StandardLists=true

Course of Algebra 1

Said AISSAOUI

December 8, 2024

Contents

Chapter 1

Introduction to Mathematical logic

Chapter 2

Sets and functions

Chapter 3

Binary relations

Chapter 4

Algebraic structures

4.1 Binary operation

Definition 4.1.1 *Let S be a non-empty set. A function*

$$\begin{aligned} \star : S \times S &\longrightarrow S, \\ (a,b) &\longmapsto a \star b. \end{aligned}$$

is called a binary operation on S. So $\star$ takes 2 inputs a, b from S and produces a single output $a \star b \in S$. In this situation we may say that S is closed under $\star$.

In other word , we can say also that a binary operation on a set S is a correspondence that assigns to each ordered pair of elements of the set S a uniquely determined element of the set S .

Example 4.1.1 ✔ *Addition, " + ", is a binary operation on each of the following: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. But $+$ is NOT a binary operation on the set $S = \{0,1\}$: we have $1 \in S$ but $1+1=2 \notin S$.*

✔ *Multiplication, ".", is a binary operation on each of the following sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\{-1,1\}$, and $\{0,1\}$.*

✔ *Let the function $\star$ defined by :*

$$\begin{aligned} [1, +\infty[\times [1, +\infty[&\longrightarrow [1, +\infty[\\ (x, y) &\longmapsto x \star y = (x-1)y+1 \end{aligned}$$

is it a binary operation on $[1,\ +\infty[$ *?*
Let $x \in [1,\ +\infty[$,

$$x \in [1,\ +\infty[\iff x \geqslant 1 \iff x-1 \geqslant 0.$$
$$y \in [1,\ +\infty[\iff y \geqslant 1 \iff y-1 \geqslant 0.$$
$$\textit{we have} \quad (x-1)y \geqslant 0 \iff (x-1)y+1 \geqslant 1 \iff x\star y \in [1,\ +\infty[.$$

Exercise 4.1.1 *which of the following are binary operations?*

1. $a \star b = a+b, \forall a, b \in \mathbb{R}^*$.
2. $a\#b = a+b-3, \forall a, b \in \mathbb{N}$.
3. $a \circ b = a+2b-5, \forall a, b \in \mathbb{R}^*$
4. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \forall \frac{a}{b}, \frac{c}{d} \in \mathbb{Q} \setminus \{0\}$.

Definition 4.1.2 (Closed Under an Operation) *A set S is said to be closed under a binary operation* $\star$ *if for every s and t in S,* $s \star t$ *is in S.*

Remark 4.1.1 *Notice that the term "closed", as defined here, only makes sense in the context of a set with an operation. Notice also that it is the set that is closed, not the operation. The operation is important as well; as we have seen, a given set can be closed under one operation but not another.*

Example 4.1.2 ✔ *The set* $S = \{1,\ -1\}$ *closed under usual multiplication on* $\mathbb{R}^*$

✔ *The set* $S = \{1,\ -1\}$ *is not closed under usual addition on* $\mathbb{R}$ *(we have* $1+(-1) = 0 \notin S$*).*

✔ *The subset* $2\mathbb{Z}$ *is closed under the usual addition "+".*

✔ *The subset* $\mathbb{R}_-$ *is closed under* $+$ *but not closed under the multiplication.*

✔ *We define a binary operation* $\star$ *on the set* $\mathbb{R}$ *by*

$$x \star y = xy - 3x - 3y + 12.$$

Let $S =]3,\ +\infty[$. *Show that* S *is a closed subset under the binary operation* $\star$.

$$\begin{aligned} x\star y \in S &\iff x\star y > 3 \\ &\iff x\star y - 3 > 0 \\ &\iff xy - 3x - 3y + 9 = x(y-3) - 3(y-3) = (y-3)(x-3) > 0. \end{aligned}$$

(*because* $x-3>0$ *and* $y-3>0$).

4.1.1 Properties of binary operation

A binary operation is an operation that combines two elements to produce another element. It is a fundamental concept in mathematics and computer science. Here are some properties of binary operations: Let S be a set with a binary operation $\star$ defined on it.

1. We say that $\star$ is commutative if and only if : $\forall a, b \in S : a \star b = b \star a$.

2. We say that $\star$ is associative if and only if $\forall a, b, c \in S : (a \star b) \star c = a \star (b \star c)$.

3. Let $e \in S$, be an element in the set S, we say that e is an identity element for $\star$ if $\forall a \in S : a \star e = e \star a = a$.

4. Let $x \in S$, we say that x admits an inverse element under the binary operation $\star$, if there exists $x^{'} \in S$, such that $x \star x^{'} = x^{'} \star x = e$.

$x^{'}$ is called inverse element of x under the binary operation $\star$.

Example 4.1.3 *Let $\mathbb{R}$ be a set of real numbers and $\star$ be a binary operation on $\mathbb{R}$. defined as $a \star b = a + b - ab$, then $\star$ is commutative and associative.*

Solution 4.1.1 *1. $a \star b = a + b - ab = b + a - ba = b \star a$. Which implies that $\star$ is commutative.*

2. Let $a, b, c \in \mathbb{R}$, then

$$\begin{aligned}(a \star b) \star c &= (a + b - ab) \star c = a + b - ab + c\hat{a}a + b - abc \\ &= a + b + c - ab - ac - bc + abc \cdots (1) \\ a \star (b \star c) &= a \star (b + c - bc) = a + b + c - bc - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \cdots .(2)\end{aligned}$$

we have then $(1) = (2)$ therefore $\star$ is associative.

4.2 Groups

The first Mathematician who used the word "group" is **Evarist Galois** (1811 – 1832), We find the structure of groups in different domains, in physics with the symmetry groups of an object,
in mathematics in the resolution of equations algebraic, arithmetic...etc.

Definition 4.2.1 (The Group) *A group $(G,\star)$ is a non-empty set G and a binary operation $\star$, such that the following axioms are satisfied:*

❶ *The binary operation $\star$ is associative if:*

$$\boxed{\forall a, b, c \in G : (a \star b) \star c = a \star (b \star c)}.$$

❷ *Existence of the Identity element e*
There is an element e in G such that

$$\boxed{\exists e \in G, \forall x \in G : a \star e = e \star a = a.}$$

This element e is an identity element for $\star$ on G .

❸ *Existence of Inverse elements*
For each a in G, there is an element b in G such that

$$\boxed{\forall a \in G, \exists b \in G : a \star b = b \star a = e}.$$

The element b is an inverse of a and denoted by a^{-1} or $a^{'}$ or $-a$.

We will denote such a group $(G,\star)$ (since it is given by both the set G and the operation $\star$).

Definition 4.2.2 *(Commutative group) A group $(G,\star)$ is called a commutative group(or abelian group) if and only if $a \star b = b \star a, \forall a, b \in G$.*

Example 4.2.1 ✔ $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, *are all abelian*[1] *group.*

✔ $(\mathbb{Q}^*,.)$, $(\mathbb{R}^*,.)$, $(\mathbb{C}^*,.)$, *are commutative group.*

✔ $(\mathbb{Z}^*,.)$ *is not a group, the inverse of element* 3 *does not exist. The only inverse element under the multiplication in* $\mathbb{Z}^*$ *are* 1 *and* -1

✔ $(\mathbb{R},.)$ *is not a group* : 0 *doesn't have an inverse under the multiplication on* $\mathbb{R}$.

[1] honors Niels Abel (1802-1829)

✔ $(\mathbb{N},+)$ *is not a group : for all element* $a \in \mathbb{N}-\{0\}$, $a+b>0$, *there is not an inverse for a natural number not nul under addition.*

✔ *Let* X *be an arbitrary set. The set of functions from* X *to* X

$$S(X) = \Big\{f\ : X \longrightarrow X : f \textit{ is a function}\Big\}$$

together with a composition is a group. In particular, for $X = \Big\{1,\ 2,\ \cdots, n\Big\}$, *the set of permutations of* n *elements* $S_n = S(X)$ *is called symmetric group .*

Definition 4.2.3 (Order of a group) *The order of a group* $(G,\star)$ *is the number of elements in* G. *It is a natural number or* ∞. *We denote it by* $|G|$ *or* $\circ(G)$.

