Algebraic structures

1. Binary operations

Definition 1. *Let G be a non-empty set. Binary operation or (law of internal composition) on G any map $*$: $G \times G \longrightarrow G$. We usually write $x * y$ instead $*(x, y)$. Binary operations are designated by the symbols $*, \bullet, \star, ..., etc.$*

Examples

1- Addition and multiplication are binary operations on $\mathbb{Z}; \mathbb{Q}; \mathbb{R}; \mathbb{C}$.

2- The map:

$$\begin{aligned} * : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto x * y = xy + y \end{aligned}$$

is a binary operation on $\mathbb{R}$.

3- Let E be a non-empty set. The map:

$$\begin{aligned} * : \mathcal{P}(E) \times \mathcal{P}(E) &\longrightarrow \mathcal{P}(E) \\ (A, B) &\longmapsto A * B = A \cup B \end{aligned}$$

is a binary operation on $\mathcal{P}(E)$.

4- Let E be a non-empty set. The map:

$$\begin{aligned} \Theta : \mathcal{P}(E) \times \mathcal{P}(E) &\longrightarrow \mathbb{R} \\ (A, B) &\longmapsto A \Theta B = |A \cup B| \end{aligned}$$

is not a binary operation on $\mathcal{P}(E)$.

Definition 2.

1- A binary operation $*$ on a set G is said to be associative if

$$\forall x, y, z \in G, x * (y * z) = (x * y) * z.$$

2- A binary operation $*$ on a set G is said to be commutative if

$$\forall x, y \in G, x * y = y * x.$$

Examples

1- The usual operations $+$ and $\times$ defined on $\mathbb{R}$ are associative and commutative.

2- The operation $*$ defined on $\mathbb{R}$ by $x*y = y-x$ is neither associative nor commutative.

3- The operation $*$ defined on $\mathbb{R}^\star$ by $x * y = y \div x$ is associative, not commutative.

Definition 3. *Let $*$ a binary operation on a set G.*

1-An element $e \in G$ is called to be a neutral element (identity element) if

$$\forall x \in G : x * e = e * x = x$$

2- Let e be an identity element of G. We say that an element x in the set G admits a symmetric (inverse) element, if

$$\exists x' \in G : x * x' = x' * x = e$$

Examples

1- 0 is the identity element for the usual operation $+$ defined on $\mathbb{R}$.

2- 2 is the identity element for the operation $*$ defined on $\mathbb{R}\setminus\{1\}$ by $x*y = xy - x - y + 2$.

Remarks

1- If the binary operation is denoted $+$ additively (resp. $\times$ multiplicatively), the identity element e will be denoted by 0 (resp. 1), and the inverse x' will be denoted by $-x$ (resp. x^{-1}).

2- If they exist, the neutral and inverse elements are unique.

2. Group

Definition 4. *Let G be a non-empty set equipped with a binary operation $*$. We say that $(G, *)$, (or simply G), is a group if and only if:*

1- The operation $*$ is associative.

2- The operation $*$ admits a neutral element.

3- Every element $x \in G$ admits a symmetric $x' \in G$.

Furthermore, if the operation $*$ is commutative, then $(G, *)$, is called a commutative or an Abelian group.

Examples

1- The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are commutative groups for addition, and if e is the neutral element and if x belongs to one of these groups then:

$$e = 0 \quad \wedge \quad x^{-1} = -x$$

2- The sets $\mathbb{Q}^*, \mathbb{R}^*$, and $\mathbb{C}^*$ are commutative groups for multiplication and if e is the neutral element and if x belongs to one of these groups then:

$$e = 1 \wedge x^{-1} = \frac{1}{x}$$

3- Let E be a non-empty set. The set $S(E)$ of bijective maps from E to E is a non-commutative group for the operation $(\circ)$. The neutral element is the identity map id_E and the symmetric of a map f is the inverse map f^{-1} of f.

