Chapter 4

Algebraic Structures

4.1 Internal Composition Law

Definition 4.1.1

An internal composition law (LCI) on a set E is any function $\star : E \times E \to E$. A subset F of E is said to be "stable" with respect to the law if

$$\forall x, y \in F;\ x \star y \in F.$$

Example 4.1.2

1. $\cap$ and $\cup$ are internal composition laws on $P(E)$.
2. The sum " $+$ " and the product " $\cdot$ " are $LCIs$ on $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, but not on $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$.
3. The difference " $-$ " on $\mathbb{R}$, $\mathbb{C}$.
4. The composition " $\circ$ " of mappings defined on F into F.

Example 4.1.3

Let

$$E = \{1,\ 2,\ 3\},$$

and

$$F = \{\{1,2\},\ \{2,3\},\ \{1,3\}\} \subset P(E).$$

F is not stable with respect to the intersection $\cap$ and the union $\cup$ because :

$$\exists \{1,2\},\ \{2,3\} \in F,\ \{1,2\} \cap \{2,3\} = \{2\} \notin F,$$

$$\exists \{1,2\},\ \{2,3\} \in F,\ \{1,2\} \cup \{2,3\} = \{1,2,3\} \notin F,$$

Definition 4.1.4

Let $\star$ and $\triangle$ be two internal composition laws (LCI) on a set E, we say that :

1. It is commutative if :
$$\forall x, y \in E, \quad x \star y = y \star x.$$
2. It is associative if :
$$\forall x, y \in E, \quad (x \star y) \star z = x \star (y \star z).$$
3. Exists $e \in E$ is a left neutral element (respectively right neutral) of the law if
$$\forall x \in E; e \star x = x\ (respectively x \star e = x).$$

If e is a neutral element both on the left and right of $\star$ we say that e is a neutral element of $\star$.

4. Let $e \in E$ be a neutral element, we say that an element $x \in E$ is invertible, or symmetric, on the right (respectively on the left) if

$$\exists x' \in E, \quad x \star x' = e \ (respectively x' \star x = e).$$

We say x is invertible (or symmetrical) if it is invertible on the right and on the left of $\star$. and x' is called an inverse (or a symmetric) on the right (respectively on the left) of x.

5. $\star$ is distributive with respect to $\triangle$ if :

$$\forall x, y, z \in E, x \star (y \triangle z) = (x \star y) \triangle (x \star z) \quad \text{and} \quad (y \triangle z) \star x = (y \star x) \triangle (z \star x).$$

6. We say that an element $r \in E$ is right-regular (respectively left-regular) of *Soit* if

$$\forall x, y \in E, x \star r = y \star r \Rightarrow x = y.$$

$$(respectively \forall x, y \in E, r \star x = r \star y \Rightarrow x = y).$$

Example 4.1.5

1. The sum and the product on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are associative and commutative, and have respective neutral elements 0 and 1.
2. The difference is neither associative nor commutative on $\mathbb{R}$.
3. The composition " $\circ$ " is associative, but not commutative on mappings defined from F into F , it has a neutral element, which is the application Id_F.
4. The laws $\cap$, $\cup$, $\triangle$ on $P(E)$ are associative and commutative. They have respective neutral elements E, ϕ, ϕ.

Note 4.1.6

1. If $\star$ is an associative internal composition law on E that has a neutral element, then this neutral element is unique
2. The neutral element e is invertible (or symmetrical) and its unique inverse (or symmetric) is e.
3. If the symmetric element x' of x exists, it is unique. It is generally denoted by x^{-1}.

4.2 Groups

Definition 4.2.1

A group is a non-empty set G equipped with an internal composition law $\star$, denoted $(G, \star)$ such that :

1. $\star$ is associative ;
2. $\star$ has a neutral element e.
3. every element of G is symmetrical (has a symmetrical) for $\star$.

If it is commutative, we say that $(G, \star)$ is commutative, or abelian.

Example 4.2.2

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ endowed with the sum are abelian groups.
2. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ endowed with the product are abelian groups.
3. $P(E)$ endowed with $\triangle$ is an abelian group.