Definition 4.2.4 (Finite group) *If* $|G|$ *or* $\circ(G)$ *is finite, the group* G *is said to be finite group. Otherwise it is said to be infinite group.*

Example 4.2.2 *1.* $(\Big\{-1,\ 1\Big\},\ .)$ *is a finite abelian group.*

2. $(\mathbb{Z},\ +)$ *is an infinite abelian group.*

Groups of small order may be given or described in the table (called cayley[2] table)

$\star$	e
e	e

$\star$	e	a
e	e	a
a	a	e

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

where an element in G occurs in every row and column exactly once, since the equation $ax = b$ (resp. $xa = b$) has in G a unique solution, namely $x = a^{-1}b$,(resp. $x = ba^{-1}$).

Definition 4.2.5 (Quasi group) *A order pair* $(S,\star)$ *of non empty set* S *together with binary operation* $\star$ *is said to be a Quasi group if* $\star$ *satisfies only the closed property, which means*

$$\forall a, b \in S, a\star b \in S.$$

[2]Arthur Cayley (A821-1895) was an early group theorist.

Definition 4.2.6 (semi group) *A order pair $(S,\star)$ of non empty set S together with binary operation $\star$ is said to be a semi group if $\star$ satisfies the closed property and the associativity property which means*

$$\forall a,b\in S, a\star b\in S,$$
$$\forall a,b,c\in S, (a\star b)\star c = a\star(b\star c).$$

Definition 4.2.7 (Monoid) *A order pair $(S,\star)$ of non empty set S together with binary operation $\star$ is said to be a monoid if $\star$ satisfies the closed property, the associativity property and existance of Identity. In other words*

$$\forall a,b\in S, a\star b\in S,$$
$$\forall a,b,c\in S, (a\star b)\star c = a\star(b\star c),$$
$$\exists e\in S, \forall a\in S: a\star e = e\star a = a.$$

Example 4.2.3

- ✔ $(\mathbb{N},+)$ *is a monoid but not a group.*
- ✔ $(\mathbb{Z},.)$ *is a monoid but not a group.*

Exercise 4.2.1 *we define the operation $\star$ on $]-1,\ 1[$ by*

$$\forall x,y\in]-1,\ 1[,\ x\ \star\ y\ = \frac{x+y}{1+xy}.$$

Show that $(]-1,\ 1[,\ \star)$ is a commutative group.

Solution 4.2.1 ❶ ***Closure property*** *First, we must verify if the operation $\star$ is closed on the set $]-1,\ 1[$, that means we show if: $\forall x,y\in]-1,\ 1[,\quad x\star y\in]-1,\ 1[$.*

✔ *Show that $-1<x\star y$, we have*

$$-1<x\star y \iff -1<\frac{x+y}{1+xy} \iff -1-xy<x+y \iff 0<1+x+xy+y$$
$$\iff 0<(1+x)+y(1+x) \iff 0<(x+1)(y+1).$$

comme $x,y\in]-1,\ 1[$ so $0<(x+1)(y+1)$ thus $-1<x\star y$.

✔ *Show that* $x \star y < 1$,*we have*

$$x \star y < 1 \iff \frac{x+y}{1+xy} < 1 \iff x+y < 1+xy \iff x-xy+y-1<0$$
$$\iff x(1-y)-(1-y)<0 \iff (1-y)(x-1)<0.$$

if $x, y \in]-1,\ 1[$ *then* $(1-y)(x-1)<0$ *so* $x \star y < 1$.

therefore we $\forall x, y \in]-1,\ 1[, x \star y \in]-1,\ 1[$, *which means that* $\star$ *is a binary operation (closed) on* $]-1,\ 1[$.

❷ ***Associativity property*** *Show that* $\star$ *is associative :* $\forall x, y, z \in]-1, 1[, (x \star y) \star z = x \star (y \star z)$

$$(x \star y) \star z = (\frac{x+y}{1+xy}) \star z = \frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}z} = \frac{x+y+z+xyz}{1+xy+yz}.$$

and the same calcul, we obtain the same result for $x \star (y \star z)$.

❸ ***Existence of identity element*** $\exists e \in]-1,\ 1[, \forall x \in]-1,\ 1[,\ x \star e = e \star x = x.$

$$e \star x = x \iff \frac{e+x}{1+ex} = x$$
$$\iff e+x = x(1+ex) \iff e = ex^2$$
$$\iff e - ex^2 = 0 \iff e(1-x^2)=0$$
$$\iff e = 0 \quad (as\ x\ \in]-1,\ 1[)$$

and we have $x \star 0 = x$ *so the identity element of* $\star$ *is* $e = 0$.

❹ ***Existence of inverse elements,*** $\forall x \in]-1,\ 1[,\ \exists x' \in]-1,\ 1[$, *such that* $x \star x' = x' \star x = 0$.

$$x \star x' = 0 \iff \frac{x+x'}{1+xx'} = 0$$
$$\iff x + x' = 0$$
$$\iff x' = -x$$

,

satisfies that $(-x) \star x = 0$, *we notice that if* $x \in]-1,\, 1[$ *then* $-x \in]-1,\, 1[$, *so every element of* $]-1,\, 1[$ *admits an inverse under* $\star$.

conclusion

$$(]-1,\, 1[,\, \star) \text{ is a group.}$$

Exercise 4.2.2 *Show that the set* $G = \left\{1, -1, i, -i\right\}$ *is a group under multiplication.*

Remark 4.2.1 *if the binary operation is commutative, to find an identity element and an inverse element, it is enough to solve one equation, for example for the identity element, we solve this equation* $e \star x = x$ *(left equation) or the other equation (right equation)* $x \star e = x$.

Exercise 4.2.3 . *We define on the set* $G = \mathbb{R} - \{2\}$ *a binary relation* $\star$ *by :*

$$\forall x,\ y \in G,\ x \star y = xy - 2x - 2y + 6.$$

Show that $(G,\, \star)$ *is a group*

Solution 4.2.2 . ⚠ ✍ *be careful, the firs thing to check is to show that the set is closed under the binary operation. (* $\forall x,\ y \in G, x \star y \in G$*).*

The following properties are very important :

Proposition 1 . *Let* $(G,\, \star)$ *be a group , so we have*

❶ *a group* $(G, \star)$ *is always a non empty set.*

❷ *The identity element is unique.*

❸ *The inverse of any element* $a \in G$ *is unique (i.e a has only one inverse, if a has 2 inverses then they are equal).*

❹ *For every* $a \in G$, $(a^{-1})^{-1} = a$.

❺ *For every* $a,\ b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

❻ *For every* $a_1, a_2, \cdots a_n \in G$, $(a_1 a_2 a_3 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$.

❼ *For every element* $a \in G$: $a \star x = a \star y \Longrightarrow x = y$ *(left cancellation).*

❽ *For every element* $a \in G$: $x \star a = y \star a \Longrightarrow x = y$ *(right cancellation).*

Proof 4.2.0.1 ✘ *To prove the uniqueness identity element e, We suppose there exist an another identity element $e^{'}$*

$$\begin{aligned} e \star e^{'} &= e \quad (e^{'} \text{ identity element}) \\ &= e^{'} \quad (e \text{ identity element}). \end{aligned}$$

so $e = e^{'}$.

✘ *To prove the uniqueness inverse element $x^{'}$, for the element x.*
We suppose that there exist an another inverse element $x^{"}$

$$\begin{aligned} a \star a^{'} = e &\Longleftrightarrow a^{"} \star (a \star a^{'}) = a^{"} \star e \\ &\Longleftrightarrow (a^{"} \star a) \star a^{'} \quad (\star \text{ associative}) \\ &\Longleftrightarrow e \star a^{'} = a^{"} \quad (e \text{ identity element}). \end{aligned}$$

so $a^{"} = a^{'}$.