Some conventions

- The notation $(G, +)$ is called additive. In this case, the symmetric element of an element $x \in G$ is $-x$ and for any $n \in \mathbb{Z}$ we define

$$nx = \begin{cases} 0 & \text{if } n = 0 \\ \underbrace{x + x + \cdots + x}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ times}} & \text{if } n < 0. \end{cases}$$

- The notation $(G, .)$ or $(G, \times)$ is called multiplicative. In this notation the symmetric element of an element $x \in G$ is x^{-1} and for any $n \in \mathbb{Z}$ we define

$$x^n = \begin{cases} 1 & \text{if } n = 0 \\ \underbrace{x \cdot x \cdots x}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{(x^{-1}) \cdot (x^{-1}) \cdots (x^{-1})}_{n \text{ times}} & \text{if } n < 0. \end{cases}$$

2.1. Subgroups.

Definition 5. *Let $(G, *)$ be a group. A non-empty subset H of G is a subgroup of G if $(H, *)$ is a group.*

Theorem 1. *Let $(G, *)$ be a group. A subset H of G is a subgroup of G if and only if:*

1. $H \neq \emptyset$
2. $\forall x, y \in H, x * y \in H$
3. $\forall x \in H, x' \in H$

Remarks

1- Properties 2 and 3 are equivalent to the following property:

$$\forall x, y \in H, x * y^{'} \in H$$

2- Any subgroup of a group G contains the neutral element e.

3- The group G and $\{e\}$ are subgroups of G called trivial subgroups.

4- If $(G, *)$ a group then:

$$\forall x, y \in G, (x * y)^{'} = y^{'} * x^{'}$$

Examples

1- For addition, the sets $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are subgroups of $\mathbb{C}$ and for multiplication $\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$ which is a subgroup of $\mathbb{C}^*$.

2- Consider the additive group $\mathbb{Z}$. It is easy to show that $H = 3\mathbb{Z} = \{3\alpha, \alpha \in \mathbb{Z}\} \subset \mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

2.2. Group homomorphisms.

Definition 6. *Let $(G,*)$ and (G',T) be two groups and $f : G \longrightarrow G'$ be a map. We say that f is a group homomorphism if and only if:*

$$\forall g_1, g_2 \in G, \quad f(g_1 * g_2) = f(g_1)\, T f(g_2)$$

Notation

The set of group homomorphisms from G to G' is denoted by $\mathrm{Hom}(G, G')$.

Examples

1- It is easy to verify that the following maps:

$$\begin{aligned} f : (\mathbb{R},+) &\longrightarrow (\mathbb{R},.) \\ x &\longmapsto f(x) = e^x \end{aligned} \qquad \begin{aligned} g : \left(\mathbb{R}^*_+,\cdot\right) &\longrightarrow (\mathbb{R},+) \\ x &\longmapsto g(x) = \log x \end{aligned}$$

are group homomorphisms.

2- Let $(G, .)$ be a group and g be an element of G. The following map:

$$\begin{aligned} f_g : G &\longrightarrow G \\ x &\longmapsto f_g(x) = g \cdot x \cdot g^{-1} \end{aligned}$$

$$f_g\left(x_1 \cdot x_2\right) = f_g\left(x_1\right) \cdot f_g\left(x_2\right)$$

We then have:

$$\begin{aligned} f_g\left(x_1 \cdot x_2\right) &= g \cdot \left(x_1 \cdot x_2\right) \cdot g^{-1} \\ &= g \cdot \left(x_1 \cdot g^{-1} \cdot g \cdot x_2\right) \cdot g^{-1} \quad \left(\text{ because } g^{-1} \cdot g = e\right) \\ &= \left(g \cdot x_1 \cdot g^{-1}\right) \cdot \left(g \cdot x_2 \cdot g^{-1}\right) \quad \left(\text{associativity }\right) \\ &= f_g\left(x_1\right) \cdot f_g\left(x_2\right) \end{aligned}$$

- It is easy to show that f_g is bijective.

Definition 7. *Let G and G' be two groups and $f \in \mathrm{Hom}(G, G')$.*

1. *If f is injective then f is called monomorphism.*
2. *If f is surjective then f is called epimorphism.*
3. *If f is bijective then f is called isomorphism.*
4. *If $f \in \mathrm{Hom}(G,G)$ then f is called endomorphism of G and we write $f \in \mathrm{Hom}(G)$.*
5. *If $f \in \mathrm{Hom}(G)$ and f is bijective then f is called automorphism of G and we write $f \in \mathrm{Aut}(G)$.*

3. Rings

Definition 8. *Let R be a non-empty set equipped with two binary operations $(*)$ and (T). We say that $(R,*,T)$ (or simply R) is a ring if and only if:*

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

2. *The binary operation (T) is associative.*

3. *The binary operation (T) is distributive to the left and right for the binary operation $(*)$, i.e, $\forall x,y,z \in R$, we have :*

$$xT(y*z) = (xTy)*(xTz)$$

$$(x*y)Tz = (xTz)*(yTz)$$

4. *The binary operation (T) admits a neutral element denoted 1_R or 1. Furthermore, if (T) is commutative, then R is a commutative ring.*

