# Chapter 3

# Algebraic Structures

## 3.1 Law of internal composition

**Definition 3.1.1.**
*Let $E$ be a non-empty set.*

1. *A **law of internal composition** on $E$ is a function from $E \times E$ to $E$. If $T$ denotes this function, then the image of the pair $(x, y) \in E \times E$ under $T$ is denoted as $xTy$.*
2. ***A structured set** is any pair $(E, T)$ where $E$ is a non-empty set and $T$ is a law of internal composition on $E$.*

**Example 3.1.1.**
*The most common internal composition laws are:*

1. $+$ *in* $\mathbb{N}, \mathbb{N}^*, \mathrm{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, *but not in* $\mathrm{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$
2. $-$ *in* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
3. $\times$ *in* $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
4. $/$ *in* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$
5. $\circ$ *(composition of functions) defined on the set of functions from* E *to* $E$.
6. *The law* $\oplus$ *defined on* $\mathbb{R}^2$ *by* $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
7. *The law* $T$ *defined on* $\mathbb{R}$ *by* $xTy = x + y - xy$

8. *The laws $\cup$, $\cap$ (union, intersection) defined on $P(E)$ (power set of a set $E$)*

**Definition 3.1.2.** *(Properties of laws)*
*Let $(E, T)$ be a structured set.*

1. *The law $T$ is called **associative** on $E$ if $(xTy)Tz = xT(yTz)$ for all $x, y, z$ in $E$.*

2. *The law $T$ is called **commutative** on $E$ if $xTy = yTx$ for all $x, y$ in $E$.*

**Example 3.1.2.**
*Addition and multiplication are associative and commutative on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.*

**Definition 3.1.3.** *(Properties of laws)*
*Let $(E, T)$ be a structured set.*

1. *An element $e$ of $E$ is called **neutral** for the law $T$ if,*

$$\forall x \in E,\ xTe = eTx = x.$$

2. *If $(E, T)$ has a neutral element $e$, then an element $x$ of $E$ is said to be invertible (or symmetrizable) for the law $T$ if there exists an element $x'$ in $E$ such that:*

$$xTx' = x'Tx = e$$

*The element $x'$ is then called the symmetric element of $x$ for the law $T$.*

**Proposition 3.1.1.**
*Let $(E, T)$ be a structured set. If the neutral element of $E$ for the law $T$ exists, then it is unique.*

**Proof 3.1.1.**
*Suppose there exist two neutral elements $e$ and $e'$. Then,*

$$e' = eTe' = e$$

*which implies $e = e'$.*

**Proposition 3.1.2.**
*Let $(E, T)$ be a structured set where the law $T$ is associative and has a neutral element.*

1. *If $x \in E$ is symmetrizable, then its symmetric element is unique.*
2. *If $x \in E$ and $y \in E$ are symmetrizable, then $xTy$ is symmetrizable and its symmetric element $(xTy)'$ is given by $(xTy)' = y'Tx'$ where $x'$ denotes the symmetric element of $x$ and $y'$ denotes the symmetric element of $y$.*

**Proof 3.1.2.**

1. *Let's suppose an element $x$ has two symmetric elements $x'$ and $x''$. Then,*

$$xTx' = e \Rightarrow x''T(xTx') = x'' \Rightarrow (x''Tx)Tx' = x'' \Rightarrow x' = x''.$$

2. *We have*

$$(y'Tx')T(xTy) = y'T(x'Tx)Ty = y'Ty = e.$$

*Also,*

$$(xTy)T(y'Tx') = xT(yTy')Tx' = xTx' = e.$$

*Thus, $(xTy)' = y'Tx'$.*

## 3.2 Groups

### 3.2.1 Group Structure

**Definition 3.2.1.**
*Let $(G, T)$ be a structured set.*

1. *We say that $(G, T)$ is a **group** if*
   (a) *the operation $T$ is associative on $G$,*
   (b) *there exists a neutral element for the operation $T$ in $G$,*
   (c) *every element of $G$ is symmetrizable for the operation $T$.*