Example 4.2.3

The following pairs are not groups.

1. $(\mathbb{N},+)$, $(\mathbb{R},\times)$, $(\mathbb{Z},\times)$.
2. $(P(E),\cap)$, $(P(E),\cup)$.

4.2.1 Subgroups

Definition 4.2.4

A subgroup of a group $(G,\star)$ is a non-empty subset H of G such that :

1. $\star$ induces an internal composition law on H.
2. H equipped with this law is a group. In practice, to show that a non-empty subset H of G constitutes a subgroup, it suffices to verify one of the following propositions :

Proposition 4.2.5

Let $(G,\star)$ be a group and $H \subset G$ then, H is a subgroup of

$$G \Leftrightarrow \begin{cases} i) & H \neq \phi, \\ ii) & \forall x,y \in H, \quad x \star y \in H, (H \text{ is closed under } \star), \\ iii) & \forall x \in H, \quad x^{-1} \in H, (x^{-1} \text{ is the inverse of } x.) \end{cases}$$

Proposition 4.2.6

Let $(G,\star)$ be a group and $H \subset G$. Then, H is a subgroup of

$$G \Leftrightarrow \{\ i)\ H \neq \phi \quad ii)\ \forall x,y \in H, \quad x \star y^{-1} \in H$$

Note 4.2.7

If e is the neutral element of a group $(G,\star)$, then every subgroup of G contains e and we deduce the following property :

Proposition 4.2.8

Let $(G,\star)$ be a group, e the neutral element of $\star$ and H a subset of G. Then, H is a subgroup of

$$G \Leftrightarrow \{\ i)\ e \in H \quad ii)\ \forall x,y \in H, \quad x \star y^{-1} \in H$$

Example 4.2.9

1. Consider the group $(\mathbb{C}^*\ ,\ \times\ )$. Let

$$U = \{z \in \mathbb{C};\ \ |z| = 1\}.$$

   Show that U is a subgroup of $\mathbb{C}^*$

2. Let $n \in \mathbb{N}$,

$$n\mathbb{Z} = \{np,\ p \in \mathbb{Z}\},$$

   is a subgroup of $(Z,+)$.

Solution

1. (a) $|1| = 1$. Thus, $1 \in U$. Hence $U \neq \phi$.

   (b) Let

   $$z_1 z_2 \in U, \quad \left|z_1 \times z_2^{-1}\right| = \left|\frac{z_1}{z_2}\right| = \frac{1}{1} = 1 \Rightarrow z_1 \times z_2^{-1} \in U.$$

   Therefore, $(U\ , \times)$ is a subgroup of $(\mathbb{C}^*\ , \times\ )$.

2. (a) We have $0 \in n\mathbb{Z}$ because

   $$\exists p = 0, \quad n \times 0 = 0 \in n\mathbb{Z}.$$

   Thus $n\mathbb{Z} \neq \phi$.

   (b) For all

   $$x, y \in n\mathbb{Z},\ \exists p_1, p_2 \in \mathbb{Z}, x = np_1, y = np_2.$$

   Then,

   $$x - y = np_1 - np_2 = n(p_1 - p_2) = nh,$$

   with

   $$h = p_1 - p_2 \in \mathbb{Z}.$$

   Therefore $x - y \in nZ$. So, $(n\mathbb{Z}, +)$ is a subgroup of $(Z, +)$.

4.2.2 Group Homomorphisms

Definition 4.2.11

Let $(G, \star)$ and $(G^{'}, T)$ be two groups. A function f from G to $G^{'}$ is a "group homomorphism" when :

$$\forall x, y \in G, \quad f(x \star y) = f(x) T f(y).$$

— If $G = G'$ and $\star = T$, it is called an endomorphism.
— If f is bijective, it is called an isomorphism.
— If f is a bijective endomorphism, it is called an automorphism.

Example 4.2.12

1. $x \to 2^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$.
2. $x \to 2x$ is an automorphism of $(\mathbb{R}, +)$.
3. $x \to 3 \ln x$ is an isomorphism from $(\mathbb{R}_+^*, \times)$ to $(\mathbb{R}, +)$.
4. $z \to |z|$ is a homomorphism from $(\mathbb{C}^*, \times)$ to $(\mathbb{R}_+^*, \times)$.