Example

1- $(\mathbb{Z},+,.),(\mathbb{Q},+,.),(\mathbb{R},+,.)$ and $(\mathbb{C},+,.)$ are commutative rings and we have: $e = 0, 1_R = 1$

Definition 9. *Let $(R,*,T)$ be a ring such that $e \neq 1_R$ (e and 1_R are the neutral elements for $(*)$ and (T) respectively). We say that R is an integral domain if and only if:*

$$\forall x, y \in R, xTy = e \Rightarrow x = e \vee y = e$$

Example

The rings $(\mathbb{Z},+,.),(\mathbb{Q},+,.),(\mathbb{R},+,.)$ and $(\mathbb{C},+,.)$ are integral domains because for all x and all y in one of these rings, we have:

$$x.y = 0 \Rightarrow x = 0 \vee y = 0$$

Notation

When there is no ambiguity. we denote by

$$(R,*,T) := (R,+,\cdot)$$

$$ab := a \cdot b = a \times b.$$

$$a - b := a + (-b).$$

Proposition 1. *Let* $(R, +, \cdot)$ *be a ring. Then*

1. $\forall a \in R : a0 = 0a = 0.$
2. $\forall a \in R : (-1)(a) = (a)(-1) = -a:$
3. $\forall a; b \in R : (-a)(b) = (a)(-b) = -(ab):$
4. $\forall a; b \in R; \forall n \in \mathbb{Z} : (na)b = a(nb) = n(ab).$

Proof. 1. $a0 = a(0 + 0) = a0 + a0$ then $a0 - a0 = a0$ then $a0 = 0$: In the same way we obtain $0a = 0$:

2. On one hand $(-1)a + (+1)a = (-1 + 1)a = 0a = 0$: On the other hand, $(-1)a + (+1)a = (-1)a + a$ this gives $-a = (-1)a$: The second equality is obtained in a similar way.

3. $(a - a)b = 0$ gives $ab + (a)b = 0$ hence $-(ab) = (-a)b$: In a similar way we get $(ab) = a(b)$.

4. By induction on n when n is positive and on n when n is negative. ∎

Proposition 2. *Let $(R, +, .)$ be a ring and $a, b \in R$ such that $ab = ba$: For any integer $n \geq 0$ we have*

1. $(a+b)^n = \sum_{p=0}^{n} C_n^p a^{n-p} b^p$
2. $a^{n+1} - b^{n+1} = (a-b) \sum_{p=0}^{n} a^{n-p} b^p$

Proof. By induction on n. ∎

Definition 10. *Let R and S be two rings. A map $f : R \to S$ is called a ring homomorphism if*

1. $f(a+b) = f(a) + f(b)$ *for all* $a, b \in R$.
2. $f(ab) = f(a)f(b)$ *for all* $a, b \in R$.
3. $f(1_R) = 1_S$.

3.1. Subrings.

Definition 11. *Let* $(R,+,.)$ *be a ring and* $B \subseteq R$. *Then* B *is a subring of* R *if and only if:*

1. B *is a subgroup of* R *for the operation* $+$

2. $\forall x, y \in B, xy \in B$

3.$1_R \in B$

Examples

1- $(\mathbb{Z},+,.)$ is a subring of $(\mathbb{Q},+,.)$ which is a subring of $(\mathbb{R},+,.)$.

2- The following set: $B = \{x + y\sqrt{7}, x, y \in \mathbb{Z}\}$ is a subring of $(\mathbb{R},+,.)$.

4. Field

Definition 12. *Let F be a non-empty set equipped with two binary operations $(+)$ and $(.)$. We say that $(F, +, .)$ (or just F) is a field if and only if:*

1. *$(F, +, .)$ is a commutative ring.*
2. *$\forall x \in F - \{e\}, x^{-1} \in F \quad (x^{-1}$ being the symmetric of x for the law (T)).*

Furthermore, if the law (T) is commutative then F is a commutative field.

Examples

The rings $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ and $(\mathbb{C}, +, .)$ are commutative fields.

4.1. **Subfield.**

Definition 13. *Let* $(F, +, .)$ *be a field and* $K \subseteq F$. *Then* K *is a subfield of* F *if and only if:*

(1) $1_F \in K$;
(2) $\forall\ a, b \in K, a - b \in K$;
(3) $\forall a, b \in K, ab \in K$;
(4) $\forall\ a \in K^*$, $a^{-1} \in K$, *where* $K^* = K - \{0_K\}$.