   *We also say that the set $G$ has a **group structure** for the operation $T$.*
2. *We say that the group $(G, T)$ is **commutative (or abelian)** if the operation $T$ is commutative on $G$.*

**Example 3.2.1.**
*First, examples of groups are provided:*

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *equipped with addition.*
2. $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ *equipped with multiplication.*

**Example 3.2.2.**
*For various reasons (to be determined), the following pairs are not groups:*

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

### 3.2.2 Subgroups

**Definition 3.2.2.** *(Subgroups)*
*A* ***subgroup*** *of a group $(G, *)$ is a non-empty subset $H$ of $G$ such that:*

1. $*$ *induces an internal composition law on $H$.*
2. *With this law, $H$ forms a group. We denote this as $H < G$.*

**Proposition 3.2.1.**
*The subset $H \subset G$ is a* ***subgroup*** *of a group $(G, *)$ if and only if*

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y \in H$,
3. $\forall x \in H,\ x^{-1} \in H$.

**Example 3.2.3.**

1. *Let $(G, *)$ be a group. Then $G$ and $\{e_G\}$ are subgroups of $G$.*
2. *$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.*

**Proposition 3.2.2.**
*The subset $H \subset G$ is a subgroup of a group $(G, *)$ if and only if*

1. $H \neq \varnothing$,

2. $\forall (x, y) \in H^2,\ x * y^{-1} \in H$.

**Proposition 3.2.3.**
*The intersection of any family of subgroups of a group $(G, *)$ is a subgroup of $(G, *)$.*

**Proof 3.2.1.**
*Let $(H_i)_{i \in I}$ be a family of subgroups of a group $G$. Define $K = \bigcap_{i \in I} H_i$, the intersection of all $H_i$. The set $K$ is non-empty since it contains the identity element $e$, which belongs to each subgroup $H_i$. Let $x$ and $y$ be two elements of $K$. For every $i \in I$, we have $x * y^{-1} \in H_i$ because $H_i$ is a subgroup. Therefore, $x * y^{-1} \in K$. This proves that $K$ is a subgroup of $G$.*

**Remark 3.2.1.**
*The arbitrary union of subgroups of a group $(G, *)$ is not necessarily a subgroup of $(G, *)$.*

**Example 3.2.4.**
*Let $T$ be the internal composition law defined on $\mathbb{R}^2$ by*

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2, \quad (x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

*We have $(\mathbb{R}^2, T)$ is a group, $\mathbb{R} \times \{0\}$ and $\{0\} \times \mathbb{R}$ are two subgroups of $(\mathbb{R}^2, T)$ but $\mathbb{R} \times \{0\} \cup \{0\} \times \mathbb{R}$ does not form a subgroup of $(\mathbb{R}^2, T)$.*

**Proposition 3.2.4.**
*The union of two subgroups $H$ and $K$ of the same group $(G, *)$ is a subgroup $(H \cup K < G)$ if and only if $H \subset K$ or $K \subset H$.*

**Proof 3.2.2.**
*Suppose $H \cup K$ is a subgroup of $G$ and $H$ is not included in $K$, meaning there exists $h \in H$ such that $h \notin K$. Let's show that $K \subset H$. Take any $k \in K$. We have $h * k \in H \cap K$. However, $h * k \notin K$ because otherwise $h = (h * k) * k' \in K$. Hence, $h * k \in H$, implying $k = h' * (h * k) \in H$.*

### 3.2.3 Examples of Groups

#### 3.2.3.1 The Group $\mathbb{Z}/n\mathbb{Z}$

It is initially clear that if $n$ is a positive integer (which we can assume to be positive and non-zero), the set $n\mathbb{Z}$ consisting of integers of the form $nk$, where $k$ ranges over $\mathbb{Z}$ (the set of multiples of $n$), is an additive subgroup of $(\mathbb{Z}, +)$.

