1 Algebraic structures

2 Law of internal composition

Definition

Any application $* : E \times E \to E.$ on a set E is called a law of internal composition. A subset F of E is said to be stable with respect to the law $*$ if :

$$\forall a, b \in F,\ a * b \in F.$$

Example

Let A be a set and $E = P(A)$, then intersection and reunion of sets are two laws of internal compositions in E because : $\forall X,\ Y \in P(A)$,

$$X \cap Y \subset X \subset A,$$

and we have

$$\forall x, \quad x \in X \cup Y \Rightarrow (x \in X) \vee (x \in Y) \Rightarrow (x \in A) \vee (x \in A) \Rightarrow (x \in A)\,,$$

So

$$X \cup Y \subset A,$$

Example

which shows that $\cap$ and $\cup$ are laws of internal compositions in $P(A)$.

Example

Let $F = \{\{a, b\}, \{a, c\}, \{b, c\}\} \subset P(\{a, b, c\})$, then F is not stable with respect to intersection and reunion, because :

$$\exists X = \{a, b\}, Y = \{a, c\} \in F;\ X \cap Y = \{a\} \notin F.$$

$$\exists X = \{a, b\},\ Y = \{a, c\} \in F;\ X \cup Y = \{a, b, c\} \notin F.$$

Definition

If $*$ and . are two internal composition laws on E, we say that :

1. $*$ is commutative if :

$$\forall a, b \in E,\ a * b = b * a.$$

2. $*$ is associative if :

$$\forall a, b, c \in E,\ (a * b) * c = a * (b * c).$$

3. $*$is distributive with respect to . if :

$$\forall a, b, c \in E,\ a * (b.c) = (a * b).(a * c) \text{ et } (b.c) * a = (b * a).(c * a).$$

4. $e \in E$ is a left (respectively right) neutral element of the $*$ law if

$$\forall a \in E,\ e * a = a \text{ (respectively} a * e = a).$$

If e is a neutral element to the right and left of $*$ we say that e is a neutral element of $*$.

Example

Let F be a set and $E = P(F)$. Consider on E the internal composition laws "$\cap$" and "$\cup$", then it's very easy to show that:

– "$\cap$" and "$\cup$" are associative.

– "$\cap$" and "$\cup$" are commutative.

– $\varnothing$ is the neutral element of $\cup$.

– F is the neutral element of $\cap$.

– $\cap$ is distributive with respect to $\cup$ and $\cup$ is distributive with respect to $\cap$.

Proposition

If an internal composition law $*$ has a right-neutral element e' and an e'' left-neutral element, then $e' = e''$and it is a neutral element of $*$.

Proof

Let e'(respectively e'') be a right-neutral (respectively left-neutral) element of $*$, then

$$e' = e'' * e' \text{ car } e''\text{élément neutre à gauche de} * ,$$

$$e'' = e'' * e' \text{ car } e'\text{élément neutre à droite de} * ,$$

which shows that

$$e' = e''.$$

Remark:

According to the latter property, if $*$ has a neutral element, then it is unique.

Definition:

Let $*$ be an internal composition law on a set E admitting a neutral element e. An element $a \in E$ is said to be invertible, or symmetrizable, to the right (respectively left) of $*$ if

$$\exists a' \in E,\, a * a' = e \text{ (respectively } a' * a = e),$$

and a' is said to be a right-hand (respectively left-hand) inverse (or symmetrical) of a.

If there exists $a' \in E$ such that

$$a' * a = a * a' = e$$

a is said to be invertible (or symetrisable) and a' is said to be an inverse (or symmetric) of a with respect to $*$.

Remark:

The symmetric of an element is not always unique.

Example

Let $E = \{a, b, c\}$, we define an internal composition law in E by :

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	a

Note that :
- a is the neutral element of $*$.
–All elements of E are invertible with :
i) a is the inverse of a,
ii) c is the inverse of b,
iii) b and c are inverses of c.
Proposition

Let $*$ be a law of internal composition in E, associative and admitting a neutral element e. If an element $x \in E$ is symmetrizable, then its symmetric is unique.