✘ *Find the inverse element of $a \star b$.*

$$\begin{aligned} (a \star b) \star (a \star b)^{-1} = e &\Longleftrightarrow a^{-1} \star (a \star b) \star (a \star b)^{-1} = a^{-1} \star e \\ &\Longleftrightarrow (a^{-1} \star a) \star b \star (a \star b)^{-1} = a^{-1} \\ &\Longleftrightarrow e \star b \star (a^{-1} \star a) \star b \star (a \star b)^{-1} = a^{-1} \\ &\Longleftrightarrow b \star (a \star b)^{-1} = a^{-1} \\ &\Longleftrightarrow b^{-1} \star (b \star (a \star b)^{-1}) = b^{-1} \star a^{-1} \\ &\Longleftrightarrow (b^{-1} \star b) \star (a \star b)^{-1} = b^{-1} \star a^{-1} \\ &\Longleftrightarrow e \star (a \star b)^{-1} = b^{-1} \star a^{-1} \\ &\Longleftrightarrow (a \star b)^{-1} = b^{-1} \star a^{-1}. \end{aligned}$$

so

$$(a \star b)^{-1} = b^{-1} \star a^{-1}$$

✘ *Prove the left cancellation*

$$\forall a \in G,\ a.x = a.y \Longrightarrow x = y. \tag{4.2.1}$$

By multiplying a^{-1} on both side of equation 4.2.1, we write

$$\begin{aligned} a^{-1}.(a.x) = a^{-1}(a.y) &\Longrightarrow (a^{-1}.a).x = (a^{-1}.a).y \\ &\Longrightarrow e.x = e.y \\ &\Longrightarrow x = y \end{aligned}$$

✘ *The right cancellation law are defined as*

$$\forall a \in G,\ x.a = y.a \Longrightarrow x = y. \tag{4.2.2}$$

By multiplying a^{-1} on both side of equation 4.2.2, we write

$$\begin{aligned} (x.a).a^{-1} = (y.a).a^{-1} &\Longrightarrow x.(a.a^{-1}) = y.(a.a^{-1}) \\ &\Longrightarrow x.e = y.e \\ &\Longrightarrow x = y \end{aligned}$$

4.2.1 Subgroups

Definition 4.2.8 *Let $(G, \star)$ be a group and a subset $H \subset G$ is called a sub-group of $(G, \star)$, if it remains a group with respect to the same binary operation. We write $H \leqslant G$ .That means*

1. *The identity element belongs to H.*
2. *The set H is closed under the binary operation of G ($\star$), ie $\forall a, b \in H, a \star b \in H$.*
3. *Every element of H has its inverse element in H.*

Remark 4.2.2

A subgroup H is a proper subgroup if $H \neq G$, this is written $H < G$.

The trivial subgroup is the singleton $\{e\}$, all other subgroups are non trivial.

- $\{e\}$ and G are subgroups of G, for any group G.
- $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.
- $(\mathbb{Q}^*, .)$ is a subgroup of $(\mathbb{R}^*, .)$.

- $(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$.

Proposition 2 *Let H be a subset of the group $(G,.)$ H is a subgroup of $(G,.)$ if and only if*

❶ *H is not empty.*

❷ $\forall a,b\in H, a.b^{-1}\in H,$ *(a^{-1} is the inverse element of a).*

Proof 4.2.1.1 1. *if H is a subgroup of G, then there exist the identity element $e\in H$ that means that H is not empty. if $b\in H$, then b^{-1} the inverse element of b is in H. so $a.b^{-1}\in H$ (because H is closed).*

2. *We have to prove that H is closed and contains the identity element and inverse elements. because of (1), H is not empty, $\exists a\in H$*

   - *If $a\in H$ then $a.a^{-1}=e\in H$ (from (2)), therefore the identity element belongs to H.*
   - *If $a,e\in H$ then $e.a^{-1}\in H$, then $a^{-1}\in H$.*
   - *If $b^{-1}\in H$ and $a\in H$ then $a.(b^{-1})^{-1}=ab\in H$, so $a.b\in H$ (closure of H).*

Example 4.2.4 ✔ *if $(G,\star)$ is a group with its identity element e, then G and $\{e\}$ are a subgroups of G.*

✔ *$(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$ which is itself is a subgroup of $(\mathbb{R},+)$. we have*

$$\begin{cases} \underline{0\in\mathbb{Z}} \\ \\ \underline{\forall x,y\in\mathbb{Z},\ x+(-y)\in\mathbb{Z}} \end{cases} \tag{4.2.3}$$

✔ *$(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$. We have*

$$\begin{cases} \underline{0\in\mathbb{Z}} \\ \\ \underline{\forall x,y\in 2\mathbb{Z},\ x+(-y)\in 2\mathbb{Z}} \end{cases} \tag{4.2.4}$$

Indeed,

$$\begin{aligned} x,y\in 2\mathbb{Z} &\Longrightarrow \exists k,k^{'}\in\mathbb{Z},\ \text{such that}\ x=2k\ \text{and}\ y=2k^{'} \\ &\Longrightarrow x+(-y)=2k+(-2k^{'})=2(k-k^{'})\in 2\mathbb{Z}. \end{aligned}$$

✔ $(2\mathbb{Z}+1,+)$ *is not a subgroup of* $(\mathbb{Z},+)$. *The set* $2\mathbb{Z}+1$ *is not closed under* $+$. *For example* $3,\ 5 \in 2\mathbb{Z}+1$, *but* $3+5=8 \notin 2\mathbb{Z}+1$

Exercise 4.2.4 *Let* H_1, H_2 *be two subgroups of* $(G,\star)$.

❶ *Show that* $H_1 \cap H_2$ *is subgroup of* $(G,\star)$.

❷ *Show that, in general,* $H_1 \cup H_2$ *is not a subgroup of* $(G,\star)$.

Solution 4.2.3 ✘ *We have* $H_1 \cap H_2 \neq \emptyset$ *because* $e \in H_1 \cap H_2$. *Indeed ,* $e \in H_1$ *and* $e \in H_2$. *(* H_1, H_2 *be two subgroup of* G*). Let* $x, y \in H_1 \cap H_2$

$$\begin{aligned} x,\ y \in H_1 \cap H_2 &\Longrightarrow x,\ y \in H_1 \text{ et } x,\ y \in H_2. \\ &\Longrightarrow x \star y^{-1} \in H_1 \text{ et } x \star y^{-1} \in H_2\,, \quad (H_1,\ H_2 \text{ be subgroup of } G). \\ &\Longrightarrow x \star y^{-1} \in H_1 \cap H_2. \end{aligned}$$

✘ *For the union, we have* $2\mathbb{Z}$ *and* $3\mathbb{Z}$ *two subgroups of* $(\mathbb{Z},\ +)$, *but* $(2\mathbb{Z} \cup 3\mathbb{Z})$ *is not a subgroup of* $(\mathbb{Z},\ +)$ *, because it is not closed under* $+$. *If we take* $x=2 \in 2\mathbb{Z}$ *and* $y=3 \in 3\mathbb{Z}$ *then* $2+3=5 \notin (2\mathbb{Z} \cup 3\mathbb{Z})$

4.2.2 Group Homomorphisms

Definition 4.2.9 *Let* $(G,\star)$, $(G^{'},\Delta)$ *be two groups. We said group homomorphism from* G *to* $G^{'}$ *every function* $f:(G,\star) \longrightarrow (G^{'},\ \Delta)$ *such that :*

$$\boxed{\forall x,\ y \in G:\ f(x \star y) = f(x)\,\Delta f(y)}.$$

In other words, every function from G to $G^{'}$ *that preserves the group's structure.*

❶ *Injective group homomorphisms are called monomorphisms*

❷ *Surjective group homorphisms are called epimorphisms.*

❸ *An isomorphism group* $\phi G_1 \longrightarrow G_2$ *is bijective homomorphism. The inverse function* $\phi^{-1}: G_2 \longrightarrow G_1$ *is then also a isomorphism group. we write* $G_1 \simeq G_2$

