CHAPITRE 1

ALGEBRAIC STRUCTURES

1.1 Internal Composition Law

Definition 1.1. *Let E be a non-empty set. An internal composition law **(ICL)** on E is any mapping $*$ from $E \times E$ to E, i.e.*

$$\begin{aligned} * : E \times E &\longrightarrow E \\ (x, y) &\longmapsto x * y \end{aligned}$$

Remark 1.1. *The operation "$*$" is an internal composition law on E if and only if :*

$$\forall x, y \in E,\ x * y \in E.$$

Example 1.1.

1. *We know that for all $x, y \in \mathbb{N}$: $x + y \in \mathbb{N}$ and $x \cdot y \in \mathbb{N}$. Therefore, the usual addition "$+$" and the usual multiplication "$.$" are internal composition laws on $\mathbb{N}$. It is clear that the usual addition "$+$" and the usual multiplication "$.$" are internal composition laws on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.*
2. *The usual subtraction "$-$" is an internal composition law on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, but not on $\mathbb{N}$.*
3. *The usual addition "$+$" on the set $B = \{0, 1\}$ is not an internal composition law. Indeed :*

(x, y)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$x + y$	*0*	*1*	*1*	$2 \notin B$

*The usual multiplication "$.$" on the set $B = \{0, 1\}$ **is** an internal composition law. Indeed :*

(x, y)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$x \cdot y$	*0*	*0*	*0*	*1*

4. *The intersection $\cap$ is an internal composition law on the set $\mathcal{P}(E)$ of all subsets of E.*

Definition 1.2. *Let $*$ be an internal composition law on a non-empty set E. Then :*

1. *The law $*$ is said to be **commutative** if :*

$$\forall x, y \in E,\ x * y = y * x$$

2. *The law $*$ is said to be **associative** if :*

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

3. *The law $*$ admits a* ***neutral element*** *if :*

$$\exists e \in E,\ \forall x \in E,\ (x * e = x) \wedge (e * x = x)$$

The element e (if it exists) is called the neutral element of $*$.

4. *When $*$ admits a neutral element e, an element of E is said to be* ***invertible*** *with respect to $*$ if :*

$$\forall x \in E,\ \exists x' \in E,\ (x * x' = e) \wedge (x' * x = e)$$

The element x' (if it exists) is called the inverse (or symmetric) of x and is denoted by x^{-1}.

Example 1.2. 1. *The usual addition "$+$" on $\mathbb{R}$:*
   - *$\forall x, y \in \mathbb{R},\ x + y = y + x$, hence the usual addition "$+$" is commutative on $\mathbb{R}$.*
   - *$\forall x, y, z \in \mathbb{R},\ x + (y + z) = (x + y) + z$, hence the usual addition "$+$" is associative on $\mathbb{R}$.*
   - *$\exists e = 0 \in \mathbb{R},\ \forall x \in \mathbb{R},\ (x + 0 = x) \wedge (0 + x = x)$, hence 0 is the neutral element for "$+$" on $\mathbb{R}$.*
   - *$\forall x \in \mathbb{R},\ \exists x' = -x \in \mathbb{R},\ (x + (-x) = 0) \wedge ((-x) + x = 0)$, hence every element of $\mathbb{R}$ is invertible with respect to "$+$".*

2. *The usual multiplication "$\cdot$" on $\mathbb{R}$:*
   - *$\forall x, y \in \mathbb{R},\ x \cdot y = y \cdot x$, hence the usual multiplication "$\cdot$" is commutative on $\mathbb{R}$.*
   - *We know that $\forall x, y, z \in \mathbb{R},\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$, hence the usual multiplication "$\cdot$" is associative on $\mathbb{R}$.*
   - *$\exists e = 1 \in \mathbb{R},\ \forall x \in \mathbb{R},\ (x \cdot 1 = x) \wedge (1 \cdot x = x)$, hence 1 is the neutral element for "$\cdot$" on $\mathbb{R}$.*
   - *For $x = 0$, we cannot find $x' \in \mathbb{R}$ such that $0 \cdot x' = 1$; hence $x = 0$ is not invertible with respect to the usual multiplication "$\cdot$". That is : $\exists x = 0 \in \mathbb{R},\ \forall x' \in \mathbb{R},\ (x \cdot x' \neq 1) \vee (x' \cdot x \neq 1)$, therefore not all elements of $\mathbb{R}$ are invertible with respect to "$\cdot$".*

1.2 Group Structure

Definition 1.3. *Let $*$ be an internal composition law on a non-empty set G. We say that $(G, *)$ is a group if $*$ is associative, admits a neutral element e, and every element of G is invertible with respect to $*$.*
If, in addition, $*$ is commutative, the group is said to be commutative or abelian.

