# Chapter n°4 Algebraic structures

## 1| Internal composition law

Let E be a non-empty set, the internal composition law on E is mapping, or function

$$* : E \times E \longrightarrow E$$
$$(a,b) \longmapsto a*b$$

. The law $*$ is called internal composition law if:

$\forall a,b \in E,\ a*b \in E$ (closure law)

(E is closed with respect to law $*$)

Exple $* : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$

$$(a,b) \longmapsto a*b = $$
$$= a+b+2ab$$

Since, $a,b \in \mathbb{N} \Rightarrow a+b+2ab \in \mathbb{N}$

Then, $*$ is an internal composition law

## 2| Group

Def. Let $*$ an internal composition law in non-empty set G.

$(G,*)$ is a group if the following axioms are satisfied

$G_1$| Associativity:

$\forall x,y,z \in G : (x*y)*z = x*(y*z)$

$G_2$| There exist a neutral element (Existence of identity)

$G_3$| Existence of inverse:

$\forall x \in G,\ \exists x' \in G :$

$$x*x' = x'*x = e$$

Remark

. If $*$ is commutative:

$\forall x,y \in G : x*y = y*x$, the group $(G,*)$ is called commutative group

. The addition inverse:

$x' = -x,\ \forall x \in G$

and we have:

$x+(-x) = (-x)+x = 0$

. The multiplication inverse

$x' = x^{-1}$, and we have

$x x^{-1} = x^{-1} . x = 1$

~~Exercise: Let $G = ]-1,1[$ We define the internal composition~~

Exple. $* : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$

$$(x,y) \longmapsto x*y = x+y$$

1) $\forall x,y \in \mathbb{N},\ x+y \in \mathbb{N} \Rightarrow$
$x*y \in \mathbb{N} \Rightarrow *$ is a closure la

2) $\forall x,y,z \in \mathbb{N} : (x*y)*z = (x+y)*z$
$= x+y+z = x*(y+z) = x*(y*z)$
$\Rightarrow *$ is associative

3) $\forall x \in \mathbb{N}, \begin{cases} x*e_r = x \\ e_l * x = x \end{cases} \Rightarrow \begin{cases} e_r = 0 \in \mathbb{N} \\ e_l = 0 \in \mathbb{N} \end{cases}$

$\Rightarrow \exists e = 0 \in \mathbb{N}$ is a neutral element

4) $\forall x \in \mathbb{N}$, we have

$$\begin{cases} x * x_1' = e \\ x' * x_2 = e \end{cases} \Rightarrow \begin{cases} x_2' = -x \notin \mathbb{N} \\ x_2' = -x \in \mathbb{N} \end{cases}$$

$\Rightarrow \nexists x' \in \mathbb{N} : x * x' = x' * x = e$

$\Rightarrow *$ has no inverse element

Then, $(\mathbb{N}, *)$ is not a group

5) $\forall x, y \in \mathbb{N} : x * y = x + y$
$= y + x$
$= y * x$

$\Rightarrow *$ is commutative

Exple. $\times : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$
$(x, y) \longmapsto x \times y = x . y$

$(\mathbb{R}, \times)$ is not a group, because:

$\forall x \in \mathbb{R}, \ x \times e = x \Rightarrow$

$x . e = x \Rightarrow e = \frac{x}{x}$

if $x = 0 \Rightarrow \nexists e \in \mathbb{R}$ such that

$x * e = e * x = x \Rightarrow$ there isn't an identity

## Subgroup

Let $(G, *)$ be a group, $H$ a subset of $G$, $H \subset G$,

$(H, *)$ is called a subgroup of $(G, *)$ if:

$$\begin{cases} H \neq \phi \\ \forall x, y \in H, \ x * y^{-1} \in H \end{cases}$$

$\Longleftrightarrow$

$$\begin{cases} H \neq \phi \\ \forall x, y \in H, \ x * y \in H \\ \forall x \in H, \ x^{-1} \in H \end{cases}$$

Exple. Let $(\mathbb{R}^*, .)$ be a group

Prove that $(\mathbb{R}^*_+, .)$ is a subgroup of $(\mathbb{R}^*, .)$

Proof. We have:

1) $e_{\mathbb{R}^*} = 1 \in \mathbb{R}^*_+$, and $\mathbb{R}^*_+ \subset \mathbb{R}^*$

