Chapter 1

Algebraic structures

1.1 Group

1.1.1 Definitions and examples

Definition 1.1 (*Binary operation*)

*A **binary operation** (or binary law) on a nonempty set S is a map from $S \times S$ to S. Such a binary operation is usually denoted*

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

Example : The set $\mathbb{N}$ of all natural numbers comes with the binary operation "addition of two numbers".

$$\begin{array}{rccc} + : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (a,b) & \longmapsto & a + b \end{array}$$

Example : Similarly, the addition provides a binary operation on the set $\mathbb{Z}$ of all integers.

$$\begin{array}{rccc} + : & \mathbb{Z} \times \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & (a,b) & \longmapsto & a + b \end{array}$$

Moreover this binary operation satisfies the following properties

i) $\forall (a,b,c) \in \mathbb{Z}^3,\ (a+b)+c = a+(b+c) = a+b+c$

ii) $0 \in \mathbb{Z}$ is such that $\forall a \in \mathbb{Z},\ a+0 = 0+a = a$

iii) $\forall a \in \mathbb{Z},\ \exists b \in \mathbb{Z} /\ a+b = b+a = 0$ (actually $b = -a$, the opposite number of a)

Example : Let $\mathcal{B}$ be the set of all bijective functions from the segment $[0,1]$ to itself.

$$\mathcal{B} = \{f : [0,1] \to [0,1] \,/\, f \text{ bijective}\}$$

Notice this set is nonempty (for instance $\mathrm{Id}_{[0,1]} = (x \mapsto x) \in \mathcal{B}$). The composition of functions provides a binary operation on $\mathcal{B}$.

$$\begin{array}{rccc} \circ : & \mathcal{B} \times \mathcal{B} & \longrightarrow & \mathcal{B} \\ & (f,g) & \longmapsto & f \circ g \end{array}$$

Indeed $f \circ g$ is well in $\mathcal{B}$ since $f \circ g : [0,1] \to [0,1]$ is bijective as composition of bijective functions. Moreover this binary operation satisfies the following properties

i) $\forall (f,g,h) \in \mathcal{B}^3,\ (f \circ g) \circ h = f \circ (g \circ h) = f \circ g \circ h$

ii) $\mathrm{Id}_{[0,1]} \in \mathcal{B}$ is such that $\forall f \in \mathcal{B},\ f \circ \mathrm{Id}_{[0,1]} = \mathrm{Id}_{[0,1]} \circ f = f$

iii) $\forall f \in \mathcal{B},\ \exists g \in \mathcal{B} /\ f \circ g = g \circ f = \mathrm{Id}_{[0,1]}$ (actually $g = f^{-1}$, the bijective inverse function of f)

Definition 1.2 (*Group*)

Let $(G, \star)$ be a nonempty set with a binary operation. $(G, \star)$ is said to be a ***group*** *if it satisfies each of the following group axioms*

i) Associativity: $\forall (a,b,c) \in G^3,\ (a \star b) \star c = a \star (b \star c) = a \star b \star c$

ii) Identity element: $\exists e \in G /\ \forall a \in G,\ a \star e = e \star a = a$ *(e is called identity element)*

iii) Inverse element: $\forall a \in G,\ \exists a' \in G /\ a \star a' = a' \star a = e$ *(a' is called inverse element of a)*

Examples : $(\mathbb{Z}, +)$ and $(\mathcal{B}, \circ)$ are groups whose identity elements are respectively $0 \in \mathbb{Z}$ and $\mathrm{Id}_{[0,1]} \in \mathcal{B}$.

Definition 1.3 (*Abelian group*)

A binary operation $\star$ on a nonempty set S is said ***commutative*** *if*

$$\forall (a,b) \in S^2,\ a \star b = b \star a$$

An ***abelian group*** *(or commutative group) is a group $(G, \star)$ for which its binary operation $\star$ is commutative.*

Example : $(\mathbb{Z}, +)$ is an abelian group since the addition of numbers is commutative.

Example : $(\mathcal{B}, \circ)$ is not abelian since $\exists (f,g) \in \mathcal{B}^2 /\ f \circ g \neq g \circ f$. For instance, consider $f = (x \mapsto x^2) \in \mathcal{B}$ (its associated inverse element is $f^{-1} = (y \mapsto \sqrt{y}) \in \mathcal{B}$) and $g = (x \mapsto 1 - x) \in \mathcal{B}$ (its associated inverse element is $g^{-1} = (x \mapsto 1 - x) = g \in \mathcal{B}$). Then

$$\forall x \in [0,1],\ \begin{cases} f \circ g(x) = f(1-x) = (1-x)^2 = 1 - 2x + x^2 \\ g \circ f(x) = g(x^2) = 1 - x^2 \end{cases}$$

So $f \circ g \neq g \circ f$ (for instance at $x = \frac{1}{2}$).