**Proposition 3.2.5.**
*Every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$.*

**Proof 3.2.3.**
*Let $S$ be a subgroup of $\mathbb{Z}$ other than $\{0\}$ and $\mathbb{Z}$. Hence, $S$ does not contain 1. The set of positive integers in $S$, denoted by $S^+$, has a smallest element $n$ which is at least 2 (since $S$ is countable and bounded below). Every integer of the form $kn$, where $k$ is a natural number, belongs to $S$ (clear from induction since $kn = n + n + \ldots + n$). Therefore, $S$ contains $n\mathbb{Z}$.*

*By Euclidean division, every positive integer in $S^+$ that is not of the form $kn$ can be written as $a = kn + r$, where $0 < r < n$. It follows that $r = a - kn > 0$. Since both $a$ and $kn$ are in $S^+$, $r$ must also be in $S^+$. This contradicts $n$ being the smallest element of $S^+$, hence $r = 0$. This shows that $S = n\mathbb{Z}$.*

We easily show that the congruence relation modulo $n$, where $n \in \mathbb{N}$, due to Gauss, denoted by $\equiv$, is defined as:

$$\forall x, y \in \mathbb{Z}, \quad x \equiv y[n] \Leftrightarrow (x - y) \in n\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}, \quad y = x - nk.$$

$x \equiv y[n]$ reads as "$x$ is congruent to $y$ modulo $n$," which is an equivalence relation defined in $(\mathbb{Z}, +)$. The quotient set is finite and can thus be written:

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \widehat{\dot{n-1}}\}.$$

For example: $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$, and $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

- Quotient addition on $\mathbb{Z}/n\mathbb{Z}$ induced by $\mathbb{Z}$ is:

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z}, \quad \dot{x} + \dot{y} = \widehat{\dot{x + y}}.$$

- Quotient multiplication on $\mathbb{Z}/n\mathbb{Z}$ induced by $\mathbb{Z}$ is:

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z}, \quad \overset{\bullet}{x} \overset{\bullet}{\times} \overset{\bullet}{y} = \overset{\bullet}{\widehat{x \times y}}.$$

**Proposition 3.2.6.**
*The set $(\mathbb{Z}/n\mathbb{Z}, \overset{\bullet}{+})$ is a commutative additive group (the quotient group of $\mathbb{Z}$ by the congruence relation).*

**Proof 3.2.4.** *Leave it to the reader.*

#### 3.2.3.2 Group of Permutations

**Definition 3.2.3.**
*Let $E$ be a set. A permutation of $E$ is a bijection from $E$ to itself. We denote by $S_E$ the set of permutations of $E$. If $E = \{1, \ldots, n\}$, we simply denote it by $S_n$. The set $S_E$, equipped with the composition of mappings, forms a group with identity $e = id$, called the symmetric group on the set $E$.*

**Example 3.2.5.**
*Let's assume $E = \{1, 2, 3, 4, 5\}$. A permutation $\sigma \in S_5$ is represented as follows:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

*which means $\sigma(1) = 3$, $\sigma(2) = 5$, and so on.*

### 3.2.4 Group Homomorphisms

**Definition 3.2.4.**
*Let $(G, *)$ and $(H, T)$ be two groups. A function $f$ from $G$ to $H$ is a **group homomorphism** if:*

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

*Moreover:*

1. *If $G = H$ and $* = T$, it is called an **endomorphism**.*
2. *If $f$ is bijective, it is an **isomorphism**.*

3. *If $f$ is a bijective endomorphism, it is an* ***automorphism****.*

**Example 3.2.6.**
*The map $x \mapsto 2x$ defines an automorphism of $(\mathbb{R}, +)$.*

**Example 3.2.7.**
*The function $f : \mathbb{R} \to \mathbb{R}_+^*$, where $\mathbb{R}_+^*$ is the set of positive real numbers under multiplication, defined by $f(x) = \exp(x)$, is a group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$ because $\exp(x + y) = \exp(x) \times \exp(y)$ for all $x, y \in \mathbb{R}$.*