$\Rightarrow \mathbb{R}^*_+ \neq \phi$

2) $\forall x, y \in \mathbb{R}^*_+ : x . y^{-1} = \frac{x}{y} \in \mathbb{R}^*_+$

$\Rightarrow x . y^{-1} \in \mathbb{R}^*_+$

So, $(\mathbb{R}^*_+, .)$ is a subgroup of $(\mathbb{R}^*, .)$

Exple. $(\mathbb{Z}, +)$ is subgroup of a group $(\mathbb{Q}, +)$

We have:

1) $e_{\mathbb{Q}} = 0 \in \mathbb{Z}$ and $\mathbb{Z} \subset \mathbb{Q}$

$\Rightarrow \mathbb{Z} \neq \phi$

2) $\forall x, y \in \mathbb{Z} : x + (-y) = x - y \in \mathbb{Z}$

$\Rightarrow x + (-y) \in \mathbb{Z}$ #

## Subgroup of $\mathbb{Z}$

Let $(\mathbb{Z}, +)$ be the additive group of integers

. The subgroups of $(\mathbb{Z}, +)$ are the $(n\mathbb{Z}, +)$, $\forall n \in \mathbb{Z}$.

. The set $n\mathbb{Z}$ is the set of integers multiples of $n$

$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

Expl. $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$
is the set of even integers

$7\mathbb{Z} = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$
is the set of integers which are divisible by 7 (the multiples of 7)

## Congruence

**Def.** If a and b are integers and $n > 0$, we write $a \equiv b \pmod n$

we read: "a congruent to b modulo n" (or, mod n)

to means: $n / (a-b)$

or, we say

$\exists k \in \mathbb{Z} : a = kn + b$

**Expl.** $26 \equiv 2 \pmod 3$

means

$26 = 24 + 2$
$= 8 \times 3 + 2$

$b - a = 26 - 2 = 24$

$n / 24 \iff 3/24$

$\frac{24}{3} = 8 \Rightarrow 24 \in 3\mathbb{Z}$

**Def.** For fixed n, we write the equivalence class of a called: residue class as:

$\bar{a} = \{ b \in \mathbb{Z} \,/\, a \equiv b \pmod n \}$

$= \{ a + kn \mid k \in \mathbb{Z} \}$

~~Hence, $a \equiv b \pmod n \iff \bar{a} = \bar{b}$~~

**Exo1** $(\mathbb{Z}_{odd}, +)$ is not a group

since: $\forall a, b \in \mathbb{Z}_{odd} \Rightarrow a + b \notin \mathbb{Z}_{odd}$

for example: $a = 3, b = 7 \in \mathbb{Z}_{odd}$

but, $a + b = 3 + 7 = 10 \notin \mathbb{Z}_{odd}$

$\mathbb{Z}_{odd}$ is not closed under +

**Exo2.** $(\mathbb{Z} - \{0\}, \cdot)$ is not a group

since: $\exists a \in \mathbb{Z} - \{0\}$ has no multiplicative inverse.

for example:

$a = 3 \in \mathbb{Z} - \{0\}$ and

$a^{-1} = 3^{-1} = \frac{1}{3} \notin \mathbb{Z} - \{0\}$.

**Exo3.** Let

$G = \{ n.a \,,\, n \in \mathbb{Z} \,,\, a \neq 0 \}$. Prove that $(G, +)$ is a commutative group.

**Exo4.** Let $X \neq \phi$ and

$\mathcal{P}(X) = \{ A, A \subset X \}$ be the power set of a non-empty set.

Prove that: $(\mathcal{P}(X), \cup)$ form a group.

**Exo5** Let $G = \{1, -1, i, -i\}$, where $i^2 = -1$.

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

## $\mathbb{Z}/n\mathbb{Z}$

Let n be a positive integer the set of equivalence classes of integers modulo n, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Exple (1) $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, where

$\bar{1} = \{\dots, -7, -5, -3, -1, 1, 3, 5, 7, \dots\}$ is the set of odd integers

$\bar{0} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$ is the set of even integers

Remark. If $\bar{a}$ and $\bar{b}$ are elements of $\mathbb{Z}/n\mathbb{Z}$, we define:

$\overline{a.b} = \bar{a}.\bar{b}$ and, $\bar{a}+\bar{b} = \overline{a+b}$

Exple (2). $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

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

$(\mathbb{Z}/n\mathbb{Z}, +)$ : integers modulo $n$ with addition

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

$\bar{3}+\bar{5} = \bar{2}$ , $\bar{2}+\bar{4} = \bar{0}$

Questions.