Proof

Say x_1 is a right-hand inverse of x and x_2 is a left-hand inverse of x, then

$$x * x_1 = e \text{ et } x_2 * x = e$$

So,

$$\begin{aligned} x_1 &= e * x_1 = (x_2 * x) * x_1 \\ &= x_2 * (x * x_1) \text{ because } * \text{ is associative} \\ &= x_2 * e = x_2. \end{aligned}$$

Proposition

Let $*$ be a law of internal composition in a set E, associative and admitting a neutral element e, then if a and b are two invertible (symmetrizable) elements so will be $(a * b)$ and we have :

$$(a \star b)^{-1} = b^{-1} * a^{-1} \text{ where } a^{-1} \text{ is the inverse element of } a$$

Proof

Let $a, b \in E$ be two invertible elements, then

$$\begin{aligned} (a \star b) * b^{-1} * a^{-1} &= a \star \left(b * b^{-1}\right) * a^{-1} \\ &= (a \star e) * a^{-1} = a * a^{-1} = e. \end{aligned}$$

In the same way, we show that

$$\left(b^{-1} * a^{-1}\right) * (a \star b) = e,$$

we deduce that $(a * b)$ is invertible and that

$$(a \star b)^{-1} = b^{-1} * a^{-1}.$$

3 Group structure

Definition

We call a group, any non-empty set G provided with an internal composition law $*$ such that :

1. $*$ is associative ,
2. $*$ has a neutral element e ,
3. Every element of G is symmetrizable.

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

Example

$(\mathbb{R}^*, \times)$ is a commutative group, $\times$ is the usual multiplication. Let's check each of the properties:

1. If $x, y \in \mathbb{R}^*$ then

$$x \times y \in \mathbb{R}^*.$$

2. For all $x, y, z \in \mathbb{R}^*$, then

$$x \times (y \times z) = (x \times y) \times z,$$

is the associativity of multiplication of real numbers.

3. 1 is the neutral element for multiplication because

$$1 \times x = x \text{ and } x \times 1 = x,$$

whatever $x \in \mathbb{R}^*$.

4. The inverse of an element $x \in \mathbb{R}^*\}$ is

$$x^{-1} = \frac{1}{x}$$

(because $x \times \frac{1}{x}$ =1).

Note in passing that we had excluded 0 from our group, as it has no inverse.

These properties make $(\mathbb{R}^*, \times)$ a group.

$$x \times y = y \times x,$$

- $(\mathbb{Q}^*, \times)$, $(\mathbb{C}^*, \times)$ are commutative groups.
- $(\mathbb{Z}, +)$ is a commutative group. Here $+$ is the usual addition.

1. If x, $y \in \mathbb{Z}$ then

$$x + y \in \mathbb{Z}.$$

2. For all $x, y, z \in \mathbb{Z}$ then

$$(x + y) + z = x + (y + z).$$

3. 0 is the neutral element for addition.

$$0 + x = x \text{ and } x + 0 = x,$$

whatever $x \in \mathbb{Z}$..

4. The inverse of an element $x \in \mathbb{Z}$ is

$$x' = -x$$

because

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

5. Finally

$$x + y = y + x,$$

and therefore $(\mathbb{Z}, +)$ is a commutative group.
- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups.

3.1 Subgroups

Definition

Let $(G, *)$ be a group, and let G' be a non-empty subset of G, we say that G'' is a subgroup of $(G, *)$ if :

$$\begin{cases} (i)\ \forall a, b \in G',\ a * b \in G' \\ (ii)\ \ \forall a \in G',\ a^{-1} \in G' \end{cases}.$$

Example

Let $n \in \mathbb{N}$, then

$$n\mathbb{Z} = \{n.p;\ p \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$.
Indeed:
i) Let x, $y \in n\mathbb{Z}$ then there exist p_1, $p_2 \in \mathbb{Z}$ such that

$$x = n.p_1 et y = n.p_2,$$

so,

$$x + y = n.p_1 + n.p_2 = n.(p_1 + p_2) \in n\mathbb{Z}.$$

ii) Let $x \in n\mathbb{Z}$ then $\exists\ p \in \mathbb{Z}$ such that

$$x = n.p.$$

Let x' be the symmetric of x, so,$x + x' = e = 0$

$$(o \text{ is the neutral elementof } (\mathbb{Z}, +)),$$

$$\Rightarrow x' = -x = -n.p = n.(-p) \in n\mathbb{Z}.$$

From i) and ii) we deduce that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
Proposition:
Let $(G, *)$ be a group and $G' \subset G$, then

$$G' \text{is a subgroup of } G \Leftrightarrow \begin{cases} (1)\ G' \neq \varnothing \\ (2)\ \forall a, b \in G',\ a * b^{-1} \in G' \end{cases}.$$

Proof

I. Let G' be a subgroup of $(G, *))$, then:

1) $*$ has a neutral element in G' because

$$\forall a \in G', a^{-1} \in G' (\text{according to (ii) of the definition}).$$

according to (i), we have

$$a * a^{-1} = e \in G',$$

So

$$G' \neq \varnothing.$$

2) Let $a, b \in G'$, from (ii) we have $b^{-1} \in G'$, so

$$a * b^{-1} \in G' (\text{according to} \, (i) \,).$$

II. Conversely, let G' be a subset of G such that

$$\begin{cases} (1) \;\; G' \neq \varnothing \\ (2) \;\; \forall a, \, b \in G', \, a * b^{-1} \in G' \end{cases}.$$

1) Since $G' \neq \varnothing$, then there exists $a \in G'$ and according to the second hypothesis we have

$$e = a * a^{-1} \in G'.$$

2) Let $x \in G'$, as $e \in G'$,, then according to the second hypothesis we will have

$$x^{-1} = e * x^{-1} \in G'.$$

3) $\forall x, \, y \in G'$, from ii) we have

$$x * y = x * \left(y^{-1}\right)^{-1} \in G',$$

therefore, $G'$is a subgroup of G.