**Proposition 3.2.7.** *(Properties of Group Homomorphisms)*
*Let $f$ be a homomorphism from $(G, *)$ to $(H, T)$:*

1. $f(e_G) = e_H$.
2. $\forall x \in G, f(x^{-1}) = \big(f(x)\big)^{-1}$,
3. *If $f$ is an isomorphism, then its inverse $f^{-1}$ is also an isomorphism from $(H, T)$ to $(G, *)$.*
4. *If $G' < G$ (subgroup of $G$), then $f(G') < H$.*
5. *If $H' < H$ (subgroup of $H$), then $f^{-1}(H') < G$.*

**Definition 3.2.5.**
*Let $f$ be a homomorphism from $G$ to $H$:*

1. *The kernel of $f$, denoted $Ker(f)$, is the set of pre-images of $e_H$:*

$$Ker(f) = \{x \in G \mid f(x) = e_H\} = f^{-1}(\{e_H\}).$$

   *(Note: $f$ is not assumed to be bijective; hence there's no mention of the inverse bijection of $f$.)*

2. *The image of $f$, denoted $Im(f)$, is $f(G)$ (set of images by $f$ of elements of $G$).*

**Remark 3.2.2.**
*According to the last two points of proposition (3.2.7), the kernel and image of $f$ are respective subgroups of $G$ and $H$.*

**Proposition 3.2.8.**
*Let $f$ be a homomorphism from $(G, *)$ to $(H, T)$:*

1. *$f$ is surjective if and only if $Im(f) = H$.*

2. *$f$ is injective if and only if $Ker(f) = \{e_G\}$.*

**Proof 3.2.5.**
*The point (1) follows directly from the definition of surjectivity. To prove (2), suppose first that $f$ is injective. Let $x \in Ker(f)$. Then $f(x) = e_H$, and since $f(e_G) = e_H$ as stated, we conclude $f(x) = f(e_G)$, which implies $x = e_G$ by injectivity of $f$. Thus, $Ker(f) = \{e_G\}$. Conversely, suppose $Ker(f) = \{e_G\}$ and show that $f$ is injective. Consider $x, y \in G$ such that $f(x) = f(y)$. Then $f(x)Tf(y)' = e_H$, so $f(x * y') = e_H$, meaning $x * y' \in Ker(f)$. The assumption $Ker(f) = \{e_G\}$ then implies $x * y' = e_G$, hence $x = y$. Injectivity of $f$ is thus demonstrated, completing the Proof.*

## 3.3 Ring Structure

**Definition 3.3.1.**
***A ring*** *is a set equipped with two binary operations $(A, *, T)$ such that:*

1. *$(A, *)$ is a commutative group with identity element denoted by $0_A$.*

2. *The operation $T$ is associative and distributive on the left and right with respect to $*$:*

$$\forall x, y, z \in A, \quad xT(y * z) = xTy * xTz \quad \text{and} \quad (x * y)Tz = xTz * yTz.$$

3. *The operation $T$ has a neutral element different from $0_A$, denoted by $1_A$.*

**Example 3.3.1.**
*$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are well-known rings.*

**Remark 3.3.1.**

1. *If the operation $T$ is commutative, the ring is called commutative or abelian.*

2. *The set $A - \{0_A\}$ is denoted by $A^*$.*

3. *For simplicity, we temporarily use the additive $(+)$ and multiplicative $(\times)$ notations instead of the internal operations $*$ and $T$. Therefore, we refer to the ring $(A, +, \times)$ instead of $(A, *, T)$.*

**Definition 3.3.2.**

1. *A commutative ring* $(A, +, \times)$ *is called* ***integral*** *if it is*
   (a) *non-zero (i.e.,* $1_A \neq 0_A$*),*
   (b) $\forall (x, y) \in A^2, \quad x \times y = 0 \Rightarrow (x = 0 \text{ or } y = 0)$.
2. *When a product* $a \times b$ *is zero but neither* $a$ *nor* $b$ *is zero,* $a$ *and* $b$ *are called zero divisors.*