(1) What is the identity?

(2) Does 1 have an inverse.

Answers.

(1) $\bar{0}$ is the identity, because $\bar{1}+\bar{0} = \bar{0}+\bar{1} = \bar{1}$

(2) The inverse element of 1 is 5

$\bar{1}+\bar{5} = \bar{6} = \bar{0}$, means that

$[1]^{-1} = \overline{6-1} = \bar{5}$ because $(\bar{a})^{-1} = \overline{n-a}$

(in $\mathbb{Z}_n$: $\bar{a} + \overline{n-a} = \overline{a+n-a} = \bar{n} = \bar{0}$)

and $\bar{5} = \overline{(-1)} = -\bar{1}+\bar{0} = -\bar{1}+\bar{6} = \bar{5}$

then, $\begin{cases} \bar{1}+\bar{5} = \bar{0} \\ 1 + \overline{(-1)} = 0 \end{cases}$

Exercise (1) Show that $(\mathbb{Z}_4, +)$ is a group

(2) Prove that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a commutative group

Def. Order of finite groupe

Group Homomorphism.

Def. Let $(G, *)$ and $(G', \Delta)$ be a groups.

A group homomorphism $f$, $f: G \longrightarrow G'$ is a function such that: $\forall x, y \in G$

$f(x*y) = f(x) \Delta f(y)$

Exple. Let $f: (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$

, $(\mathbb{R}, +)$ and $(\mathbb{R}_+^*, \times)$ are a groups

and, $f(x) = e^x$

$\forall x, y \in \mathbb{R}$: $f(x+y) = e^{x+y} =$

$= e^x \times e^y = f(x) \times f(y)$

$\Rightarrow f$ is a group homomorphism

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

1) $f(e_G) = e_{G'}$
2) $\forall x \in G : f(x^{-1}) = (f(x))^{-1}$

**Exple.** $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$

$x \longmapsto e^x$

We know that

1) $e_{\mathbb{R}} = 0$ and $e_{\mathbb{R}_+^*} = 1$,

We have

$f(e_{\mathbb{R}}) = f(0) = e^0 = 1 = e_{\mathbb{R}_+^*}$

2) The symmetric of $x$ in $(\mathbb{R}, +)$ is $(-x)$, and the symmetric of $f(x)$ in $(\mathbb{R}_+^*, \times)$ is $(f(x))^{-1}$

We have:

$f(-x) = e^{-x} = \frac{1}{e^x} = \frac{1}{f(x)} = (f(x))^{-1}$

**Proposition** Let $f: G \longrightarrow G'$, and $g: G' \longrightarrow H'$, two group morphisms. Then

1) $g \circ f : G \longrightarrow H$ is a group morphism
2) If, $f$ is ~~fu~~ bijective, then $f^{-1}: G' \rightarrow G$ is a bijective group morphism

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

$x \longmapsto e^x$

We have

$f(x) = e^x = y \Rightarrow x = \ln y \in \mathbb{R}$

so, $f^{-1} : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$

$x \longmapsto \ln x$

$f^{-1}(x \times y) = \ln(x \times y) = \ln x + \ln y$

$= f^{-1}(x) + f^{-1}(y)$

$\Rightarrow f^{-1}$ is a group morphism

**Def.** (A group isomorphism)
A group isomorphism is a group morphism wich is bijection (bijective)

**Def.** Let, $f : (G, *) \longrightarrow (G', \times)$ be a group morphism

1) If, $G' = G \Rightarrow f$ is an endomorphism
2) If, $f$ is isomorphism and $G = G' \Rightarrow f$ is an automorphism.

---

**Def.** The order of finite group $(G, *)$ is the number of all its elements, denoted by $|G|$ or $O(G)$

**exple.** $G = \{1, -1, i, -i\}$

$|G| = 4$

$|\mathbb{Z}_n| = n$ and $|\mathbb{Z}_4| = 4$

**Ex** Let $G = \{1, -1, i, -i\}$, where $i^2 = -1$

Show that $(G, \cdot)$ is a commutative group

**Solution:**

| $\cdot$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

1) From the table G is closed under multiply

2) $\cdot$ is associative ?