Example 4.2.5 ✔ *The function* $f:(\mathbb{R},+) \longrightarrow (\mathbb{R}^{*+},.)$ *such that* $f(x)=e^x$, *is a group homomorphism. Indeed*

$$f(x+y) = e^{x+y} = e^x.e^y = f(x).f(y).$$

✔ *The function* $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ *such that* $f(x) = 3x$*, is a group homomorphism.*

✔ *The function* $f : (\mathbb{R}_+^*, .) \longrightarrow (\mathbb{R}, +)$ *such that* $f(x) = \ln(x)$*, is a group homomorphism. Indeed ,*

$$\forall x,\ y \in \mathbb{R}_+^*,\ f(xy) = \ln(xy) = \ln(x) + \ln(y) = f(x) + f(y).$$

$$f \text{ is bijective } \Longleftrightarrow \forall y \in \mathbb{R},\ \exists! x = e^y \in \mathbb{R}_+^*, \text{ such that } y = \ln(x).$$

✔ *The function* $f : (\mathbb{C}^*, .) \longrightarrow (\mathbb{R}^*, .)$ *such that* $f(z) = |z|$*, is a group homomorphism. Indeed, we have :*

$$\forall z,\ z^{'} \in \mathbb{C}^*,\ f(z.z^{'}) = |z.z^{'}| = |z|.|z^{'}| = f(z).f(z^{'})$$

Proposition 3 *Let* f *be a group homomorphism from* $(G_1, \star)$ *to* (G_2, Δ) *(with identity elements* e_1, e_2 *of* G_1, G_2 *respectively), then we have:*

❶ $f(e_1) = e_2$.

❷ $\forall x \in G_1,\ f(x^{-1}) = [f(x)]^{-1}$.

❸ *Let* H *be a subgroup of* G_1*, then the the direct image of* H*,* $f(H)$*, is a subgroup of* G_2.

❹ *Let* $H^{'}$ *be a subgroup of* G_2*, then the Inverse image of* $H^{'}$*,* $f^{-1}(H^{'})$*, is a subgroup of* G_1.

Proof 4.2.2.1 ■ *We have :*

$$\begin{aligned} f(e_1 \star e_1) = f(e_1)\Delta f(e_1) &\Longrightarrow f(e_1) = f(e_1)\Delta f(e_1) \\ &\Longrightarrow [f(e_1)]^{-1}\Delta f(e_1) = [f(e_1)]^{-1}\Delta\big(f(e_1)\Delta f(e_1)\big) \\ &\Longrightarrow e_2 = \big([f(e_1)]^{-1}\Delta f(e_1)\big)\Delta f(e_1) \\ &\Longrightarrow e_2 = f(e_1). \end{aligned}$$

■

$$\begin{aligned}\forall x\in G_1, f(x\star x^{-1}) = f(x)\Delta f(x^{-1}) &\Longrightarrow f(e_1) = f(x)\Delta f(x^{-1})\\ &\Longrightarrow e_2 = f(x)\Delta f(x^{-1})\\ &\Longrightarrow [f(x)]^{-1}\Delta e_2 = [f(x)]^{-1}\Delta\big(f(x)\Delta f(x^{-1})\big)\\ &\Longrightarrow [f(x)]^{-1} = \big([f(x)]^{-1}\Delta f(x)\big)\Delta f(x^{-1})\\ &\Longrightarrow [f(x)]^{-1} = e_2\Delta f(x^{-1})\\ &\Longrightarrow [f(x)]^{-1} = f(x^{-1}).\end{aligned}$$

■ *Let H be a subgroup of G_1, Show that $f(H)$ is a subgroup of G_2. First, $f(H)\neq\emptyset$, because $e_2 = f(e_1)\in f(H)$.*
Secondly, Let $x,\ y\in f(H), show that\ x\Delta y^{-1}\in f(H)$?.
If $x,\ y\in f(H)$, then $\exists t,\ s\in H$ such that $x = f(t)$ and $y = f(s)$. We have :

$$\begin{aligned}x\Delta y^{-1} &= f(t)\Delta[f(s)]^{-1} = f(t)\Delta f(s^{-1}\\ &= f(t\star s^{-1})\in f(H).(\,because\ t\star s^{-1}\in H.\ and\ H\ subgroup\ G_1)\end{aligned}$$

■ *Let $H^{'}$ be a subgroup of G_2, Show $f^{-1}(H^{'})$ is a subgroup of G_1. First, $f^{-1}(H^{'})\neq\emptyset$, because $e_2 = f(e_1)\in H^{'}$, so $e_1\in f^{-1}(H^{'})$*
secondly , let $x,\ y\in f^{-1}(H^{'})$, show that $x\Delta y^{-1}\in f^{-1}(H^{'})$?. in other words $f(x\Delta y^{-1})\in H^{'}$?

$we have: f(x\Delta y^{-1}) = f(x)\Delta f(y^{-1}) = f(x)\Delta[f(y)]^{-1}\in H^{'}.(\,because\ H^{'}\ subgroup\ G_2)$

Exercise 4.2.5 *Which of the following are homomorphism /isomorphism of a binary structures? explain*

❶ $\phi : (\mathbb{Z},+)\longrightarrow(\mathbb{Z},+),\ \phi(n) = -n.$

❷ $\phi : (\mathbb{Z},+)\longrightarrow(\mathbb{Z},+),\ \phi(n) = n+1$

❸ $\phi : (\mathbb{Q},+)\longrightarrow(\mathbb{Q},+),\ \phi(x) = \frac{3}{4}x.$

❹ $\phi : (\mathbb{Q},.)\longrightarrow(\mathbb{Q},.),\ \phi(x) = x^2.$

❺ $\phi : (\mathbb{R},+)\longrightarrow(\mathbb{R},.),\ \phi(x) = 2^x.$

❻ $\phi : (\mathbb{R},.)\longrightarrow(\mathbb{R},.),\ \phi(x) = x^5.$

4.2.3 Kernel and Image

Definition 4.2.10 *Let* $(G_1,\star)$ *and* $(G_2,\top)$ *be two groups and* $f : G_1 \longrightarrow G_2$ *be a group homomorphism from* $(G_1,\star)$ *to* $(G_2,\top)$.

❶ *We say kernel of* f, *denoted* $\ker f$, *is the set*

$$\boxed{\ker f == f^{-1}(\{e_2\}) = \left\{x \in G_1 \ / f(x) = e_2\right\}}.$$

❷ *We called image of* f, *noté* Imf, *is the set*

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

Theorem 4.2.1 *Let* f *be a group homomorphism from* $(G_1,\star)$ *to* (G_2,Δ).

❶ $\ker f$ *is a subgroup of* G_1.

❷ Imf *is a subgroup of* G_2.

❸ f *injective (or one to one)* $\Longleftrightarrow$ $\ker f = \{e_1\}$.

❹ f *surjective. (or onto)* $\Longleftrightarrow$ $Imf = G_2$.