**Example 3.3.2.**

1. $(\mathbb{Z}, +, \times)$ *of integers is integral: it has no zero divisors.*
2. *The ring* $\mathbb{Z}/6\mathbb{Z}$ *of residue classes modulo* 6 *is not integral because* $\overset{\bullet}{2} \times \overset{\bullet}{3} = \overset{\bullet}{6}$*, hence* $\overset{\bullet}{2} \times \overset{\bullet}{3} = \overset{\bullet}{0}$*. Similarly,* $\mathbb{Z}/4\mathbb{Z}$*.*

**Proposition 3.3.1.**
*Let* $(A, +, \times)$ *be a ring. The following rules apply in rings:*

1. $x \times 0_A = 0_A \times x = 0_A$*. The element* $0_A$ *is absorbing for the operation* $\times$*.*
2. $\forall (x, y) \in A^2, \quad (-x) \times y = x \times (-y) = -(x \times y)$.
3. $\forall x \in A, \quad (-1_A) \times x = -x$.
4. $\forall (x, y) \in A^2, \quad (-x) \times (-y) = x \times y$.
5. $\forall (x, y, z) \in A^3, \quad x \times (y - z) = x \times y - x \times z$ *and* $(y - z) \times x = y \times x - z \times x$.

**Proof 3.3.1.**

1. $x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A$*. Therefore, by the regularity of elements in the group* $(A, +)$*,* $x \times 0_A = 0_A$*. Similarly for the other side.*
2. $x \times y + (-x) \times y = (x + (-x)) \times y = 0_A \times y = 0_A$*. Thus,* $(-x) \times y = -(x \times y)$*. Similarly for the other equality.*
3. $(-1_A) \times x + x = (-1_A) \times x + 1_A \times x = (-1_A + 1_A) \times x = 0_A \times x = 0_A$*. Hence,* $(-1_A) \times x = -x$.

4. *Left to the reader.*

5. *Left to the reader.*

**Notations and Conventions**

Let $(A, *, T)$ be a ring. Let $n$ be a non-zero natural number and $x$ an element of $A$.

1. We denote by $nx$ the element of $A$ that is equal to the composition by the first operation $*$ of $n$ terms equal to $x$. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,
$$nx = \underbrace{x * x * \ldots * x}_{\text{n times}}.$$
In particular, for $n = 1$, we have $1 \cdot x = x$ for all $x \in A$.

2. Similarly, we denote by $x^n$ the element of $A$ that is equal to the composition by the second operation $T$ of $n$ terms equal to $x$. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,
$$x^n = \underbrace{xTxT \ldots Tx}_{\text{n times}}.$$
In particular, for $n = 1$, we have $x^1 = x$ for all $x \in A$.

3. What about $n = 0$? Let $0_A$ denote the zero element and $1_A$ denote the unit element of $(A, *, T)$ (this notation is somewhat unfortunate here because it recalls the additive notation and the multiplicative notation that we are precisely trying to avoid). Then, by convention, for all $x \in A$, $0 \cdot x = 0_A$ and $x^0 = 1_A$.

### 3.3.1 Subrings

**Definition 3.3.3.**

*Let $(A, *, T)$ be a ring. A non-empty subset $A_1$ of $A$ is a **subring** of $A$ if:*

1. $1_A \in A_1$;

2. *the operations $*$ and $T$ induce binary operations on $A_1$, and with these operations, $(A_1, *, T)$ is a ring.*

**Proposition 3.3.2.**

*A subset $A_1$ of $A$ is a subring if and only if:*

1. $(A_1, *)$ *is a subgroup of* $(A, *)$*;*
2. $1_A \in A_1$*;*
3. $\forall (x, y) \in A_1^2, \quad xTy \in A_1$ *(*$T$ *induces a binary operation on* $A_1$*).*

**Example 3.3.3.**
$(\mathbb{Z}, +, \times)$ *is a subring of* $(\mathbb{Q}, +, \times)$*, which is a subring of* $(\mathbb{R}, +, \times)$*, which is a subring of* $(\mathbb{C}, +, \times)$*.*