Further examples :

a) Additive groups: $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$ are abelian groups.

b) Multiplicative groups: $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^* \times)$ are abelian groups. The same goes for $(\mathbb{R}^*_+, \times)$ (but not for $\mathbb{R}^*_-$ because the multiplication is not a binary operation on this set).

Proof : For instance for $(\mathbb{R}^*, \times)$:

1. $\times$ is a binary operation on $\mathbb{R}^*$ since the multiplication of two real numbers not equal to 0 remains a real number not equal to 0.
2. $\times$ is associative: $\forall (a,b,c) \in (\mathbb{R}^*)^3,\ (ab)c = a(bc) = abc$
3. $1 \in \mathbb{R}^*$ is identity element: $\forall a \in \mathbb{R}^*,\ a \times 1 = 1 \times a = a$
4. Every real number a not equal to 0 has a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^*$ which is inverse element of a (since $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$).
5. Finally the group is abelian since the multiplication of numbers is commutative.

■

c) Counterexamples $(\mathbb{N},+)$ is not a group since $1\in\mathbb{N}$ but there is no positive integer $a\in\mathbb{N}$ such that $1+a=a+1=0$ (actually $-1\notin\mathbb{N}$). The same goes for $(\mathbb{Z}-\{0\},\times)$ since $2\in\mathbb{Z}$ but $\frac{1}{2}\notin\mathbb{Z}$.

Proposition 1.4

Let $(G,\star)$ be a group. Then the following properties hold

1. *The identity element $e\in G$ is unique.*
2. *For any element $a\in G$, the inverse element of a in $(G,\star)$ is unique, denoted a^{-1}.*
3. *Simplifications are possible: $\forall(a,b,c)\in G^3$, $\begin{cases} a\star b=a\star c\Longrightarrow b=c\\ b\star a=c\star a\Longrightarrow b=c\end{cases}$*
4. *$\forall(a,b)\in G^2,\ (a\star b)^{-1}=b^{-1}\star a^{-1}$*

Proof: 1. By contradiction, assume e_1 and e_2 in G are identity elements for $\star$. Then

$$\forall a\in G,\ \begin{cases} a\star e_1=e_1\star a=a\\ a\star e_2=e_2\star a=a\end{cases}$$

$a=e_2$ in the first line gives $e_2\star e_1=e_1\star e_2=e_2$.
$a=e_1$ in the second line gives $e_1\star e_2=e_2\star e_1=e_1$.
Consequently $e_1=e_1\star e_2=e_2$, that is all identity elements must be equal. In other words there is only one identity element.

2. Similarly, given any element $a\in G$, assume a' and a'' in G are inverse elements of a. Then

$$\begin{cases} a\star a'=a'\star a=e\\ a\star a''=a''\star a=e\end{cases}$$

Using the identity element e and the associativity of binary operation $\star$, we get:

$$a'=a'\star e=a'\star(a\star a'')=(a'\star a)\star a''=e\star a''=a''$$

Thus, there is only one inverse element of a.

3. Using the inverse element of a and the associativity, we get:

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

The same goes for the second simplification.

4. We need to check the axiom of inverse element in Definition 1.2.

$$\begin{cases} (a\star b)\star(b^{-1}\star a^{-1})=a\star(b\star b^{-1})\star a^{-1}=a\star e\star a^{-1}=a\star a^{-1}=e\\ (b^{-1}\star a^{-1})\star(a\star b)=b^{-1}\star(a^{-1}\star a)\star b=b^{-1}\star e\star b=b^{-1}\star b=e\end{cases}$$

So $b^{-1}\star a^{-1}$ is the inverse element of the element $a\star b$. ■

Example: If f and g are two bijective functions from the segment $[0,1]$ to itself then $(f\circ g)^{-1}=g^{-1}\circ f^{-1}$ (which is not necessary equal to $f^{-1}\circ g^{-1}$ since composition of functions is not a commutative binary operation).

1.1.2 Subgroup

Example: Consider the abelian group $(\mathbb{Z},+)$ and the following subsets

$$\mathcal{E} = \{\text{even numbers}\} = \{2k,\ k\in\mathbb{Z}\}$$
$$\mathcal{O} = \{\text{odd numbers}\} = \{2k+1,\ k\in\mathbb{Z}\}$$

We have $\forall (a,b)\in\mathcal{E},\ a+b\in\mathcal{E}$ (if $a=2k$ and $b=2k'$ then $a+b=2k''$ with $k''=k+k'\in\mathbb{Z}$) but it is no longer true in $\mathcal{O}$. In other words, $+$ is a binary operation on $\mathcal{E}$ but not on $\mathcal{O}$.

