# Chapter 2

# Algebraic structures

## Groups

**Definition 27.** Let $G$ be a non empty set and $\cdot : G \times G \to G$ a mapping.
We say that $\cdot$ is a law of composition or a binary operation on $G$ and we write $a \cdot b = c$ instead of $\cdot(a, b) = c$.

**Example 16.**
$(+)$ is a law of composition on $\mathbb{N}$
$(-)$ is not a law of composition $\mathbb{N}$
$(*)$ is a law of composition on $\mathbb{N}$ with $x * y = x^2 + y^2$

**Definition 28.** Let $G$ be a non empty set and $\cdot$ a law of composition on $G$. We say that $(G, \cdot)$ is a group if the following conditions are satisfied:

1. The law of composition $(\cdot)$ is associative. i.e: $\forall x, y, z \in G, \ (x * y) * z = x * (y * z)$
2. $\exists e \in G, \ \forall x \in G / x * e = e * x = x$
3. For each element $x \in G$, there exists an inverse element $x^{-1} \in G$, , such that
$$x \cdot x^{-1} = x^{-1} \cdot x = e$$

If $\forall x, y \in G, x \cdot y = y \cdot x$,
$(G, \cdot)$ is said to be abelian or commutative.

**Lemma 1.**
The identity element $e$ is unique.
For each element $x \in G$, the inverse element $x^{-1}$ is unique.

**Example 17.**
$(\mathbb{Z}, +), (\mathbb{Q}, \times)$ are abelian groups.
$(\mathbb{Z}, \times), (\mathbb{N}, +)$ are not groups.

**Example 18.** $\left(\mathbb{R}^2, +\right)$ is a an abelian group.

**Example 19.** Let $E$ be a nonempty set. $\left(P(E), \cap\right)$ and $\left(P(E), \cup\right)$ are not groups.

**Example 20.** $\left(P(E), \Delta\right)$ is an abelian group.

**Theorem 10.** Let $(G, \cdot)$ be a group and $x, y \in G$

$$\boxed{(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}}$$

## Subgroups

**Definition 29.** Let $(G, \cdot)$ be a group.
A subset $H$ of $G$ is said to be a subgroup of $(G, \cdot)$ if and only if:

1. $H$ is non empty.
2. $\forall a, b \in H, a \cdot b \in H$
3. $\forall a \in H, a^{-1} \in H$

**Example 21.**

The set of even integers $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

The set of odd integers is not a subgroup of $(\mathbb{Z}, +)$.

## Cyclic groups

For $k \in \mathbb{Z}$, Let us denote $x^k = \underbrace{x \cdot x \cdots x}_{k\text{times}}$ when $k > 0$, $x^k = \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{k\text{times}}$ when $k < 0$
and $k^0 = e$ where $e$ is the identity element.

**Theorem 11.** Let $G$ be a group and $a$ be any element in $G$. Then the set $< a >= \{a^k : k \in Z\}$ is a subgroup of $G$.
$< a >$ is called the cyclic group generated by $a$.

**Example 22.** Consider the group $(\mathbb{Z}, +)$.
$< 5 >= \{x = 5n : \ n \in \mathbb{Z}\}$ is a cyclic group generated by $5$.

# Homomorphism

**Definition 30.** Let $(G, \cdot)$ et $(F, *)$ two groups and $f : G \to F$ a mapping.
We say that $f$ is a group homomorphism if and only if:

$$\forall x, y \in G, \ f(x \cdot y) = f(x) * f(y)$$

A bijective homomorphism is called an isomorphism. An automorphism is an isomorphism from $G$ to itself.

**Theorem 12.** Let $(G, \cdot)$ et $(F, *)$ be two groups and $f : G \to F$ a group homomorphism, then:

1. $f(e_1) = e_2$
2. $\forall x \in E, \ [f(x)]^{-1} = f(x^{-1})$

**Example 23.** Let $f : \mathbb{C} \to \mathbb{C}^*$ be a map such that $f(z) = e^z$.
$f$ is a group homomorphism from $(\mathbb{C}, +)$ to $(\mathbb{C}^*, \times)$. In fact,
$\forall z_1, z_2 \in \mathbb{C}, \ f(z_1 + z_2) = e^{z_1+z_2} = e^{z_1} \times e^{z_2} = f(z_1)f(z_2)$
We observe that $f(0) = 1$, and $f(1) = e \Rightarrow [f(1)]^{-1} = \dfrac{1}{e}$
On the other hand, $f(-1) = e^{-1} = \dfrac{1}{e} \Rightarrow [f(1)]^{-1} = f(-1)$