longrightarrow E$$
$$(x, y) \longmapsto x * y$$

Examples:

$(+)$ and $(\times)$ are internal composition laws on $\mathbb{N}$.

$(-)$ and $(\div)$ are an internal composition laws on $\mathbb{N}$.

Properties of an internal composition law

Definition

Let $*$ be an internal law on a set E. We say that

- The law $*$ is commutative if for all $x, y \in E$: $(x * y = y * x)$.
- The law $*$ is associative if for all $x, y, z \in E$: $((x * y) * z = x * (y * z))$.
- e of is an identity element for the law $*$ if for all $x \in E$: $(x * e = e * x = x)$
- x has an inverse element x' for the law $*$, if: $(x * x' = x' * x = e)$ hold
- $*$ is distributive with respect to Δ if for all elements $x, y, z \in E$;
  $x * (y \Delta z) = (x * y) \Delta (x * z)$ and $(x \Delta y) * z = (x * z) \Delta (y * z)$

Example:

Let $*$ be an internal law on $E = \mathbb{R} - \{-1\}$ defined by: $\forall x, y \in E; x * y = x + y + xy$.

$*$ is commutative, associative, has an identity element and each element has an inverse element.

Proposition

Let $*$ be an internal law on a set E, if $*$ has an identity element, it is unique

2 Groups

Definition

Let $*$ be an internal law on a set G, we say that $(G,*)$ is a group if the following properties are satisfied:

- $*$ is associative
- $*$ has an identity element
- Each element in G has an inverse

Remark
If $*$ is commutative we say that $(G,*)$ is a commutative group or abelian group.

Example:

Let $*$ be an internal law on $G = \mathbb{R}$ defined by: $\forall x, y \in G; x * y = x + y - 1$

Show that $(G,*)$ is a commutative group.

Subgroup

Let $(G,*)$ be a group

Definition
A subpart $H \subset G$ is a subgroup of G if:

- $e \in H,$
- For all $x, y \in H$, we have $x \star y \in H,$
- For all $x \in H$, we have $x' \in H.$

Remark
To show that H is a subgroup it suffices to show that:

- $H \neq \emptyset$ that's to say $e \in H$
- $\forall x, y \in H \Longrightarrow x * y' \in H$

Example:

$H = \{z \in \mathbb{C}^*;\ |z| = 1\}$, $(H, \times)$ is a subgroup of $(\mathbb{C}^*, \times)$

Group homomorphism

Definition
Let $(G,\star)$ and (G', Δ) be two groups. A map $f : G \longrightarrow G'$ is a group morphism if:
For all $x, x' \in G;\ f(x \star x') = f(x)\, \Delta\, f(x')$

Example:

$f: (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times)$, $f(x) = e^x$ is a group morphism.

Properties

Proposition
Let $f : G \longrightarrow G'$ a group morphism, then:

- $f(e_G) = e_{G'}$
- For all $x \in G, f(x') = \big(f(x)\big)'$

Example:

$f: (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +),\ f(x) = \ln x$

Proposition

- Let there be two group morphisms $f : G \longrightarrow G'$ and $g : G' \longrightarrow G''$.

Then $g \circ f : G \longrightarrow G''$ is a group morphism.

- If $f : G \longrightarrow G'$ is a bijective morphism then $f^{-1} : G' \longrightarrow G$ is also a group morphism.

Group isomorphism

Definition

A bijective morphism is an isomorphism. Two groups G, G' are isomorphic if there exists a bijective morphism $f : G \longrightarrow G'$.

Example:

$f: (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +),\ f(x) = \ln x$ is group isomorphism.

Finite $\frac{\mathbb{Z}}{n\mathbb{Z}}$ groups

The set and the $\frac{\mathbb{Z}}{n\mathbb{Z}}$ group

Let $n \geqslant 1$. Remember that $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is the set $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ where $\bar{p}$ denotes the equivalence class of p modulo n, in other words $\bar{p} = \bar{q} \Leftrightarrow p \equiv q (\mathrm{mod} n)$.

Or $\bar{p} = \bar{q} \Leftrightarrow \exists k \in \mathbb{Z}, p = q + kn$.

Examples:

$\frac{\mathbb{Z}}{3\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}\}, \frac{\mathbb{Z}}{6\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

An addition on $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is defined by: $\overline{p+q} = \bar{p} + \bar{q}$

The product on $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is defined by: $\overline{p \times q} = \bar{p} \times \bar{q}$

Example:

On $\frac{\mathbb{Z}}{12\mathbb{Z}}$ we have $\overline{10} + \bar{5} = \overline{10+5} = \overline{15} = \bar{3}, \bar{7} + \bar{5} = \overline{7+5} = \overline{12} = \bar{0}$.

$\overline{10}\ \overline{\times 5} = \overline{10 \times 5} = \overline{50} = \bar{2}, \bar{7} \times \bar{5} = \overline{7 \times 5} = \overline{35} = \overline{11}$.

Theorem

$(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ is a commutative group.

Example: $\frac{\mathbb{Z}}{5\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5} = \bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5} = \bar{0}$	$\bar{6} = \bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5} = \bar{0}$	$\bar{6} = \bar{1}$	$\bar{7} = \bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5} = \bar{0}$	$\bar{6} = \bar{1}$	$\bar{7} = \bar{2}$	$\bar{8} = \bar{3}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

S_3 Permutation group

Proposition

The set of bijections from $\{1, 2, \ldots, n\}$ into itself, equipped with the composition of functions, is a group, denoted $(S_n, \circ)$.