Example 4.2.13

Show that the composition of two group homomorphisms is a group homomorphism.

Proposition 4.2.14

Let e, e' be the neutral elements of G and G' respectively. Let $f : G \to G'$ be a group homomorphism. Then,

1. $f(e) = e'$.
2. $\forall x \in G\,;\ f(x^{-1}) = (f(x))^{-1}$ (x^{-1} is the inverse of x).

Proposition 4.2.15

Let $f : (G; *) \to (G'; T)$ be a group homomorphism. Then,

1. The image of a subgroup of G under f is a subgroup of G'.
2. The inverse image of a subgroup of G' under f is a subgroup of G.

Proof

1. Let H be a subgroup of G and show that $f(H)$ satisfies the two conditions of the subgroup characterization.
   (a) Since H is a subgroup of G, then $e \in H$ hence $f(e) \in f(H)$, therefore $f(H) \neq \phi$.
   (b) Let $x', y' \in f(H)$, then there exist $xy \in H$ such that $x' = f(x)$ and $y' = f(y)$, thus according to the second property. We have
   $$x'T(y')^{-1} = f(x)T(f(y))^{-1} = f(x)Tf(y^{-1}) = f(x * y^{-1}),$$
   and since H is a subgroup of G then $(x * y^{-1}) \in H$. Hence
   $$x'T(y')^{-1} = f(x * y^{-1}) \in f(H).$$
   From i) and ii) we deduce that $f(H)$ is a subgroup of G'.
2. Let H' be a subgroup of G'. Then,
   (a) According to the first property $f(e) = e'$ and since H' is a subgroup of G' then $e' \in H'$. Hence
   $$e \in f^{-1}(H').$$
   (b) Let $x, y \in f^{-1}(H')$, then $f(x), f(y) \in H'$ and since H' is a subgroup of G'. Then $f(x)T(f(y))^{-1} \in H'$ and from the second property we deduce that
   $$f(x * y^{-1}) = f(x)Tf(y^{-1}) = f(x)T(f(y))^{-1} \in H',$$
   which shows that
   $$(x * y^{-1}) \in f^{-1}(H').$$
   From i) and ii) we deduce that $f^{-1}(H')$ is a subgroup of G.

4.2.3 The kernel and image of a homomorphism

Definition 4.2.16

Let f be a homomorphism from G to G', e, e' are the neutral elements of G, G' respectively :

1. The kernel of f, denoted $\ker f$, is the set defined by :
   $$\ker f = \{x \in G,\ f(x) = e'\} = f^{-1}(e').$$
2. The image of f, denoted $\text{Im } f$, is the set defined by :
   $$\text{Im } f = \{f(x),\ x \in G\} = f(G).$$

Proposition 4.2.17

As special cases of proposition 4.2.15. We have :

1. $\text{Im } f$ is a subgroup of (G', T),
2. $\ker f$ is a subgroup of $(G, *)$. The following result is much more interesting, as it greatly reduces the work to show that a homomorphism is bijective.

Proposition 4.2.18

Let $f : (G, *) \to (G', T)$ be a group homomorphism. Then,

1. f is injective if and only if $\ker f = \{e\}$, (where e is the neutral element of G).
2. f is surjective if and only if Im $f = G'$.

4.3 Ring Structure

Definition 4.3.1

A set A equipped with two internal composition laws $+$ and $\times$ is called a ring if :

1. $(A, +)$ is an abelian group (the neutral element of $+$ is denoted by 0 or 0_A).
2. $\times$ is associative and distributive with respect to $+$.
   (a) If furthermore $\times$ is commutative, then $(A, +, \times)$ is called a commutative ring.
   (b) If A has a neutral element for $\times$, it is denoted by 1 or 1_A, and $(A, +, \times)$ is called a unitary ring.

Example 4.3.2

The sets $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are unitary commutative rings.