Proof 4.2.3.1 ✔ *We have* $\ker f = f^{-1}(e_2)$, *inverse image of subgroup is a subgroup of* G_1. *see theorem 3.*

✔ *We have* $Imf = f(G_1)$, *the direct image of a subgroup is a subgroup of* G_2. *see theorem 3.*

✔ *Show by double implication*

✙ *We suppose* f *is injective and show that* $\ker f = \{e_1\}$.

$$x \in \ker f \Longleftrightarrow f(x) = e_2 \Longleftrightarrow f(x) = f(e_1) = e_2 \Longleftrightarrow x = e_1$$

so $\ker f = e_1$,

✙ *Inversely, we suppose that* $\ker f = \{e_1\}$ *and show that* f *is injective,*

$$\begin{aligned}\forall x, y \in G_1,\ f(x) = f(y) &\Longrightarrow f(x) - f(y) = e_2\\ &\Longrightarrow f(x-y) = e_2\ (f \text{ is a homomorphism group}).\\ &\Longrightarrow x - y \in \ker f\\ &\Longrightarrow x - y = e_1\ (\text{because } \ker f = \{e_1\}\\ &\Longrightarrow x = y\end{aligned}$$

so f *is injective.*

✔ *It follows by the definition of surjectivity.*

4.3 Rings

Definition 4.3.1 *Let* A *be a arbitrary non empty set. We define on* A *two binary operations* $\oplus$ *et* $\otimes$*. we said that* $(A, \oplus, \otimes)$ *is a ring if*

❶ $(A, \oplus)$ *is an abelian group.*

❷ $\otimes$ *is associative*

❸ $\otimes$ *is distributive*

$$\begin{aligned}\forall x, y, z, \in A,\ x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z.\ &(\text{left distributivity law}).\\ (y \oplus z) \otimes x = y \otimes x \oplus z \otimes x.\ &(\text{right distributivity}).\end{aligned}$$

Remark 4.3.1
1. *If we have* $\otimes$ *is commutative, we say that* $(A, \oplus, \otimes)$ *is a commutative ring.*

2. *If under the second binary operation* $\otimes$ *we have an identity element (called unity element), we say that* $(A, \oplus, \otimes)$ *is a ring with unity*

3. *A ring, then, is a triple comprising a set* A *and two binary operations* $\oplus$ *and* $\otimes$ *satisfying at least the axioms indicated above. Frequently one 'forgets' the* $\oplus$ *and* $\otimes$ *and talks of the ring* A*. This is bad since* A *is only the underlying set. Further,* A *could well be the underlying set for two different rings, if we are in this case we must precise the ring with its two operations in order to avoid confusion.*

4. *We do not demand that the second operation* $\otimes$ *in a ring be commutative. As consequence we must postulate distributivity as 2 laws, since neither follows from the other in general. For example : in the ring of real functions* $(F(\mathbb{R},\mathbb{R}),+,\circ)$ *we have* $(f+g)\circ h = f\circ h + g\circ h$ *but not in general* $h\circ(f+g) = h\circ f + h\circ g$.

Example 4.3.1 ✔ $(\mathbb{R},+,.),(\mathbb{Z},+,.),(\mathbb{Q},+,.)$ *et* $(\mathbb{C},+,.)$ *are all a commutative rings with unity.*

✔ $(2\mathbb{Z},+,.)$ *is a commutative ring (be careful without unit element).*

✔ *The set of real sequences equipped by the addition and produit between two sequences is a commutative ring.*

✔ *The set of functions from I (subset of* $\mathbb{R}$*) to* $\mathbb{R}$*, equipped by addition and multiplication is a commutative ring with unity.*

4.3.1 Some properties of rings

Proposition 4 *Let* $(A,+,\times)$ *be a ring. We denote the identity element by* 0_A.

❶ $\forall x \in A, x \times 0_A = 0_A = 0_A \times x.$

❷ $\forall x, y \in A.: (-x)\times y = -(x\times y) = x\times(-y).$

❸ $\forall x, y \in A: (-x)\times(-y) = x\times y.$

❹ *If the ring* $(A,+,\otimes)$ *has the unity element* 1_A *then* $\forall x \in A: -x = (-1_A)\times x.$

Proof 4.3.1.1 ✔

$$\begin{aligned} x.0_A &= x.0_A + 0_A \\ &= x.0_A + [x\times 0_A + (-(x\times 0_A))] \\ &= [x\times 0_A + x\times 0_A] + (-(x\times 0_A)) \\ &= x\times(0_A+0_A) + (-(x\times 0_A)) \\ &= x\times 0_A + (-(x\times 0_A) = 0_A. \end{aligned}$$

In the same manner, we show that $0_A \times x = 0_A$.

- ✔ *Let x, y be two elements of A*

$$\begin{aligned} x \times y + (-x) \times y &= (x + (-x)) \times y \\ &= 0_A \times y \\ &= 0_A. \end{aligned}$$

So $-x \times y = -(x \times y)$. In the same method , we show that $(x \times (-y) = -(x \times y)$

- ✔ *Let x, y be two elements of A*

$$\begin{aligned} (-x) \times (-y) &= -[(-x) \times y)] \\ &= -[-(x \times y)] \\ &= x \times y. \end{aligned}$$

Definition 4.3.2 *Let A be a ring such that $A \neq 0_A$; $a \neq 0_A$ is called* ***zero divisor*** *of A if there is some nonzero b in A with $ab = 0$*

$$\exists b \in A, \text{such that } b \neq 0_A \text{ and } a \times b = 0_A.$$

Definition 4.3.3 (Integral domain) *We say that a ring, with identity element 0_A, is an integral domain if it is a nonzero ring $A \neq \{0_A\}$ and having nonzero divisors.*

$$\boxed{(A,+,\times) \text{ integral domain} \iff [A \neq \{0_A\} \text{ and } (\forall a, b \in A : a \times b = 0_A \Longrightarrow a = 0_A \text{ or } b = 0_A).]}$$

Notice that 0_A is an identity element of A.

Example 4.3.2 ✔ *$(\mathbb{Z}, +, .)$ is an integral domain, it doesn't possess any zero divisors.*

- ✔ *The ring $(\mathbb{Z}/6\mathbb{Z}, \dot{+}, \dot{\times})$ is not an integral domain, because $\dot{3}\dot{\times}\dot{2} = \dot{6} = \dot{0}$, since $\dot{3} \neq \dot{0}$ and $\dot{2} \neq \dot{0}$. Recall the construction of the ring $\mathbb{Z}/6\mathbb{Z}$. We define on $\mathbb{Z}$ a binary relation by*

$$\forall x, y \in \mathbb{Z}, \; x \mathfrak{R} y \iff \exists k \in \mathbb{Z} \text{ such that } x - y = 6k.$$

We verify that this relation is an equivalence relation ($\mathfrak{R}$ is reflexive, $\mathfrak{R}$ symmetric and $\mathfrak{R}$ transitive). The set of equivalence classes of $\mathfrak{R}$, denoted $\mathbb{Z}/6\mathbb{Z}$, contains 6 elements (classes).

$$\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \; \dot{1}\, \dot{2}, \; \dot{3}, \; \dot{4}, \; \dot{5}\}$$

For example

$$\begin{aligned}\dot{0} &= \{x \in \mathbb{Z},\ \textit{such that } x\mathfrak{R}0\}\\ &= \{x \in \mathbb{Z},\ \textit{such that } x-0 = 6k, k \in \mathbb{Z}.\}\\ &= \{x \in \mathbb{Z},\ \textit{such that } x = 6k, k \in \mathbb{Z}.\}\\ &= \{6k,\ k \in \mathbb{Z}.\}.\end{aligned}$$

in the same manner we show that

$$\dot{1} = \{6k+1,\ k \in \mathbb{Z}.\},\ \dot{2} = \{6k+2,\ k \in \mathbb{Z}.\},\ \dot{3} = \{6k+3,\ k \in \mathbb{Z}.\}$$
$$\dot{4} = \{6k+4,\ k \in \mathbb{Z}.\},\ \dot{5} = \{6k+5,\ k \in \mathbb{Z}.\}$$

We define on $\mathbb{Z}/6\mathbb{Z}$ *two binary operations* $\dot{+}$ *and* $\dot{\times}$ *by*

$$\boxed{\forall \dot{x},\ \dot{y} \in \mathbb{Z}/6\mathbb{Z},\ \dot{x} \dot{+} \dot{y} = \widehat{x+y}}. \quad \textit{and} \quad \boxed{\forall \dot{x},\ \dot{y} \in \mathbb{Z}/6\mathbb{Z},\ \dot{x} \dot{\times} \dot{y} = \widehat{x \times y}}.$$

We show that $(\mathbb{Z}/6\mathbb{Z},\ \dot{+},\ \dot{\times})$ *is a ring with unity and not an integral domain. See the table below*

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

4.3.2 Ring homomorphisms

Definition 4.3.4 *Let A, B be two rings and let $f : A \longrightarrow B$ be a function. We say that f is a ring homomorphism if*

❶ $\forall a,\ b \in A,\ f(a+b) = f(a) + f(b)$.