Definition 1.5 (*Subgroup*)

Let $(G,\star)$ be a group and $H\subset G$ be a nonempty subset. $(H,\star)$ is a **subgroup** *of $(G,\star)$ if it satisfies each of the following subgroup axioms*

i) *$\star$ is a binary operation on H*

ii) *$(H,\star)$ is a group*

Example: For any group $(G,\star)$ with identity element e, $(\{e\},\star)$ is a subgroup of $(G,\star)$ called the **trivial subgroup**.

Proposition 1.6

Let $(G,\star)$ be a group and $H\subset G$ be a nonempty subset. $(H,\star)$ is a subgroup of $(G,\star)$ if and only if it satisfies the following condition

$$\forall (a,b)\in H^2,\ a\star b^{-1}\in H$$

Proof: **Necessary.** Let a and b be two elements in H. The axiom of inverse element in Definition 1.2 gives $b^{-1}\in H$. And because $\star$ is a binary operation on H, we get $a\star b^{-1}\in H$.

Sufficient. We need to check that each axiom from Definition 1.2 is satisfied for $(H,\star)$ and $\star$ is a binary operation on H.

1. The axiom of associativity for $(H,\star)$ comes directly from that one satisfied by $(G,\star)$.
2. Denote $e\in G$ the identity element of $(G,\star)$. Since H is nonempty, there exists an element $a\in H$. It follows $e=a\star a^{-1}\in H$. Consequently there exists an identity element in $(H,\star)$ or equivalently, the axiom of identity element is checked for $(H,\star)$.
3. Now the inverse element in $(G,\star)$ of any $a\in H$ satisfy $a^{-1}=e\star a^{-1}\in H$ (since $e\in H$). In particular any element $a\in H$ has an inverse element in $(H,\star)$ or equivalently, the axiom of inverse element is checked for $(H,\star)$.
4. Finally for every elements a and b in H, we get $a\star b=a\star(b^{-1})^{-1}\in H$ (since $b^{-1}\in H$). In other words, $\star$ is well a binary operation on H. ■

Remark: In practice, it is more convenient to use Proposition 1.6 to show that $(H,\star)$ is a subgroup of $(G,\star)$ than Definition 1.5

Examples: $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$. $(\mathbb{Q},+)$ is a subgroup of $(\mathbb{R},+)$ and $(\mathbb{C},+)$. $(\mathbb{R}^*_+,\times)$ is a subgroup of $(\mathbb{R}^*,\times)$ and $(\mathbb{C}^*,\times)$.

Proposition 1.7

For every positive integer $n \in \mathbb{N}^*$, consider the following subset of $\mathbb{Z}$

$$n\mathbb{Z} = \{\text{multiples of } n\} = \{nk,\ k \in \mathbb{Z}\}$$

Then $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Proof: $n\mathbb{Z}$ is well a nonempty subset of $\mathbb{Z}$ (for instance $0 \in n\mathbb{Z}$). Let $a = nk$ and $b = nk'$ be two elements in $n\mathbb{Z}$. Then

$$a + (-b) = (nk) + \big(-(nk')\big) = n(k - k') \in n\mathbb{Z}$$

Hence, the result follows from Proposition 1.6. ■

Example: $\mathcal{E} = \{\text{even numbers}\} = 2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Further examples:

a) Consider the following set of all complex numbers with absolute value 1 (that is the unital circle in the complex plane)

$$\mathbb{T} = \{z \in \mathbb{C} \,/\, |z| = 1\}$$

Then $(\mathbb{T}, \times)$ is a subgroup of $(\mathbb{C}^*, \times)$ called the **circle group**.

Proof: If $|z| = 1$ for a complex number $z \in \mathbb{C}$ then $z \neq 0$. Moreover $1 \in \mathbb{T}$. So $\mathbb{T}$ is a nonempty subset of $\mathbb{C}^*$. Now using the claims that the absolute value of the multiplicative inverse of a complex number is the multiplicative inverse of its absolute value and the absolute value of the product of two complex numbers is equal to the product of their absolute values, we get

$$\forall (z, w) \in \mathbb{T}^2,\ |z \times w^{-1}| = \frac{|z|}{|w|} = 1$$

The conclusion follows with Proposition 1.6. ■

b) For every positive integer $n \in \mathbb{N}^*$, consider the following subset of $\mathbb{C}$

$$\mathcal{R}_n = \{n^{\text{th}} \text{ root of unity}\} = \{z \in \mathbb{C} \,/\, z^n = 1\}$$

Then $(\mathcal{R}_n, \times)$ is a subgroup of $(\mathbb{T}, \times)$ (and of $(\mathbb{C}^*, \times)$ as well). It is finite with cardinality n.

