4.4.1 Subgroup

Definition 4.9. *Let* $(G, *)$ *. a non-empty subset* H *of* G *is a subgroup of* G *if :*

$$\begin{cases} \forall(a,b) \in H \times H & \Longrightarrow \quad a * b \in H.........(1) \\ \forall a \in H & \Longrightarrow \quad a' \in H........(2) \end{cases}$$

Example 4.9. *Let* $(\mathbb{Z}, +)$ *be a group, then* $3\mathbb{Z}$ *is a subgroup of* $\mathbb{Z}$*.*

We have :

$$\begin{aligned} 3\mathbb{Z} &= \{3z/z \in \mathbb{Z}\} \\ &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \end{aligned}$$

1. *Let* $a, b \in 3\mathbb{Z}$*, then* $\exists z_1 \in \mathbb{Z}$ *such that* $a = 3z_1$ *and* $\exists z_2 \in \mathbb{Z}$ *such that* $b = 3z_2$*, so* $a + b = 3(z_1 + z_2) \in 3\mathbb{Z}$*.*

2. *Let* $a \in 3\mathbb{Z}$*, then* $-a = -3z_1 = 3(-z_1) \in 3\mathbb{Z}$*.*

For (1) *and* (2)*, then* $3\mathbb{Z}$ *is a subgroup of* $\mathbb{Z}$*.*

Theorem 4.1. *Let* H *be a non-empty subset of a group* G*, then* H *is a subgroup of* G *if and only if :*

$$\forall(a,b) \in H \times H \Longrightarrow a * b' \in H.$$

4.4.2 Homomorphism

Definition 4.10. *For groups* $(G_1, *)$ *and* $(G_2, \top)$*, an homomorphisme from* $(G_1, *)$ *to* $(G_2, \top)$ *is defined as any function* $f : G_1 \longrightarrow G_2$ *such that:*

$$\forall(x,y) \in G_1^2 : \ f(x * y) = f(x) \top f(y).$$

Remark 4.3.

- *If f is bijective, it is refferred to as an isomorphism.*
- *An endomorphism is an homomorphism from* $(G_1, *)$ *to itself.*
- *An automorphism is a bijective endomorphism from* $(G_1, *)$ *to itself.*

Example 4.10. *The function*

$$\begin{array}{rcl} f:\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x)=2^x \end{array}$$

is an homomorphism from $(\mathbb{R},+)$ *to* $(\mathbb{R},\times)$ *because*

$$\begin{array}{rcl} \forall(x,y)\in\mathbb{R}^2 : f(x+y) & = & 2^{x+y} \\ & = & 2^x\times 2^y \\ & = & f(x)\times f(y). \end{array}$$

Definition 4.11. *Let* $(G_1,*)$ *and* $(G_2,\top)$ *be two groups, and* $f:G_1\longrightarrow G_2$ *is an homomorphism from* $(G_1,*)$ *to* $(G_2,\top)$.

1. *The kernel of* f *is referred as the set*

$$ker f=\{x\in G_1\,/\,f(x)=e_2\}.$$

2. *The image of* f *is referred as the set*

$$Im f=\{f(x)\in G_2\,/\,x\in G_1\}.$$

Theorem 4.2. *Let* f *be an homomorphism from* $(G_1,*)$ *to* $(G_2,\top)$*, then:*

1. $ker f$ *is a sub-group of* G_1.

2. $Im f$ *is a sub-group of* G_2.

3. f *is injective* $\Longleftrightarrow$ $ker f=\{e_1\}$.

4. f *is surjective* $\Longleftrightarrow$ $Im f=G_2$.

4.5 $\mathbb{Z}/n\mathbb{Z}$ *group*

Fixing $n\geqslant 1$. Recall that $\mathbb{Z}/n\mathbb{Z}$ is the set

$$\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\ldots,\overline{p},\ldots,\overline{n}\}$$

where $\overline{p}$ denotes the equivalence class of p modulo n. In other words:

$$\overline{p} = \overline{q} \Longleftrightarrow p \equiv q \ mod(n)$$

or alternatively

$$\overline{p} = \overline{q} \Longleftrightarrow \exists k \in \mathbb{Z} : p = q + kn.$$

We define in $\mathbb{Z}/n\mathbb{Z}$ two laws of composition :

- Addition :

$$\overline{p} + \overline{q} = \overline{p + q}$$

- Multiplication:

$$\overline{p} \cdot \overline{q} = \overline{p \cdot q}$$

Example 4.11. *In $\mathbb{Z}/6\mathbb{Z}$, we have*

Let $x, y \in \mathbb{Z}$

$$\begin{aligned} \overline{31} + \overline{46} &= \overline{31 + 46} \\ &= \overline{77} \\ &= \overline{5} \end{aligned}$$

and

$$\begin{aligned} \overline{31} \cdot \overline{46} &= \overline{31 \cdot 46} \\ &= \overline{1426} \\ &= \overline{4} \end{aligned}$$

Proposition 4.1. $(\mathbb{Z}/n\mathbb{Z}, +)$ *is a commutative group .*

4.6 Rings

Definition 4.12. *Let A be a set equipped with two internal composition laws, we say that A is a ring if:*

1. $(A, *)$ *is a commutative group .*

2. *The law* $\top$ *is associative.*

3. *The law* $\top$ *is distributive with respect to the operation* $*$.

Remark 4.4.
- *An ring* $(A, *, \top)$ *is called commutative if the operation* $\top$ *is commutative.*
- *An ring* $(A, *, \top)$ *is unitary if the operation* $\top$ *has a neutral element.*

Example 4.12.
1. $(\mathbb{Z}, +, \times)$ *is a commutative and unitary ring.*
2. $(\mathbb{R}, +, \times)$ *is a commutative and unitary ring.*

4.7 Field

Definition 4.13. *Let* $\mathbb{K}$ *be a set equipped with two internal composition laws, we say that* $\mathbb{K}$ *is a field if:*

1. $(\mathbb{K}, *, \top)$ *is a unitary ring.*
2. $(\mathbb{K} - \{e\}, \top)$ *is a group, wheree is the neutral element of* $*$.

Example 4.13.
1. $(\mathbb{Z}, +, \times)$ *is not a field.*
2. $(\mathbb{R}, +, \times)$ *is a commutative field.*