❷ $f(a.b) = f(a).f(b)$.

✔ *If f is injective, we say that f is a monomorphism.*

✔ *If f is surjective, we say that f is an epimorphism*

✔ *If f is bijective, we say that f is an isomorphism.*

Exercise 4.3.1 ❶ *Let A, B, C be three rings and let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be two ring homorphisms then $g \circ f$ is a ring homomorphism.*

❷ *If $f : A \longrightarrow B$ is a ring isomorphism then its inverse $f^{-1} : B \longrightarrow A$ is also a ring homomorphism.*

4.3.3 Subring

Definition 4.3.5 *Let B be a subset of A, we say that B is subring of $(A, +, \times)$ if $(B, +, \times)$ is a ring with the induced operations of A.*

Proposition 5 (Subring properties) *Let $(A, +, \times)$ be a ring and H a non empty subset of A, then H is a subring of A if and only if:*

❶ $\forall x, y \in H : x - y \in H$,

❷ $\forall x, y \in H : x \times y \in H$

Proof 4.3.3.1

Example 4.3.3 ✔ *If $f : A \longrightarrow B$ is a ring homomorphism then the direct image of A, $f(A)$, is a subring of B.*

✔ $(\mathbb{Z}[i], +, .)$ *is a subring of the ring* $(\mathbb{C}, +, .)$, *with*

$$\mathbb{Z}[i] = \{a + ib, \text{ such that } a, b \in \mathbb{Z}\}.$$

✔ $(2\mathbb{Z}, +, .)$ *is a subring of the ring* $(\mathbb{Z}, +, .)$.

Proposition 6 *Let $f : A \longrightarrow B$ be a ring homomorphism from the ring A to the ring B*

❶ *If A_1 is a subring of A then $f(A_1)$ is a subring of B.*

❷ *If B_1 is a subring of B then $f^{-1}(B_1)$ is a subring of A.*

In particular case: the two sets $\ker f = f^{-1}(\{0\})$ and $Im(f) = \{f(x); x \in A\}$ are the subrings of A and B respectively.

Proof 4.3.3.2 *$f(A_1)$ and $f^{-1}(B_1)$ are subgroups of additif group (for the first operation) B and A because f is a group homomorphism from $(A, +)$ to $(B, +)$. They are two subrings because they are closed under the second operation (multiplication):*

- ✔ *Let* $y, y_0 \in f(A_1)$ *then* $\exists x, x_0 \in A_1$ *such that* $f(x) = y, f(x_0) = y_0$ *so* $y y_0 = f(x x_0) \in f(A_1)$.

- ✔ *Let* $x, x_0 \in f^{-1}(B_1)$ *then* $f(x) \in B_1$ *and* $f(x_0) \in B_1$ *thus* $f(x x_0) = f(x) f(x_0) \in B_1$ *in other words* $x x_0 \in f^{-1}(B_1)$.

Proposition 7 (Binomial theorem) *Let* $(A, +, \times)$ *be a ring. Let* a*,* b *two element of* $\in A$ *which commute (i.e.* $a \times b = b \times a$*). Then*

$$(a+b)^n = \sum_{k=0}^{k=n} \binom{n}{k} a^k \times b^{n-k}.$$

Proof 4.3.3.3 *By induction on* $n \in \mathbb{N}$.

4.3.4 Ideals

Definition 4.3.6 *Let* I *be a non empty subset of* $I \subset A$ *is est an idéal* A *if :*

- ✔ $\forall x, y \in I,\ x. - y. \in I.$

- ✔ $\forall x \in I, \forall y \in A,\ x.y \in I$ *(and* $y.x \in I$*)*

Example 4.3.4

- ■ $6\mathbb{Z}$ *is an ideal of the ring* $(\mathbb{Z}, +, .)$.

- ■ *If* $f : A \longrightarrow B$ *is a ring homomorphism then* $\ker f$ *is an ideal of* A

- ■ *Let* $a \in A$ *(* A *is a ring), the set*

$$aA = \{xa,\ x \in A\}$$

is an ideal of A*, is the least (or smallest) ideal of* A *which contains* a*, it is called a principal ideal (ideal generated by one element).*

- ■ *every nonzero ring* A *has at least two ideals* A *and a trivial ideal* $\{0\}$.

Proposition 8 ❶ *The set* $f^{-1}(\{0_B\})$ *is an ideal* A. *We denote* $\ker f$ *and called kernel of* f. *We have in addition :*

$$\ker(f) = \{0_A\} \iff f \text{ injective.}$$

❷ *The* $f(A)$ *is a subring of* B. *We denote* $Im(f)$ *and called image of* f. *We have in addition:*

$$Im(f) = B \iff f \text{ surjective.}$$

4.3.5 Quotient ring

Let A be a commutative ring, I be an un ideal of A,

$$\forall a, b \in A, a\mathfrak{R}b \iff a - b \in I$$

We show that $\mathfrak{R}$ is an equivalence relation. We denote A/I the quotient set which is the set of all equivalence classes. We define on A/I the following binary operations:

$$\begin{aligned}(\dot{+}) : A/I \times A/I &\longrightarrow A/I \\ (\dot{a}, \dot{b}) &\longmapsto \dot{a} \dot{+} \dot{b} = \widehat{a+b}\end{aligned}$$

$$\begin{aligned}(\dot{\times}) : A/I. \times A/I &\longrightarrow A/I \\ (\dot{a}, \dot{b}) &\longmapsto \dot{a} \dot{\times} \dot{b} = \widehat{a \times b}\end{aligned}$$

We prove that $(A/I, \dot{+}, \dot{\times})$ is a ring, called quotient ring.

Example 4.3.5 *The ring* $(\mathbb{Z}/6\mathbb{Z}, +, .)$ *has unity element and it is commutative.*

4.4 Fields

Definition 4.4.1 *Let* K *be a set equipped with two binary operations* $\star$ *and* T. *We say that* $(K, \star, T)$ *is a field if :*

❶ $(K, \star, T)$ *is a ring with unity.*

❷ *Every element of* K, *except the identity element of* $\star$, *has an inverse under* T.

Remark 4.4.1 1. *If $(K,+,.)$ is a field then $(K^*,.)$ is a group.*

2. *Every field is a Integral Domain.*

3. *Every field K has at least two elements a au moins deux (identity and the unit element) 0_K and 1_K.*

4. *A field is an integral domain. Indeed :*
   if $x \times y = 0_K$, and $x \neq 0$, then x has an inverse , its inverse is denoted x^{-1}, and we compute then :

$$0_K = x^{-1} \times 0_K = x^{-1} \times x \times y = y.$$

   So K is a integral domain.

Example 4.4.1 ✔ $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$, $(\mathbb{C},+,.)$ *are all a commutative field.*

✔ $(\mathbb{Z},+,.)$ *is not a field, because the only elements which have the inverse for the multiplications in $\mathbb{Z}^*$ are. 1 and -1.*

✔ *The set*

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

equipped with the addition and the multiplication is a commutative field.

Summarize

Let S be a non empty set with two binary operations, addition " + " and multiplication ".". For any three elements $a, b, c \in S$, distinct or not,

(A1) $a+b=b+a$ *(commutativity of " + ")*

(A2) $(a+b)+c=a+(b+c)$ *(associativity of " + ")*

(A3) $\exists 0_S \in S$ *such that* $0_S+a=a+0_S=a$ *(Existence of identity element)*

(A4) *To each* $a \in S, \exists(-a) \in S$ *such that* $a+(-a)=(-a)+a=0$. *(Existence of inverse elements)*

(M1) $a.b=b.a$ *(commutativity of ".")*

(M 2) $(a.b).c=a.(b.c)$ *(associativity of ".")*

(M 3) $\exists 1_S \in S$ *such that* $1_S.a=a.1_S=a$ *(Existence of unit element)*

(M 4) *To each* $a \in S$ *such that* $a \neq 0_S$ *and* $\exists a^{-1} \in S$ *such that* $a.a^{-1}=a^{-1}.a=1_S$.