Remark

From I) of the proof of the previous proposition, we see that: If e is the neutral element of a group $((G, *)$, then every subgroup of G contains e and we deduce the following corollary.

Corollary

Let $(G, *)$ be a group, e the neutral element of $*$ and G' a subset of G,then G' is a subgroup of G if and only if:

$$\begin{cases} (1) \;\; e \in G' \\ (2) \;\; \forall a, \, b \in G', \, a * b^{-1} \in G' \end{cases}.$$

Example

Let the group $\left(\mathbb{R}^2, +\right)$ with the operation $+$ be defined by :

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

So,

$$H = \left\{(a, b) \in \mathbb{R}^2 / a + 2b = 0\right\}$$

is a subgroup of $\mathbb{R}^2$.
Indeed:
$i)$ $H \neq \varnothing$ because $(0,0) \in H$.
$ii)$ Let (a,b), $(c,d) \in H$, then

$$\left\{ \begin{array}{l} a+2b=0 \\ c+2d=0 \end{array} \right. ,$$

Example 1 *so,*

$$(a-c)+2(b-d)=0,$$

as a result,

$$(a-c, b-d) = (a,b) + (-c,-d) \in H.$$

From i) and ii) we deduce that H is a subgroup of $\mathbb{R}^2$.

3.2 Homomorphisms of groups

Definition

An application $f : (G, .) \to (H, *)$ is called a group homomorphism of G in H if :

$$\forall a, b \in G,\ f(a.b) = f(a) * f(b).$$

- If f is bijective, we say that f is an isomorphism (of groups) of G onto H. We then say that G is isomorphic to H, or that G and H are isomorphic.

- If $G = H$, we say that f is an endomorphism of G, and if moreover f is bijective, we say that f is an automorphism (of group) of G.

Example

Given the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^*, .)$, then the applications

$$\begin{array}{lclcr} f & : & (\mathbb{R},+) \to (\mathbb{R}^*,.) & \text{et} & g : (\mathbb{R},+) \to (\mathbb{R}^*,.) \\ x & \longmapsto & \exp x & & x \longmapsto \ln|x| \end{array}$$

are homomorphisms of groups

Definition

Let $f : G \to H$ be a group homomorphism with e and e' the neutral elements of G and H respectively. We call the kernel of f the set

$$Ker f = f^{-1}(e') = \{x \in G;\ f(x) = e'\},$$

and the image of f the set

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

Properties:

Let $f : G \to H$ be a homomorphism of groups, then

1. $f(e) = e'$.
2. $\forall a \in G$, $(f(a))^{-1} = f\left(a^{-1}\right)$.

3. The image of a subgroup of G is a subgroup of H .

4. The reciprocal image of a subgroup of H is a subgroup of G.

Remark:

As special cases of the properties, Imf is a subgroup of $(H, *)$ and $Ker f$ is a subgroup of $(G, .)$.

Proposition:

Let : $G \to H$ be a group homomorphism, then.

1.f is injective if and only if

$$Ker f = \{e\}.$$

2. f is surjective if and only if

$$\operatorname{Im} f = H.$$

3. f is an isomorphism if and only if f^{-1} exists and is a group homomorphism from H into G.

Proof

Let $f : G \to H$ be a group homomorphism, then

1a. If f is injective, knowing that $e \in ker f$ we'll show that

$$ker f \subset \{e\}.$$

Let $x \in ker f$, then

$$f(x) = e'$$

and as

$$f(e) = e'$$

we deduce that

$$f(x) = f(e)$$

and since f is injective we deduce that

$$x = e$$

So

$$x \in \{e\}$$

which shows that

$$ker f = \{e\}.$$

1b. Conversely, suppose $ker f = \{e\}$ and show that f is injective.