Proof: If $z^n = 1$ for a complex number $z \in \mathbb{C}$ then $|z|^n = |z^n| = 1$ and consequently $|z| = 1$ (because $|z| \in \mathbb{R}_+$). Moreover 1 is a root of unitaly for every power $n \in \mathbb{N}^*$. So $\mathcal{R}_n$ is a nonempty subset of $\mathbb{T}$. Actually $\mathcal{R}_n$ may be written as follows

$$\mathcal{R}_n = \left\{z = e^{\imath \frac{2k\pi}{n}},\ k \in \{0, 1, \ldots, n-1\}\right\} \text{ where } \forall \theta \in \mathbb{R},\ e^{\imath\theta} = \cos(\theta) + \imath \sin(\theta)$$

In particular, $\mathcal{R}_n$ is a finite set with cardinality n. We conclude as in the previous proof for $(\mathbb{T}, \times)$ since the exponentiation function $z \mapsto z^n$ satisfies the same required properties as the absolute value for complex numbers. ■

1.1.3 Group homomorphism

Definition 1.8 (*Group homomorphism*)

Let $(G, \star)$ and $(H, \cdot)$ be two groups. A ***group homomorphism*** *from $(G, \star)$ to $(H, \cdot)$ is a function $\varphi : G \to H$ such that*

$$\forall (a, b) \in G^2,\ \varphi(a \star b) = \varphi(a) \cdot \varphi(b)$$

Moreover

- *If a group homomorphism $\varphi : G \to H$ is a bijection, then it is called a* ***group isomorphism****.*
- *If $\psi : G \to G$ is a group homomorphism from $(G, \star)$ to itself, then it is called a* ***group endomorphism****. If furthermore ψ is bijective and hence a group isomorphism, it is called a* ***group automorphism****.*

Remark : If $\varphi : G \to H$ is a group isomorphism, then its bijective inverse $\varphi^{-1} : H \to G$ is also a group homomorphism.

Proof : Let a and b be two elements in H. Since φ is a surjective function, there exist two elements a' and b' in G such that $a = \varphi(a')$ and $b = \varphi(b')$. Then

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

■

Some examples :

a) The constant function $\varphi : a \mapsto \varphi(a) = e_H$ equal to the identity element of $(H, \cdot)$ is a group homomorphism from $(G, \star)$ to $(H, \cdot)$ (even onto the trivial subgroup $(\{e_H\}, \cdot)$).

b) The identity function $\varphi = \mathrm{Id}_G = (a \mapsto a)$ is a group automorphism of $(G, \star)$.

c) Given $n \in \mathbb{Z}$, $\varphi_n : \mathbb{Z} \to \mathbb{Z},\ k \mapsto nk$ is a group endomorphism from $(\mathbb{Z}, +)$ to itself and a group isomorphism from $(\mathbb{Z}, +)$ onto its subgroup $(n\mathbb{Z}, +)$.

d) Given $\lambda \in \mathbb{R}$, $\varphi_\lambda : \mathbb{R} \to \mathbb{R},\ x \mapsto \lambda x$ is a group endomorphism from $(\mathbb{R}, +)$ to itself. Moreover it is a group automorphism if and only if $\lambda \neq 0$.

Proof :

$$\forall (x, y) \in \mathbb{R}^2,\ \varphi_\lambda(x + y) = \lambda(x + y) = \lambda x + \lambda y = \varphi_\lambda(x) + \varphi_\lambda(y)$$

And φ_λ is a bijective function over $\mathbb{R}$ if and only if $\lambda \neq 0$ (in this case, the associated bijective inverse is $(x \mapsto x/\lambda) = \varphi_{1/\lambda}$). ■

e) $\exp : \mathbb{R} \to \mathbb{R}_+^*,\ x \mapsto \exp(x)$ is a group isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$.

Proof :

$$\forall (x, y) \in \mathbb{R}^2,\ \exp(x + y) = \exp(x) \exp(y)$$

And $\exp : \mathbb{R} \to \mathbb{R}_+^*$ is a bijective function (whose bijective inverse is $\ln : \mathbb{R}_+^* \to \mathbb{R}$). ■

1.2 Ring

1.2.1 Definitions and examples

Definition 1.9 (*Ring*)

Let $(R, +, \times)$ be a nonempty set with two binary operations denoted $+$ and $\times$. $(R, +, \times)$ is said to be a ***ring*** *if it satisfies each of the following ring axioms*

i) *$(R, +)$ is an abelian group*

ii) *the binary operation $\times$ is associative:*

$$\forall (a, b, c) \in R^3,\ (a \times b) \times c = a \times (b \times c) = a \times b \times c$$

iii) *the binary operation $\times$ is* ***distributive*** *over the binary operation $+$:*

$$\forall (a, b, c) \in R^3,\ \begin{cases} a \times (b + c) = (a \times b) + (a \times c) \\ (b + c) \times a = (b \times a) + (c \times a) \end{cases}$$