(D) $a.(b+c)=a.b+a.c$ *and* $(a+b).c=a.c+b.c$. *(Distributivity)*

(Z) *If* $a.b=0_S$ *then* $a=0_S$ *or* $b=0_S$ *(or both)* *(No zero divisor elements)*

	$A1$	$A2$	$A3$	$A4$	$M2$	D	$M1$	$M3$	$M4$	Z	the triple $(S,+,.)$ is called a
1	-	✔	✔	-	-	-	-	-	-	-	Monoid
2	-	✔	✔	✔	-	-	-	-	-	-	Group
3	✔	✔	✔	✔	-	-	-	-	-	-	Abelian group
4	✔	✔	✔	✔	✔	✔	-	-	-	-	Ring
5	✔	✔	✔	✔	✔	✔	✔	-	-	-	Commutative ring
6	✔	✔	✔	✔	✔	✔	-	✔	-	-	Ring with unity
7	✔	✔	✔	✔	✔	✔	-	-	-	✔	Ring with no zero divisors
8	✔	✔	✔	✔	✔	✔	✔	✔	-	-	Commutative ring with unity
9	✔	✔	✔	✔	✔	✔	✔	-	-	✔	Commutative ring with no zero divisors
10	✔	✔	✔	✔	✔	✔	-	✔	-	✔	Ring with unity and no zero divisors
11	✔	✔	✔	✔	✔	✔	✔	✔	-	✔	Integral domain
12	✔	✔	✔	✔	✔	✔	-	✔	✔	✔	Non commutaive field or division ring
13	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	Field

Notice that the axioms (**A1** to **A4**) concern the addition operation, end those (**M1** to **M4**) concern the multiplication operation, axiom **D** for distributibity, and axiome **Z** for (zero divisor element).

Theorem 4.4.1 *Let K be a commutative ring not nul.*

$$K \text{ be a field } \Longleftrightarrow \text{ the only ideals of } K \text{ are } \{0\} \text{ and } K.$$

4.4.1 Subfields

Definition 4.4.2 *Subfield Let K be a field. We say that the subset $K^{'}$ of K is a* *subfield of K if:*

❶ *$K^{'}$ is a subring of K.*

❸ *If $x \neq 0_K$ and $x \in K^{'}$ then $x^{-1} \in K^{'}$*

Example 4.4.2

Every intersection of subfields of K is a subfield of K.

4.4.2 Field homomorphisms

Solution 4.4.1 **Show that $(\mathbb{R}, *, T)$ is a commutative field.**

✔ **Show that T is commutative**: Let $x, y \in \mathbb{R}$, we have

$$\begin{aligned} xTy &= x+y+xy \\ &= y+x+yx \\ &= yTx. \end{aligned}$$

so

$$\forall x, y \in \mathbb{R}, \quad xTy = yTx,$$

so the commutativity of T.

✔ **Show that $(\mathbb{R}, *, T)$ is a ring with unity.**

- ✔ $(\mathbb{R}, *)$ **is an abelian group**
  - ✘ $*$ is a binary operation obvious
  - ✘ **Commutativity of $*$** : Let $x, y \in \mathbb{R}$, we have

$$\begin{aligned} x &= x+y+1 \\ &= y+x+1 \\ &= y*x. \end{aligned}$$

therefore
$$\forall x, y \in \mathbb{R}, \quad x * y = y * x,$$
so the commutativituy of $*$.

✘ **Associativity of** $*$: Let $x, y, z \in \mathbb{R}$, we have

$$\begin{array}{rcl} (x * y) * z & = & (x + y + 1) * z \\ & = & x + y + 1 + z + 1 \\ & = & x + y + z + 2. \end{array}$$

$$\begin{array}{rcl} x * (y * z) & = & x * (y + z + 1) \\ & = & x + y + z + 1 + 1 \\ & = & x + y + z + 2. \end{array}$$

thus
$$\forall x, y, z \in \mathbb{R}, \quad (x * y) * z = x * (y * z),$$
so the associativity of $*$.

✘ **Existence of the identity element for** $*$: $\exists ? e_1 \in \mathbb{R}, \forall x \in \mathbb{R}, x * e_1 = e_1 * x = x$. Let $x \in \mathbb{R}$, compte tenu de la commutativity $*$, we solve only one equa-

tion
$$x * e_1 = x.$$
We have
$$\begin{array}{rcl} x * e_1 = x & \Rightarrow & x + e_1 + 1 = x \\ & \Rightarrow & e_1 = -1 \end{array}$$
So $e_1 = -1$ is an identity element for $*$.

✘ **Every element of $\mathbb{R}$ admits an inverse under the operation** $*$: $\forall x \in \mathbb{R}, \exists ? x^{'} \in \mathbb{R} : x * x' = x' * x = e_1 = -1$. Let $x \in \mathbb{R}$, as we have the commutativity of $*$,

we solve only one equation
$$x * x' = -1.$$
We have
$$\begin{array}{rcl} x * x' = -1 & \Rightarrow & x + x' + 1 = -1 \\ & \Rightarrow & x' = -2 - x. \end{array}$$
So $\forall x \in \mathbb{R}, \exists x' = (-2 - x) \in \mathbb{R} : x'$ is an inverse of x.

From the previous , we deduce that , $(\mathbb{R}, *)$ is an **abelian group.**

✔ **Associativity of T** : Let $x, y, z \in \mathbb{R}$, on a

$$\begin{aligned} (xTy)Tz &= (x+y+xy)Tz \\ &= x+y+xy+z+(x+y+xy)Tz \\ &= x+y+z+xy+xz+yz+xyz. \end{aligned}$$

$$\begin{aligned} xT(yTz) &= xT(y+z+yz) \\ &= x+y+z+yz+x(y+z+yz) \\ &= x+y+z+xy+xz+yz+xyz. \end{aligned}$$

So

$$\forall x, y, z \in \mathbb{R}, \quad (xTy)Tz = xT(yTz),$$

thus we the associativity of T holds.

✔ **Distributivity law**: Let $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} xT(y) &= xT(y+z+1) \\ &= x+y+z+1+x(y+z+1) \\ &= 2x+y+z+xy+xz+1. \end{aligned}$$

$$\begin{aligned} (xTy)*(xTz) &= (x+y+xy)*(x+z+xz) \\ &= x+y+xy+x+z+xz+1 \\ &= 2x+y+z+xy+xz+1. \end{aligned}$$

So

$$\forall x, y, z \in \mathbb{R}, \quad xT(y*z) = (xTy)*(xTz).$$

Compte tenu de la commutativité de T, on a aussi

$$\forall x, y, z \in \mathbb{R}, \quad (y*z)Tx = (yTx)*(zTx).$$

✔ **Existence of the unit element**: $\exists ? e_2 \in \mathbb{R}, \forall x \in \mathbb{R}, xTe_2 = e_2Tx = x$. Let $x \in \mathbb{R}$, compte tenu de la commutativity of T, we solve the equation

$$xTe_2 = x.$$

. We have

$$\begin{aligned} xTe_2 = x &\Rightarrow x+e_2+xe_2 = x \\ &\Rightarrow e_2(1+x) = 0 \\ &\Rightarrow e_2 = 0 \ \forall x \neq -1. \end{aligned}$$

We have also

$$-1T0 = -1 + 0 + (-1)0 = -1.$$

So $e_2 = 0$ is a unit element.

Therefore we conclude that $(\mathbb{R}, *, T)$ **is a ring with unity.**

✔ **Show that** $\forall x \in \mathbb{R} - \{e_1\}$, x **admit an inverse under the second operation** T : let $x \in \mathbb{R} - \{-1\}$.

$$\begin{aligned} xTx' = 0 \quad &\Rightarrow \quad x + x' + xx' = 0 \\ &\Rightarrow \quad x' = \tfrac{-x}{1+x}. \end{aligned}$$

So $\forall x \in \mathbb{R} - \{-1\}$, $x' = \frac{-x}{1+x}$ is an inverse of x.