Example 4.3.3

Consider the quotient set of $\mathbb{Z}$ by the congruence relation modulo n, defined in example 4.3.2

$$\mathbb{Z}/n\mathbb{Z} = \overline{0}, , \overline{1}, , \overline{2}, , ..., , \overline{n-1}.$$

We define on this set the two internal composition laws "$+$" and "$\times$" as :

$$\forall p, q \in \mathbb{Z}/n\mathbb{Z} : \ \overline{p} + \overline{q} = \widehat{\overline{p+q}} \text{ and } \overline{p} \times \overline{q} = \widehat{\overline{p \times q}},$$

where $+$ and $\times$ are the addition and multiplication defined on $\mathbb{Z}$ respectively. It can be easily verified that for all $n \in \mathbb{N}$, the quotient set $\mathbb{Z}/n\mathbb{Z}$ equipped with the two operations "$+$" and "$\times$" forms a structure of unitary commutative ring, where 0 and 1 are the neutral elements of "$+$" and "$\times$" respectively.

4.3.1 Subring

Definition 4.3.4

Let $(A, +, \times)$ be a ring. A non-empty subset A' of A is a subring of A when :

1. $1_A \in A$,
2. the laws $+$ and $\times$ induce internal composition laws on A', and with these laws, $(A', +, \times)$ is a ring.

Practically, to show that a non-empty subset A' of A is a subring, it suffices to verify the following proposition :

Proposition 4.3.5

Let $(A, +, \times)$ be a ring and $A' \subset A$. Then, A' is a subring of A

$$\Leftrightarrow \begin{cases} i) A' \neq \emptyset \\ ii) \forall x, y \in A' : x - y \in A' \\ iii) \forall x, y \in A' : x \times y \in A' \end{cases}$$

4.3.2 Ring Homomorphisms

Definition 4.3.6

Let $(A, +, \times)$ and $(B, \oplus, \otimes)$ be two rings and $f : A \to B$. We say that f is a ring homomorphism if :

$$\forall x, y \in A : f(x + y) = f(x) \oplus f(y) \text{ and } f(x \times y) = f(x) \otimes f(y)$$

1. If $A = B$, we say that f is an endomorphism of the ring A.
2. If f is bijective, we say that f is an isomorphism of rings.
3. If f is bijective and $A = B$, we say that f is an automorphism of rings.

Example 4.3.7

Let $z \mapsto \overline{z}$ is an automorphism of rings of $\mathbb{C}$.

Example 4.3.8

Show that the composition of two ring homomorphisms is a ring homomorphism.

4.3.3 Zero Divisors, Invertible Elements

Definition 4.3.9

Let $(A, +, \times)$ be a commutative ring. If there exist in the ring A two elements a and b such that :

$$(a \times b = 0) \wedge (a \neq 0 \wedge b \neq 0).$$

Then a and b are called zero divisors.

Definition 4.3.10

We call a ring integral or complete, any ring that does not contain a zero divisor other than 0 itself, that is :

$$ab = 0 \Leftrightarrow a = 0 \text{ or } b = 0.$$

Example 4.3.11

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, are integral rings.
2. The ring of matrices $M_n(\mathbb{k})$ equipped with the operations $+$ (matrix addition) and $\times$ (matrix multiplication) is not integral, because :

$$\exists A = \begin{pmatrix} 0 & -1 \\ 0 & 5 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}),$$

$$\exists B = \begin{pmatrix} 2 & -3 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}).$$

But

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definition 4.3.12

Let $(A, +, \times)$ be a commutative ring. We say that $x \in A$ is invertible if it has a multiplicative inverse.

Example 4.3.13

1. In $\mathbb{Z}$, the invertible elements are 1 and -1.
2. In the rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, all non-zero elements are invertible.

Proposition 4.3.14

In a commutative ring $(A, +, \times)$:

1. 0_A is never invertible.
2. If x is invertible, then it is not a zero divisor.
3. If $x_1, x_2, y \in A$ are integral, with $y \neq 0$ and $x_1 y = x_2 y$, then $x_1 = x_2$.

We say that "we can simplify" (which does not mean divide) by $y \neq 0$: $x_1 y = x_2 y \Rightarrow (x_1 - x_2)y = 0 \Rightarrow x_1 - x_2 = 0$ or $y = 0$ because A is integral $\Rightarrow x_1 = x_2$, since $y \neq 0$.