Moreover a ring $(R, +, \times)$ is said

- ***unital*** *if there exists an identity element for the binary operation $\times$:*

$$\exists e \in R /\ \forall a \in R,\ a \times e = e \times a = a$$

- ***commutative*** *if the binary operation $\times$ is commutative:*

$$\forall (a, b) \in R^2,\ a \times b = b \times a$$

We denote

- *0_R the identity element for the binary operation $+$, called the* ***additive identity***
- *1_R the identity element for the binary operation $\times$ in case $(R, +, \times)$ is unital, called the* ***multiplicative identity***
- *$-a$ the inverse element of an element $a \in R$ for the binary operation $+$, called the* ***additive inverse*** *(or* ***opposite****)*

Example : $(\mathbb{Z}, +, \times) \subset (\mathbb{Q}, +, \times) \subset (\mathbb{R}, +, \times) \subset (\mathbb{C}, +, \times)$ are commutative unital rings.

Proof : For instance for $(\mathbb{Q}, +, \times)$:

1. $+$ and $\times$ are binary operations on $\mathbb{Q}$: $\forall (a, b) \in \mathbb{Q}^2,\ a + b \in \mathbb{Q}$ and $ab \in \mathbb{Q}$
2. $(\mathbb{Q}, +)$ is an abelian group.
3. $\times$ is associative on $\mathbb{Q}$: $\forall (a, b, c) \in \mathbb{Q}^3,\ (ab)c = a(bc) = abc$
4. $\times$ is distributive over $+$: $\forall (a, b, c) \in \mathbb{Q}^3,\ a(b + c) = (ab) + (ac)$
5. $\times$ has a multiplicative identity in $\mathbb{Q}$: $1_{\mathbb{Q}} = 1$ since $\forall a \in \mathbb{Q},\ a \times 1 = 1 \times a = a$
6. $\times$ is commutative on $\mathbb{Q}$: $\forall (a, b) \in \mathbb{Q}^2,\ ab = ba$ ■

Example : Let $\mathcal{F}$ be the set of all functions from $\mathbb{R}$ to itself.

$$\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$$

For every functions f and g in $\mathcal{F}$, the function $f+g \in \mathcal{F}$ is defined by $\forall x \in \mathbb{R},\ (f+g)(x) = f(x)+g(x)$ (using addition of real numbers) and the function $f \times g \in \mathcal{F}$ by $\forall x \in \mathbb{R},\ (f \times g)(x) = f(x)g(x)$ (using multiplication of real numbers). Then $(\mathcal{F}, +, \times)$ is a commutative unital ring.

Proof :

1. $+$ and $\times$ are binary operations on $\mathcal{F}$ by definition.
2. $(\mathcal{F}, +)$ is an abelian group: the associativity and the commutativity come from those ones of $(\mathbb{R}, +)$, the additive identity is the constant function $0_{\mathcal{F}} : x \mapsto 0$ and the additive inverse of a function $f \in \mathcal{F}$ is the function $-f$ defined by $-f : x \mapsto -x$.
3. $\times$ is associative on $\mathbb{R}$, so the same does on $\mathcal{F}$ as well.
4. $\times$ is distributive over $+$ on $\mathbb{R}$, so the same does on $\mathcal{F}$ as well.
5. The constant function $1_{\mathcal{F}} : x \mapsto 1$ is a multiplicative identity for $\times$ in $\mathcal{F}$.
6. $\times$ is commutative on $\mathbb{R}$, so the same does on $\mathcal{F}$ as well. ■

Proposition 1.10

Let $(R, +, \times)$ be a ring. Then the following properties hold

1. *If $(R, +, \times)$ is unital, then the multiplicative identity $1_R \in R$ is unique.*
2. $\forall a \in R,\ a \times 0_R = 0_R \times a = 0_R$
3. *If $(R, +, \times)$ is unital, then $\forall a \in R,\ (-1_R) \times a = a \times (-1_R) = -a$*
4. $\forall (a, b) \in R^2,\ (-a) \times b = a \times (-b) = -(a \times b)$

Proof :

1. Actually the same proof as for the first property from Proposition 1.4 still holds.
2. Using the distributivity of $+$ over $\times$ and the additive identity 0_R, we get:

$$0_R \times a + 0_R \times a = (0_R + 0_R) \times a = 0_R \times a = 0_R + 0_R \times a$$

Now a simplification on each side by $0_R \times a$ (see Proposition 1.4) gives $0_R = 0_R \times a$ as needed. The same goes for $a \times 0_R$.

3. We have

$$a + (-1_R) \times a = 1_R \times a + (-1_R) \times a = (1_R + (-1_R)) \times a = 0_R \times a = 0_R$$

Consequently $(-1_R) \times a$ is the additive inverse of the element a (since $(R, +)$ is an abelian group whose its additive identity is 0_R). The same goes for $a \times (-1_R)$.