Let $x, y \in G$, then

$$\begin{aligned} f(x) &= f(y) \\ &\Rightarrow f(x) * (f(y))^{-1} = e' \\ &\Rightarrow f(x) * f(y^{-1}) = e' \\ &\Rightarrow f(x.y^{-1}) = e' \\ &\Rightarrow x.y^{-1} \in ker f \\ &\Rightarrow x.y^{-1} = e \qquad \text{because } ker f = \{e\}. \\ &\Rightarrow x = y \end{aligned}$$

which shows that f is injective.
2. The proof of this property is immediate, given that

$$\operatorname{Im} f = f(G).$$

3. We will restrict ourselves to showing that if f is an isomorphism, then $f^{-1} : H \rightarrow G$ is a homomorphism.
Let $x, y \in H$, then there exist $a, b \in G$ such that

$$x = f(a) \text{ et } y = f(b)$$

so,

$$a = f^{-1}(x) \text{ et } b = f^{-1}(y)$$

as a result

$$\begin{aligned} f^{-1}(x * y) &= f^{-1}(f(a) * f(b)) \\ &= f^{-1}(f(a.b)) \\ &= a.b \\ &= f^{-1}(x) \,.\, f^{-1}(y) \end{aligned}$$

which shows thatf^{-1} is a group homomorphism from H into G.

4 Rings structure

Definition 2 *We call a ring any set A equipped with two internal composition laws $+$ and $.$ such that:*
1. *$(A, +)$ is an abelian group (we will denote 0_A the neutral element of $+$),*
2. *$.$ is associative and distributive with respect to $+$.*

Remark 3 *If in addition, $.$ is commutative, we say that $(A, +, .)$ is a commutative ring.*

Remark 4 - *If $.$ accepts a neutral element, we say that $(A, +, .)$ is a unitary or uniferous ring.*

Example 5 $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$,$(\mathbb{R}, +, \times)$ *are unitary commutative rings.*

Calculation rules in a Ring
Let $(A, +, .)$ be a ring, then we have the following calculation rules:
Properties :
For all x, y and $z \in A$, we have
1. $0_A\, .x = x.\, 0_A = 0_A$.
2. $x.(-y) = (-x).y = -(x.y)$.
3. $x.(y - z) = (x.y) - (x.z)$.
4. $(y - z).x = (y.x) - (z.x)$.

Definition 6 *If there exist in a ring* $(A, +, .)$ *two elements* $a \neq 0_A$, $b \neq 0_A$*:*

$$a.b = 0_A$$

we say that a *and* b *are divisors of* 0_A*.*

- We say that $(A, +, .)$ *is a complete ring if there exists no divisor of* 0_A*, i.e.*

$$a.b = 0_A \Leftrightarrow a = 0_A \vee b = 0_A.$$

Example 7 $(\mathbb{Z}, +, \times)$ *is a complete ring.*

4.1 Subrings

Definition 8 *: A subset* A' *of* $(A, +, .)$ *is a subring if and only if:*

1. $A' \neq \varnothing$.

2. $\forall x, y \in A'$, $x - y \in A'$.

3. $\forall x, y \in A'$, $x.y \in A'$.

Example 9 $(n\mathbb{Z}, +, \times)$ *is a subring of* $(\mathbb{Z}, +, \times)$*.*

4.2 Homomorphismes of rings

Let $(A, +, .)$ and $(B, \oplus, \otimes)$ be two rings and $f : A \to B$.

Definition 10 *We say that fis a ring homomorphism if:*

$$\forall x, y \in A, f(x + y) = f(x) \oplus f(y) \ et \ f(x.y) = f(x) \otimes f(y).$$

– If $A = B$ *we say that* f *is an endomorphism of rings .*

– If f *is bijective, we say that* f *is an isomorphism of rings.*

– If f *is bijective and* $A = B$*, we say that* f *is an automorphism of rings.*

Definition 11 *Let* A *and* B *be two unitary rings, we say that an homomorphism of rings* f *from* A *to* B *is unitary if* $f\ (1_A) = 1_B$*.*

Proposition 12 *Let* $f : A \to B$ *a ring homomorphism, so*

– f *is injective if and only if* $ker f = \{0_A\}$

– If A and B are two unitary rings and f is a surjective ring homomorphism, then f is unitary.

– The image (respectively the reciprocal image) of a subring of A (respectively of B) by f is a subring of B (respectively of A).

5 Fields

Definition 13 *A unitary ring* $(K, +, .)$ *is said to be a field if every non-zero element of* K *is invertible.*

If moreover, . is commutative, we say that K *is a commutative field.*

Example 14 $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{C}, +, \times)$ *are commutative fields.*

$(\mathbb{Z}, +, \times)$ *is not a field.*

5.1 Subfields

Definition 15 *A subset L' of $(K, +, .)$ is a subbody if and only if:*

1. $L \neq \varnothing$.

2. $\forall x, y \in L,\ x - y \in L$.

3. $\forall x, y \in L^*,\ x.y^{-1} \in L^*$ *(where*$L^* = L - \{0_K\}$*).*

Example 16 $(\mathbb{Q}, +, \times)$ *is a subfield of* $(\mathbb{R}, +, \times)$.