### 3.3.2 Ring Homomorphisms

**Definition 3.3.4.**
*Let* $(A, +_A, \times_A)$ *and* $(B, +_B, \times_B)$ *be two rings. A ring homomorphism from* $A$ *to* $B$ *is a function from* $A$ *to* $B$ *such that:*

1. $f(1_A) = 1_B$*;*
2. *for all* $x, y \in A$*,* $f(x +_A y) = f(x) +_B f(y)$ *and* $f(x \times_A y) = f(x) \times_B f(y)$*.*

### 3.3.3 Ideals in a Commutative Ring

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

**Definition 3.3.5.** *(Ideal)*
*A subset* $I$ *of* $A$ *is an ideal of a ring* $(A, +, \times)$ *if*

1. $(I, +)$ *is a subgroup of* $(A, +)$*,*
2. *for every* $a \in A$*, we have* $aI \subset I$*. In other words,* $\forall a \in A, \forall x \in I$*,* $ax \in I$*.*

**Proposition 3.3.3.**
*A subset* $I$ *of* $A$ *is an ideal of a ring* $(A, +, \times)$ *if and only if*

1. $I$ *contains the zero element* $0_A$*,*
2. *for all* $x, y \in I$*,* $x - y \in I$*,*
3. $\forall a \in A, \forall x \in I$*,* $ax \in I$*.*

**Example 3.3.4.**

1. *Any non-trivial ring has at least two ideals: the trivial ideal* $\{0\}$ *and* $A$ *itself. Ideals of* $A$ *that are distinct from* $A$ *are called proper ideals.*

2. *Any element* $x$ *of* $A$ *defines a principal ideal:* $\langle x \rangle = xA = \{ax \mid a \in A\}$. *It is the smallest ideal containing* $x$, *and we say it is generated by* $x$. *If* $x$ *is invertible (and only in this case),* $xA = A$.

3. *More generally, if* $x_1, \ldots, x_n \in A$, *the smallest ideal containing* $x_1, \ldots, x_n$ *is:*

$$\langle x_1, \ldots, x_n \rangle = x_1 A + \ldots + x_n A = \{a_1 x_1 + \ldots + a_n x_n \mid a_1, \ldots, a_n \in A\}.$$

*Indeed, it is immediately verified that* $I = x_1 A + \ldots + x_n A$ *is non-empty and stable under linear combinations, hence it is an ideal; and of course, any ideal containing the* $x_i$ *must contain* $I$. *We say* $I$ *is generated by* $\{x_1, \ldots, x_n\}$.

## 3.4 Field Structure

**Definition 3.4.1.** ***(Field)***

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

2. *Moreover, if the second operation* $\times$ *is commutative on* $K$, *then we say that the field* $(K, +, \times)$ *is commutative.*

**Example 3.4.1.**
$(\mathbb{Q}, +, \times)$ *and* $(\mathbb{R}, +, \times)$ *are commutative fields.*

**Definition 3.4.2.** ***Subfield***
*Let* $(K, +, \times)$ *be a field and let* $K_1$ *be a non-empty subset of* $K$.
*We say that* $K_1$ *is* ***a subfield*** *of* $K$ *if* $K_1$ *is stable under* $+$ *and* $\times$ *in* $K$, *and* $K_1$ *equipped with the induced operations from* $K$ *forms a field itself.*

**Example 3.4.2.**
$(\mathbb{Q}, +, \times)$ *is a subfield of* $(\mathbb{R}, +, \times)$.

**Proposition 3.4.1.**
*Let* $(K, +, \times)$ *be a field. A subset* $K_1$ *of* $K$ *is a subfield if and only if:*

1. $(K_1, +)$ *is a subgroup of* $(K, +)$,

2. *for all* $x, y \in K_1$, $x \times y \in K_1$ *(stability of* $K_1$ *under* $\times$*),*

3. $K_1$ *contains the identity element of* $K$*, and the inverse of every* $x \in K_1$ *in* $(K, \times)$ *is also an element of* $K_1$*.*