4. We have

$$a \times b + (-a) \times b = (a + (-a)) \times b = 0_R \times b = 0_R$$

The conclusion follows. ■

Remark : In particular, the second point of the previous proposition shows that the additive identity 0_R of a ring $(R, +, \times)$ has no multiplicative inverse: there is no element $a \in R$ such that $0_R \times a = a \times 0_R = 1_R$.

Definition 1.11 (*Subring*)

Let $(R, +, \times)$ be a ring and $T \subset R$ be a nonempty subset. $(T, +, \times)$ is a ***subring*** *of $(R, +, \times)$ if it satisfies each of the following subring axioms*

i) *$(T, +)$ is a subgroup of $(R, +)$*

ii) *$\times$ is a binary operation on T*

In this case, $(T, +, \times)$ is a ring.

Trivial example : For any ring $(R, +, \times)$, $(\{0_R\}, +, \times)$ is a subring called the **trivial subring**.

Examples : $(\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$. For every positive integer $n \in \mathbb{N}^*$, $(n\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Z}, +, \times)$ which is not unital as soon as $n \geqslant 2$ (since $1 \notin n\mathbb{Z}$).

Proof : For instance for $(n\mathbb{Z}, +, \times)$:

1. $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$ (see Proposition 1.7)
2. If $a = nk$ and $b = nk'$ are two elements in $n\mathbb{Z}$ then $a \times b = (nk) \times (nk') = n(knk') \in n\mathbb{Z}$. Hence, $\times$ is a binary operation on $n\mathbb{Z}$. ■

Definition 1.12 (*Ring homomorphism*)

Let $(R, +, \times)$ and $(T, \oplus, \otimes)$ be two rings. A ***ring homomorphism*** *from $(R, +, \times)$ to $(T, \oplus, \otimes)$ is a function $\varphi : R \to T$ such that*

$$\forall (a, b) \in R^2, \begin{cases} \varphi(a + b) = \varphi(a) \oplus \varphi(b) \\ \varphi(a \times b) = \varphi(a) \otimes \varphi(b) \end{cases}$$

Moreover

- *If a ring homomorphism $\varphi : R \to T$ is a bijection, then it is called a* ***ring isomorphism***.
- *If $\psi : R \to R$ is a ring homomorphism from $(R, +, \times)$ to itself, then it is called a* ***ring endomorphism***. *If furthermore ψ is bijective and hence a ring isomorphism, it is called a* ***ring automorphism***.

Remark : The same remark as for group isomorphism holds: the bijective inverse of any ring isomorphism is also a ring homomorphism.

1.2.2 The rings $\mathbb{Z}/n\mathbb{Z}$

Remind the following result:

Theorem 1.13 (*Division algorithm*)

For any given two integers a and d with $d \neq 0$, there exist unique integers q and r such that

$$\begin{cases} a = qd + r \\ 0 \leqslant r < |d| \end{cases}$$

The integer q is called the ***quotient***, *r the* ***remainder***, *d the* ***divisor*** *and a the* ***dividend***.

Fix a positive integer $n \in \mathbb{N}^*$.

Definition 1.14 (*Congruence modulo n*)

Two integers a and b are said **congruent modulo n** *if n divides their difference $a - b$, that is if there exists an integer q such that $a - b = qn$ (equivalently if the remainder of the division algorithm with dividend $a - b$ and divisor n is equal to 0). In this case, we write* $\boldsymbol{a \equiv b[n]}$.

Remark : In particular, any integer a is congruent modulo n to its associated remainder r of the division algorithm with dividend a and divisor n (since $a - r = qn$). Moreover if two integers a and b have the same remainder r from the division algorithm with divisor n, then they are congruent modulo n (since $a = qn + r$ and $b = q'n + r'$ with $r = r'$ imply $a - b = (q - q')n$).

Definition 1.15 (*Congruence class*)

For any given integer $a \in \mathbb{Z}$, the **congruence class modulo n** *of a is the following set*

$$\begin{aligned} \overline{a} &= \{\textit{integers congruent modulo } n \textit{ to } a\} \\ &= \{b \in \mathbb{Z} \,/\, b \equiv a[n]\} \\ &= \{\dots, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \dots\} \\ &= a + n\mathbb{Z} \end{aligned}$$

Proposition 1.16

Let $\overline{a}$ and $\overline{b}$ be two congruence classes modulo n associated to two integers a and b. Then $\overline{a}$ and $\overline{b}$ are equal if and only if a and b are congruent modulo n.

$$\forall (a, b) \in \mathbb{Z}^2,\ \overline{a} = \overline{b} \Leftrightarrow a \equiv b[n]$$

Proof : Necessary. If $\overline{a} = \overline{b}$ then in particular $b \in \overline{a}$ that is b is congruent modulo n to a.