4.3.4 Ideals

Let $(A, +, \times)$ be a ring.

Definition 4.3.15

A right (respectively left) ideal of the ring A is any subset $I \subset A$ such that :

1. I is a subgroup of $(A, +)$,
2. $\forall x \in A$, $\forall y \in I$, $x \times y \in I$ (respectively $y \times x \in I$) :
   (a) If I is both a right and left ideal of A, we call I a "two-sided ideal" of A.
   (b) If the ring A is commutative, every ideal of A is two-sided, and in this case, we only talk about ideals without specifying whether they are right, left, or two-sided.

Example 4.3.16

1. Let $(A, +, \times)$ be a ring, then $I = 0_A$ is a two-sided ideal of A.
2. In the commutative ring $(\mathbb{Z}, +, \times)$, $n\mathbb{Z}$ is an ideal.

Definition 4.3.17

We call principal ideal of a commutative ring $(A, +, \times)$, any ideal I of A such that :

$$\exists x \in A,\ I = xA.$$

The ring A is said to be principal if all its ideals are principal.

4.4 Fields

Definition 4.4.1

An associative ring with unity $(\mathbb{k}, +, \times)$ is called a field if every nonzero element of $\mathbb{k}$ is invertible. If $\mathbb{k}$ is commutative as well, we call $\mathbb{k}$ a commutative field. It is noteworthy that in practice, all fields used are commutative.

Example 4.4.2

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are fields.

Proposition 4.4.3

Every field is an integral domain.

Proof

Let $a \in A$ and consider the ring homomorphism $A \to A$, $x \mapsto ax$. Then this ring homomorphism is injective, as its kernel is reduced to 0_A since A is an integral domain.
Since A is finite, this homomorphism is necessarily bijective, and thus there exists $x \in A$ such that $ax = 1_A$. By the commutativity of A, we also have $xa = 1_A$, and thus a has an inverse. Consequently, A is a field.

4.4.1 Subfields

Definition 4.4.4

A subfield of a field $(\mathbb{k}, +, \times)$ is any subset $\mathbb{k}'$ of $\mathbb{k}$ such that, equipped with the restrictions of the operations $+$ and $\times$, it forms a field.

Proposition 4.4.5

$\mathbb{k}' \subset \mathbb{k}$ is a subfield of $(\mathbb{k}, +, \times)$ if and only if

1. $\mathbb{k}' \neq \emptyset$.
2. $\forall x, y \in \mathbb{k}'$, $x - y \in \mathbb{k}'$ and $xy^{-1} \in \mathbb{k}'$. We also have the following characterization of fields.

Proposition 4.4.6

Let $(\mathbb{k}, +, \times)$ be a commutative ring with unity. Then $\mathbb{k}$ is a field if and only if the only ideals of $\mathbb{k}$ are $0_{\mathbb{k}}$ and $\mathbb{k}$ itself.

Example 4.4.7

$(\mathbb{Z}, +, \times)$ is not a field because the only ideals in $\mathbb{Z}$ are $0_{\mathbb{k}}$, $n\mathbb{Z}$ and $\mathbb{Z}$.

Example 4.4.8

Consider the quotient ring $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ defined in example 4.3.3 In this ring, we consider the cases $n = 2$, 3, 4.
For instance, let's write down the multiplication tables for the three quotient sets $\mathbb{Z}2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$.

1. In $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, the table is :

$\dot{\times}$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$

2. In $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, the table is :

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{1}$

3. In $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$, the table is :

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

From these tables, we observe that all nonzero elements in $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are invertible, thus $(\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times})$ and $(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times})$ are commutative fields. However, in $\mathbb{Z}/4\mathbb{Z}$, only elements 1 and 3 are invertible, while 2 is not. Therefore, $(\mathbb{Z}/4\mathbb{Z}, \dot{+}, \dot{\times})$ is not a field.

More generally, it can be shown that a necessary and sufficient condition for the ring $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ to be a field is that the natural number n is a prime number.