Thus $(\mathbb{R}, *, T)$ is a commutative field.

Prove that the functions

$$\begin{array}{llll} \varphi : & (\mathbb{R}, *, T) & \longrightarrow & (\mathbb{R}, +, .) \\ & x & \longmapsto & \varphi(x) = x + 1 \end{array} \quad \text{and} \quad \begin{array}{lll} \psi : (\mathbb{R}, +, .) & \longrightarrow & (\mathbb{R}, *, T) \\ x & \longmapsto & \psi(x) = x - 1. \end{array}$$

are the field isomorphisms.

φ is a field homomorphism: Indeed, Let $x, y \in \mathbb{R}$, we have

$$\begin{aligned} \varphi(x * y) &= (x * y) + 1 \\ &= x + y + 1 + 1 \\ &= (x + 1) + (y + 1) \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

So

$$\forall x, y \in \mathbb{R}, \quad \varphi(x * y) = \varphi(x) + \varphi(y).$$

Let $x, y \in \mathbb{R}$, we have also

$$\begin{aligned} \varphi(xTy) &= (xTy) + 1 \\ &= x + y + xy + 1 \\ &= x(y + 1) + (y + 1) \\ &= (x + 1)(y + 1) \\ &= \varphi(x).\varphi(y). \end{aligned}$$

thus

$$\forall x, y \in \mathbb{R}, \quad \varphi(xTy) = \varphi(x).\varphi(y).$$

$i)$ φ is injective function : Indeed, Let $x, y \in \mathbb{R}$ such that $\varphi(x) = \varphi(y)$. We have

$$\begin{array}{rcl} \varphi(x) = \varphi(y) & \Rightarrow & x+1 = y+1 \\ & \Rightarrow & x = y. \end{array}$$

$ii)$ φ is a surjective function:Indeed, let $y \in \mathbb{R}$, $\exists ? x \in \mathbb{R}$ such that $y = \varphi(x)$. We have

$$\begin{array}{rcl} y = \varphi(x) & \Rightarrow & y = x+1 \\ & \Rightarrow & x = y-1 \end{array}$$

So $\forall y \in \mathbb{R}$, $\exists\, x = (y-1) \in \mathbb{R}$ such that $y = \varphi(x)$.

Finally, we deduce from the previous that **φ is a field isomorphism**.

✙ ψ is a field homomorphism: Indeed , Let $x, y \in \mathbb{R}$, we have

$$\begin{array}{rcl} \psi(x+y) & = & (x+y)-1 \\ & = & (x-1)+(y-1)+1 \\ & = & \psi(x)+\psi(y)+1 \\ & = & \psi(x) * \psi(y). \end{array}$$

So

$$\forall x, y \in \mathbb{R}, \quad \psi(x+y) = \psi(x) * \psi(y).$$

Let $x, y \in \mathbb{R}$, we have also

$$\begin{array}{rcl} \psi(x.y) & = & (x.y)-1 \\ & = & x+y-2+xy-x-y+1 \\ & = & (x-1)+(y-1)+(x-1)(y-1) \\ & = & \psi(x)+\psi(y)+\psi(x)\psi(y) \\ & = & \psi(x) T \psi(y). \end{array}$$

So

$$\forall x, y \in \mathbb{R}, \quad \psi(x.y) = \psi(x) T \psi(y).$$

Exercises

Exercise 4.4.2 *We define on* $G = \mathbb{R}^* \times \mathbb{R}$ *a binary operation* $\star$ *as follow:*

$$\forall (x, y), (x', y') \in G,\ (x, y) \star (x', y') = (xx', xy' + y)$$

Show that $(G, \star)$ *is an abelian group.*

Exercise 4.4.3 *Let* $\star$ *a binary operation defined on* $\mathbb{R}$ *by :*

$$x \star y = xy + (x^2 - 1)(y^2 - 1).$$

❶ *Verify that* $\star$ *is commutative, not associative et admits a identity element.*

❷ *solve these following equations:* $2 \star y = 5, x \star x = 1.$

Exercise 4.4.4 *we provide* $\mathbb{Z}$ *a binary operation* $\star$ *defined by :*

$$\forall x, y \in \mathbb{Z} \ : \ x \star y = x + y + x^2 y.$$

❶ *Show that* $\star$ *is closed ; then study the commutativity , associativity, existence of identity element, the existence of inverse element.*

❷ *Same question for the binary operation* Δ *defined on* $\mathbb{R}_+^*$ *by :*

$$\forall x, y \in \mathbb{R}_+^* \ : x \Delta y = \sqrt{x^2 + y^2}.$$

Exercise 4.4.5 *Let* $(G, \star)$ *be a group with identity element* e*, such that for all element* $x \in G : x^3 = e$*.. Show that*

$$\forall x, y \in G : (x \star y)^2 = y^2 \star x^2 \ and\ x \star y^2 \star x = y \star x^2 \star y.$$

Notice that $x^2 = x \star x$ *and* $x^3 = x \star x \star x$

Exercise 4.4.6 *Let* $(G, \star)$ *be a group.Find the condition for which the function* $f : G \longrightarrow G$ *such that* $f(x) = x \star x$ *be a group homomorphism.*

Exercise 4.4.7 *Let* $(G, \star)$ *be a group and* $Z(G)$ *be the set of elements of G which commute with all elements of G.*

$$Z(G) = \left\{x \in G \ such\ that\ x \star y = y \star x, \forall y \in G\right\}$$

Show that $Z(G)$ *is a subgroup of* G*.*

Exercise 4.4.8 *Show that* $f,\ g : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$ *defined by* $f(x) = x^2, g(x) = x^3$ *are a group homomorphisms. Determine whose Image and Kernel respectively.*

Exercise 4.4.9 *Let* $(G, \star)$ *be a group and* $f : G \longrightarrow G$ *a function defined by* $f(x) = x^2$. *(Recall:* $x^2 = x \star x$*)*
Show that if $(G, \star)$ *is an abelian group then* f *is a group homomorphism. Show then the inverse.*

Exercise 4.4.10 *Show that if every element of the group G is its own inverse, then G is abelian.*

Exercise 4.4.11 *Let G be the group of all non-zero complex numbers* $a + bi$ *(a, b real, but not both zero) under multiplication, and let*

$$H = \left\{a + bi \in G | a^2 + b^2 = 1\right\}$$

Verify that H is a subgroup of G.

Exercise 4.4.12 *On the set* $S = \left\{0, 1\right\}$ *define* $\oplus$ *and* $\otimes$ *by*

$\oplus$	0	1
0	1	0
1	0	1

$\otimes$	0	1
0	0	1
1	1	1

Show that $(S, \oplus, \otimes)$ *is a ring. Is it a field?*

Exercise 4.4.13 *Find a ring R and elements a, b, c all distinct from identity element of R (denoted by* 0_R*), such that* $a.b = a.c$ *and yet* $b \neq c$.

Exercise 4.4.14 *Which elements of* $(\mathbb{Z}_m, \oplus, \otimes)$ *are zero divisors? Which have multiplicative inverses?*

Exercise 4.4.15 *On the set* $\mathbb{Z}$ *define two new multiplications* $\circ$ *and* $\square$ *by:*

$$\forall a,\ b \in \mathbb{Z},\ a \circ b = 0 \quad \text{and} \quad a \square b = 1.$$

Show that $(\mathbb{Z}, +, \circ)$ *is a ring with zero divisors. Is* $(\mathbb{Z}, +, \square)$ *a ring?*

Exercise 4.4.16 *With the usual definitions of addition and multiplication, do the following sets form rings, integral domains, fields?*

1. *The set* $\mathbb{Z}_+$.
2. *The complex fourth roots,* $1, i, -1, -i$, *of* 1.
3. *The set of all* $a + ib$ *where* $a, b \in \mathbb{Q}$.
4. *The set of all* $a + ib$ *where* $a, b \in \mathbb{Z}$.
5. *The set of all* $\frac{a}{b} \in \mathbb{Q}$ *where* b *is odd.*

Exercise 4.4.17