Example 1.3. 1. *The structures $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are commutative groups.*
2. *The structures $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are not groups (because 0 has no inverse for the usual multiplication "$\cdot$").*
3. *The structures $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are commutative groups.*
4. *The structures $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, and $(\mathbb{Z}, \cdot)$ are not groups.*

1.2.1 Subgroup

Definition 1.4. *Let $(G, *)$ be a group and H a subset of G. We say that $(H, *)$ is a* ***subgroup*** *of $(G, *)$ if $(H, *)$ is itself a group for the operation $*$ restricted to H.*

Proposition 1.1. *Let H be a subset of a group $(G, *)$ with neutral element e. Then,*

$$(H, *) \text{ is a subgroup of } (G, *) \iff \begin{cases} e \in H \\ \forall x, y \in H,\ x * y^{-1} \in H \end{cases}$$

Démonstration. **a)** Suppose that $(H, *)$ is a subgroup of $(G, *)$, and let us show that :

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

Let $x, y \in H$. We have $x, y^{-1} \in H$ (because every element of H has an inverse with respect to $*$ in H), and $x * y^{-1} \in H$ (because $*$ is an internal operation on H).
Therefore, $\forall x, y \in H : x * y^{-1} \in H$.
Also, $H \neq \varnothing$, so there exists $x_0 \in G$ with $x_0 \in H$, hence $x_0 * x_0^{-1} \in H$. That is, $e \in H$.

b) Suppose that :

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

and let us show that $(H, *)$ is a subgroup of $(G, *)$.
Since $e \in H$, we have $H \neq \varnothing$. Moreover, since $\forall x \in G : x * e = x = e * x$, in particular $\forall x \in H : x * e = x = e * x$. That is, e is the identity element of $*$ in H.

Let $y \in H$ and $x = e \in H$. Then $x * y^{-1} = e * y^{-1} = y^{-1} \in H$, hence $\forall y \in H : y^{-1} \in H$. That is, every element of H has an inverse with respect to $*$ in H.

Let $x, y \in H$. Then $x, y^{-1} \in H$, hence $x * (y^{-1})^{-1} = x * y \in H$. Therefore, $\forall x, y \in H : x * y \in H$. That is, $*$ is a closed operation on H.

Let $x, y, z \in H$. Then $x, y, z \in G$, so $(x * y) * z = x * (y * z)$, and therefore $\forall x, y, z \in H : (x * y) * z = x * (y * z)$. That is, $*$ is associative in H.

Thus, $(H, *)$ satisfies all the group axioms, and therefore it is indeed a subgroup of $(G, *)$. □

Example 1.4. *1. $\mathbb{Z}$ is a subset of $\mathbb{Q}$ and $(\mathbb{Q}, +)$ is a group.*
We have :

$$\begin{cases} 0 \in \mathbb{Z} \\ \forall x, y \in \mathbb{Z} : x + (-y) \in \mathbb{Z}. \end{cases}$$

Therefore, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.
Similarly, $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$ and of $(\mathbb{C}, +)$.