For example, if we take: $1, -i, i \in G$

$(1 \cdot -i) \cdot i = -i \cdot i = -i^2 = 1$

$1 \cdot (-i \cdot i) = -i^2 = 1$

3) The identity element of G

$\forall a \in G,\ a \cdot 1 = 1 \cdot a = 1 \in G$

so, $e_G = 1$

4) Inverse element

$1^{-1} = 1 \in G,\ (-1)^{-1} = -1 \in G$

$i^{-1} = \frac{1}{i} = -i \in G,\ (-i)^{-1} = \frac{1}{-i} = i \in G$

5) $\cdot$ is commutative ?

$\forall a, b \in G.\ a \cdot b = b \cdot a$

$\Rightarrow (G, \cdot)$ is a commutative group

---

+ Def. (Idempotent element)

An element "a" of a group $(G, *)$ is called idempotent if:

$a^2 = a * a = a$

# Ring

Let R be a non-empty set together with two operations

$+ : R \times R \longrightarrow R$

$(x, y) \longmapsto x + y$

$\bullet : R \times R \longrightarrow R$

$(x, y) \longmapsto x \cdot y$

The set:

$(R, +, \cdot)$ is called a ring if the following axioms are satisfied:

1) $(R, +)$ is an abelian group

2) The operations are distributive, that is, $\forall a, b, c \in R$

$c \cdot (a + c) = c \cdot a + c \cdot b$, and

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

3) The multiplication "$\cdot$" is associative

- Remark

1) If the multiplication is commutative, that is:

$a \cdot b = b \cdot a$, $\forall a, b \in R$, then $(R, +, \cdot)$ is called a commutative ring

2) If there is $1 \in R$ (an identity) with, $a \cdot 1 = 1 \cdot a = a$, $\forall a \in R$

We say that, R is a ring with 1 (or with unity)

Exple. In $\mathbb{Z}^2$, we define two internal composition law denoted + and x, by:

$\forall (a,b), (c,d) \in \mathbb{Z}^2$

$(a,b) + (c,d) = (a+c, b+d)$

$(a,b) \times (c,d) = (ac, ad+bc)$

- Prove that $(\mathbb{Z}^2, +, \times)$ is a ring?

- Subring

Let $(R,+,\cdot)$ be a ring and $U$ a subset of $R$, $(U \subset R)$, then $(U,+,\cdot)$ is a subring of $R$ if

1) $(U,+)$ a subgroup of $(R,+)$

2) $\forall x,y \in U$, $x \cdot y \in U$

3) $1_R \in U$

Exple $(3\mathbb{Q},+,\cdot)$ is not a subring of $(\mathbb{Q},+,\cdot)$

Because $1_{\mathbb{Q}} \notin 3\mathbb{Q}$.

Proposition

The set $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$, $\forall n > 0$ is a commutative ring.

Ring homomorphism

Def A ring homomorphism is a function, $f:(R,+,\cdot) \to (R',*,\Delta)$ (between two rings) such that:

1) $\forall x,y \in R$:

$f(x+y) = f(x) * f(y)$

2) $\forall x,y \in R$:

$f(x \cdot y) = f(x) \Delta f(y)$

3) $f(1_R) = 1_{R'}$ ~~(multiplicative~~ (multiplicative identity)

Remark:

- A ring endomorphism is a ring homomorphism from a ring to itself.
- A ring isomorphism is a bijective ring homomorphism
- A ring automorphism is a ring isomorphism from a ring to itself.
- The identity function $I_{d_A}: A \longrightarrow A$ is a ring automorphism: (morph + $(A=A)$ + biject)

Exple. $f: \mathbb{Z} \longrightarrow \mathbb{Z}$

With: $f(x) = x+1$

or $f(x) = x^2$

$f(x)$ cannot be a ring homomorphism.

## Field

**Def.** Let $(R,+,\cdot)$ be a ring with 1,

$(R,+,\cdot)$ is a field if:

1) $1_R \neq 0_R$

2) every element of $R$ is invertible with respect to the law "$\cdot$"