Definition

A bijection from $\{1,2, \ldots, n\}$ (into itself) is called a permutation. The group $(S_n, \circ)$ is called the permutation group (or the symmetric group)

Lemma

The number of permutations S_n is $n!$

Notation and examples

Describing a permutation $f : \{1,2, \ldots, n\} \longrightarrow \{1,2, \ldots, n\}$ is equivalent to giving the images of each i going from 1 to n. We therefore denote f by

$$\begin{bmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{bmatrix}$$

In this case we will study in detail the group S_3 of permutations of $\{1,2,3\}$. We know that S_3 has $3! = 6$ elements that we list

- $id = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ identity
- $\tau_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$ a transposition
- $\tau_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ a second transposition
- $\tau_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$ a third transposition
- $\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ a cycle
- $\sigma^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ the reverse of the previous cycle

Then $S_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$

Let's calculate $\tau_1 \circ \sigma$ and $\sigma \circ \tau_1$

$$\tau_1 \circ \sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \tau_2 \text{ and } \sigma \circ \tau_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \tau_3$$

We have $\tau_1 \circ \sigma \neq \sigma \circ \tau_1$ then the group is not commutative. Generally, the group $S_n, n \geq 3$ is not commutative.

Table of the S_3 group

$g \circ f$	id	τ_1	τ_2	τ_3	σ	σ^{-1}
id	id	τ_1	τ_2	τ_3	σ	σ^{-1}
τ_1	τ_1	id	σ	σ^{-1}	τ_2	τ_3
τ_2	τ_2	σ^{-1}	id	σ	τ_3	τ_1
τ_3	τ_3	σ	σ^{-1}	id	τ_1	τ_2
σ	σ	τ_3	τ_1	τ_2	σ^{-1}	id
σ^{-1}	σ^{-1}	τ_2	τ_3	τ_1	id	σ

3 The Rings

Definition

Let $+$ and $\times$ be two internal laws on a set A, we say that $(A, +, \times)$ is a ring if the following properties are satisfied:

- $(A, +)$ is a commutative group whose identity element will be noted 0_A
- The law $\times$ is associative
- $\times$ is distributive with respect to $+$

Remarks

- The ring is commutative if $\times$ is commutative
- Unitary if $\times$ has an identity element 1_A

Examples:

$(\mathbb{Z},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ are commutative rings

Calculation rules in a ring

Let $(A,+,\times)$ be a ring and let $x,y \in A$ then

- $x \times 0_A = 0_A \times x = 0_A$
- For all $n \in \mathbb{Z}; n(ab) = (na)b = a(nb)$
- $(-a)(-b) = ab$
- If a and b commute,
  $(a+b)^n = \sum_{k=0}^{k=n} C_n^k a^k b^{n-k}$ and $a^n - b^n = (a-b)\sum_{k=0}^{k=n-1} a^k b^{n-1-k}$

Subring

If A is a ring and B is a subring of A, we say that B is a subring of A if B is stable for the $+$ and $\times$ laws and if B has the $+$ and $\times$ laws is a ring.

Proposition

A part B of the ring A is a subring of A if and only if:

- $1_A \in B$
- $\forall a,b \in B; a - b \in B$
- $\forall a,b \in B; a \times b \in B$

Invertible elements

In a ring A, not all elements $a \in A$ necessarily has an inverse for the $\times$ law. When this is the case, we say that a is invertible and we denote its inverse a^{-1}. The set of invertible elements of the ring is denoted $U(A)$. It is a group for the $\times$ law.

Zero divisors

Definition

Let A be a ring.

- A non-zero element a of A is called a zero divisor if there exists another non-zero element b of A such that $ab = 0$.
- If A is a commutative ring not reduced to $\{0\}$ and if A does not have a zero divisor, then we say that A is integral. Or integral domain.

Example:

In $\frac{\mathbb{Z}}{6\mathbb{Z}}$ we have $\bar{2} \times \bar{3} = \bar{0}$ but $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$, $\bar{2}$ and $\bar{3}$ are zero divisors.

Ring homomorphism

Definition

Let A, B be two rings. An application $f: A \to B$ is a ring morphism if the following conditions are satisfied:

- $f(1_A) = 1_B$
- For all $a, b \in A; f(a + b) = f(a) + f(b)$
- For all $a, b \in A; f(a \times b) = f(a) \times f(b)$

If f is bijective we say that $f: A \to B$ is a ring isomorphism.

Remarks

For a ring morphism $f: A \to B$ we have

- $f(0_A) = 0_B$
- For all $n \in \mathbb{Z}$ and $a \in A; f(na) = nf(a)$

Ideals

Definition

Let A be a commutative ring. A subset I of A is an ideal if $(I, +)$ is a group and if, for all $a \in A$ and all $u \in I$, then $au \in I$.

Proposition

A part I of A is an ideal if and only if I is non-empty and satisfies:

- For all $x, y \in I; x - y \in I$
- For all $x \in I$ and for all $a \in A; ax \in I$

Proposition

Let I and J be two ideals of A. Then $I \cap J$ and $I + J$ are two ideals of A.

4 Field

Definition

A field is a commutative ring in which every non-zero element is invertible

Examples:

- $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are fields
- $(\mathbb{Z}, +, \times)$ is not a field

- $(\frac{\mathbb{Z}}{p\mathbb{Z}} - \{\bar{0}\}, +, \times)$ is a field, where p is prime number, as a particular case we take $p = 5$ then

$\frac{\mathbb{Z}}{5\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\times$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$