2. The unit circle $S = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subset of $\mathbb{C}^*$, and $(\mathbb{C}^*, \cdot)$ is a group.
We have $|1| = 1$, therefore $1 \in S$. Let $z, z' \in S$. Then

$$\left|z \cdot (z')^{-1}\right| = \frac{|z|}{|z'|} = 1,$$

therefore $z \cdot (z')^{-1} \in S$. Thus,

$$\begin{cases} 1 \in S \\ \forall z, z' \in S : z \cdot (z')^{-1} \in S \end{cases}$$

and therefore $(S, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

1.2.2 Homomorphism, Endomorphism, Isomorphism, Automorphism

Definition 1.5. *Let $(G, *)$ and (G', Δ) be two groups, and let $f : G \to G'$ be a function. We say that :*

1. *f is a homomorphism from G to G' if*

$$\forall x, y \in G : \quad f(x * y) = f(x) \,\Delta\, f(y).$$

2. *f is an endomorphism of G if f is a homomorphism from G to G.*
3. *f is an isomorphism from G to G' if f is a bijective homomorphism.*
4. *f is an automorphism of G if f is a bijective endomorphism.*

Example 1.5.

1. *The function $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$ defined by $f(x) = e^x$ is a homomorphism. Indeed,*

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

2. *The function $g : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ defined by $g(x) = \ln x$ is an isomorphism, because*

$$\forall x, y \in \mathbb{R}_+^* : \quad g(x \times y) = \ln(x \times y) = \ln(x) + \ln(y) = g(x) + g(y).$$

Moreover, g is bijective.

1.3 Ring Structure

In what follows, we use the internal operations $+$ and $\cdot$ (called addition and multiplication, respectively), whose neutral elements are denoted by 0 and 1, and the inverses of an element x are : for addition, $-x$, and for multiplication, x^{-1}.

Definition 1.6. *1) A set A equipped with two operations $+$ and $\cdot$ is called a ring if and only if :*

1. *$(A, +)$ is an abelian group.*
2. *The operation "$\cdot$" is associative.*
3. *For all $x, y, z \in A$:*

$$\begin{cases} x \cdot (y + z) = (x \cdot y) + (x \cdot z), \\ (y + z) \cdot x = (y \cdot x) + (z \cdot x), \end{cases}$$

(This condition is called the distributivity of "$\cdot$" with respect to "$+$".)

Remark 1.2.

1. *If, moreover, the operation "$\cdot$" is commutative, then $(A, +, \cdot)$ is called a commutative ring.*
2. *If, in addition, the operation "$\cdot$" admits a neutral element, then $(A, +, \cdot)$ is called a unital ring.*

Example 1.6.

1. *We know that $(\mathbb{Z}, +)$ is an abelian group, and we know that the usual multiplication "$\cdot$" is associative and distributive with respect to the usual addition "$+$" in $\mathbb{Z}$. Therefore, $(\mathbb{Z}, +, \cdot)$ is a ring.*

   Moreover, the second operation "$\cdot$" is commutative and has 1 as a neutral element, so $(\mathbb{Z}, +, \cdot)$ is a commutative and unital ring.
2. *Similarly, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are unital, commutative rings.*

1.3.1 Some computation rules

Proposition 1.2. *Let $(A, +, \cdot)$ be a ring with neutral element 0. Then :*

1. $\forall x \in A : \ x \cdot 0 = 0 = 0 \cdot x$
2. $\forall x, y \in A : \ (-x) \cdot y = -(x \cdot y) = x \cdot (-y)$
3. $\forall x, y \in A : \ (-x) \cdot (-y) = x \cdot y$
4. *If the ring has a unity 1, then* $\forall x \in A : \ -x = (-1) \cdot x$.

1.3.2 Integral Domain

Definition 1.7. *A ring $(A, +, \cdot)$ is called an integral domain if*

$$\forall x, y \in A : \big(x \cdot y = 0 \ \Rightarrow \ (x = 0 \ \vee \ y = 0)\big).$$

Example 1.7. *The structures $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are integral domains.*

1.4 Field Structure

Definition 1.8. *Let $(K, +, \cdot)$ be a unital ring. We say that $(K, +, \cdot)$ is a field if :*

1. $1_K \neq 0_K$
2. *Every element of $K \setminus \{0_K\}$ is invertible with respect to the operation "$\cdot$".*
   The field is called commutative if the operation "$\cdot$" is commutative.

Example 1.8.

1. *The structures $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are commutative fields.*
2. *The structure $(\mathbb{Z}, +, \cdot)$ is not a field, because the only invertible elements in $\mathbb{Z}^*$ with respect to usual multiplication are 1 and -1.*