Sufficient. If b is congruent modulo n to a then there exists an integer q such that $a = b + qn$.
Consequently

$$\overline{a} = a + n\mathbb{Z} = b + qn + n\mathbb{Z} = b + n(q + \mathbb{Z}) = b + n\mathbb{Z} = \overline{b}$$

■

Remark : In particular, for any given integer $a \in \mathbb{Z}$, if r denotes the remainder of the division algorithm with dividend a and divisor n then $\overline{a} = \overline{r}$.

Definition 1.17 ($\mathbb{Z}/n\mathbb{Z}$)

The set of all congruence classes modulo n is denoted by $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ *(read "$\mathbb{Z}$ over $n\mathbb{Z}$").*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &= \{\textit{congruence classes modulo } n\} \\ &= \{\overline{a},\ a \in \mathbb{Z}\} \\ &= \{\textit{congruence classes modulo } n \textit{ of the remainders} \\ &\qquad\qquad \textit{from the division algorithm with divisor } n\} \\ &= \{\overline{r},\ r \in \mathbb{Z} \text{ and } 0 \leqslant r < n\} \\ &= \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} \end{aligned}$$

It is a finite set with cardinality n.

Example: For $n = 2$, $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$. For instance $\overline{2} = \overline{0}$ and $\overline{5} = \overline{1}$ (equivalently we may write $2 \equiv 0[2]$ and $5 \equiv 1[2]$). Actually

$$\left\{\begin{array}{lcl} a \text{ even} & \Longrightarrow & \overline{a} = \overline{0} \\ a \text{ odd} & \Longrightarrow & \overline{a} = \overline{1} \end{array}\right.$$

Example: For $n = 3$, $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. For instance $\overline{6} = \overline{0}$ (or $6 \equiv 0[3]$) and $\overline{13} = \overline{1}$ (or $13 \equiv 1[3]$) because $13 = 4 \times 3 + 1$.

Definition 1.18 (*Addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$*)

Two binary operations on $\mathbb{Z}/n\mathbb{Z}$ denoted by $+$ and $\times$ are defined as follows (using addition and multiplication of integers)

$$\forall (r, r') \in \{0, 1, \dots, n-1\}^2, \left\{\begin{array}{lcl} \overline{r} + \overline{r'} & = & \overline{r + r'} \\ \overline{r} \times \overline{r'} & = & \overline{rr'} \end{array}\right.$$

Proposition 1.19

$$\forall (a, b) \in \mathbb{Z}^2, \left\{\begin{array}{lcl} \overline{a} + \overline{b} & = & \overline{a + b} \\ \overline{a} \times \overline{b} & = & \overline{ab} \end{array}\right.$$

Proof: From Theorem 1.13, $a = qn + r$ and $b = q'n + r'$ for some integers q, q', r, r' with $0 \leqslant r, r' < n$.

- We have $(a + b) - (r + r') = (q + q')n$. So $(a + b)$ and $(r + r')$ are congruent modulo n. It follows from Proposition 1.16 that

$$\overline{a + b} = \overline{r + r'} = \overline{r} + \overline{r'} = \overline{a} + \overline{b}$$

- We have

$$ab = (qn + r)(q'n + r') = qq'n^2 + (qr' + q'r)n + rr'$$

Thus $ab - rr' = (qq'n + qr' + q'r)n$ that is ab and rr' are congruent modulo n. It follows from Proposition 1.16 that

$$\overline{ab} = \overline{rr'} = \overline{r} \times \overline{r'} = \overline{a} \times \overline{b}$$

■

Corollary 1.20

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *is a commutative unital ring whose identity elements are respectively* $\overline{0}$ *for the binary operation* $+$ *and* $\overline{1}$ *for the binary operation* $\times$.

Proof: Proposition 1.19 gives everything we need from the fact that $(\mathbb{Z}, +, \times)$ is a commutative unital ring whose identity elements are respectively 0 and 1. ■

Example: Some computations in $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$:

a) $\overline{15} = \overline{3}$ since $15 = 2 \times 6 + 3$

b) $\overline{4} + \overline{5} = \overline{4 + 5} = \overline{9} = \overline{3 + 6} = \overline{3}$

c) $\overline{4} + \overline{2} = \overline{6} = \overline{0}$ thus $-\overline{4} = \overline{2}$

d) $\overline{5} \times \overline{4} = \overline{5 \times 4} = \overline{20} = \overline{3 \times 6 + 2} = \overline{2}$

Remark: In $\mathbb{Z}/6\mathbb{Z}$, we have $\overline{3} \times \overline{2} = \overline{6} = \overline{0}$ but $\overline{3} \neq \overline{0}$ and $\overline{2} \neq \overline{0}$.

1.3 Field

Definition 1.21

Let $(F, +, \times)$ be a nonempty set with two binary operations. $(F, +, \times)$ is said to be a ***field*** *if it satisfies each of the following field axioms*

i) *$(F, +, \times)$ is an unital ring*

ii) *every element except 0_F has an inverse element in F for the binary operation $\times$:*

$$\forall a \in F - \{0_F\},\ \exists a^{-1} \in F /\ a \times a^{-1} = a^{-1} \times a = 1_F$$

Moreover a field $(F, +, \times)$ is said ***commutative*** *if the binary operation $\times$ is commutative:*

$$\forall (a, b) \in F^2,\ a \times b = b \times a$$

The same notations as for ring (0_F, 1_F and $-a$) are used and we denote a^{-1} the inverse element of an element $a \in F - \{0_F\}$ for the binary operation $\times$ (called the ***multiplicative inverse****).*

Remark: Equivalently $(F, +, \times)$ is a field if and only if it satisfies each of the following conditions

i) $(F, +)$ is an abelian group (whose its additive identity is denoted by 0_F)

ii) $(F - \{0_F\}, \times)$ is a group

iii) the binary operation $\times$ is distributive over the binary operation $+$

Examples: $(\mathbb{Q}, +, \times) \subset (\mathbb{R}, +, \times) \subset (\mathbb{C}, +, \times)$ are commutative fields.

Counterexample: $(\mathbb{Z}, +, \times)$ is not a field since $2 \in \mathbb{Z} - \{0\}$ has no multiplicative inverse in $\mathbb{Z}$: there is no integer $a \in \mathbb{Z}$ such that $2a = 1$ (equivalently $(\mathbb{Z} - \{0\}, \times)$ is not a group).

Proposition 1.22

Let $(F, +, \times)$ be a field. Then

$$\forall (a, b) \in F^2,\ a \times b = 0_F \Longrightarrow \text{either } a = 0_F \text{ or } b = 0_F$$

Proof: Assume $a \neq 0_F$. Consequently, there exists a multiplicative inverse $a^{-1} \in F$ and we get:

$$b = 1_F \times b = (a^{-1} \times a) \times b = a^{-1} \times (a \times b) = a^{-1} \times 0_F = 0_F$$

■

Remark: In particular, if there exist two elements a and b in a ring $(R, +, \times)$ such that $a \times b = 0_R$ but $a \neq 0_R$ and $b \neq 0_R$ (such elements are called **zero divisors**) then $(R, +, \times)$ is not a field. More precisely, any zero divisor does not have multiplicative inverse.

Example: $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ is not a field (since $\overline{3} \times \overline{2} = \overline{0}$ but $\overline{3} \neq \overline{0}$ and $\overline{2} \neq \overline{0}$).

Theorem 1.23

Let $n \in \mathbb{N}^*$ be a positive integer. Then $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a commutative field if and only if n is a prime number.

Proof : **Necessary.** The proof is the same as the previous example. By contradiction, assume that $n \in \mathbb{N}^*$ is not a prime number. In other words, there exist two integers p and q such that $1 < p, q < n$ and $n = pq$. Then $\overline{p} \times \overline{q} = \overline{pq} = \overline{n} = \overline{0}$ but $\overline{p} \neq \overline{0}$ and $\overline{q} \neq \overline{0}$. That is a contradiction with Proposition 1.22.

Sufficient. Assume n is a prime number and let $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$ be a congruence class not equal to the congruence class $\overline{0}$. We may assume that $0 < r < n$. In particular, r and n are relatively prime. Remind the following result:

Theorem 1.24 (*Bézout's identity*)

If two integers a and b are relatively prime then there exist integers x and y such that

$$ax + by = 1$$

Here we get two integers x and y such that $rx + ny = 1$. Consequently

$$\overline{r} \times \overline{x} = \overline{rx} = \overline{1 - ny} = \overline{1}$$

In other words, $\overline{x}$ is the multiplicative inverse of $\overline{r}$. So, any congruence class in $\mathbb{Z}/n\mathbb{Z}$ not equal to $\overline{0}$ has a multiplicative inverse. ■

Example : In $\mathbb{Z}/7\mathbb{Z}$, the multiplicative inverse of $\overline{2}$ is $\overline{4}$ since $\overline{2} \times \overline{4} = \overline{2 \times 4} = \overline{8} = \overline{1}$ (and then the multiplicative inverse of $\overline{4}$ is $\overline{2}$). Moreover, we have $\overline{3}^{-1} = \overline{5}$ (since $\overline{3} \times \overline{5} = \overline{15} = \overline{1 + 2 \times 7} = \overline{1}$) and $\overline{6}^{-1} = \overline{6}$ (since $\overline{6} \times \overline{6} = \overline{36} = \overline{1 + 5 \times 7} = \overline{1}$).