Chapter 4

Algebraic Structures

4.1 Internal Composition Laws and Their Properties

4.1.1 Internal Composition Laws

Definition 4.1 Let E be a set. An internal composition law $*$ on E is a mapping from $E \times E$ to E:

$$\begin{aligned} * : E \times E &\longrightarrow E \\ (x, y) &\mapsto x * y \end{aligned}$$

Notations

1. Instead of "internal composition law," we also say "operation of internal composition" or simply "internal operation."
2. $(E, *)$ is often used to denote a set E equipped with an internal operation $*$.

Example.

1. The laws $\cup$ (union), $\cap$ (intersection), and $\triangle$ (symmetric difference) on $\mathcal{P}(E)$ (the power set of E).
2. The law (composition) on $\mathcal{F}(E)$ (the set of functions from E to E).

3. The laws $+$ and $\times$ on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$.

4. Let * be defined on $\mathbb{R}$ by $x * y = \frac{1}{x+y}$. Then * is not an internal operation since $(-1, 1)$ does not have an image.

Definition 4.2 (Stable Subset for an Operation) Let E be a set equipped with an internal composition law * and F be a subset of E. We say that F is stable under the law * if

$$\forall (x, y) \in F \times F : x * y \in F$$

Example.

1. $\mathbb{R}^+$ and $\mathbb{R}^-$ are two stable subsets of $\mathbb{R}$ under the operation $+$.

2. For the operation $\times$, $\mathbb{R}^+$ is still a stable subset, but $\mathbb{R}^-$ is not.

4.1.2 Properties of internal composition laws

Definition 4.3 (Commutativity and Associativity) Let E be a set equipped with an internal composition law $*$.

We say that $*$ is commutative if $\forall (x, y) \in E^2 : x * y = y * x$.

We say that $*$ is associative if $\forall (x, y, z) \in E^3 : (x * y) * z = x * (y * z)$.

Example.

1. The addition and multiplication laws on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are commutative and associative.

2. Also, the union ($\cup$), intersection ($\cap$), and symmetric difference ($\triangle$) laws on $\mathcal{P}(E)$ are commutative and associative.

3. The composition law ($\circ$) on $\mathcal{F}(E)$ is associative but not commutative, because $f \circ g \neq g \circ f$ in general.

4. Let $*$ be the law defined on $\mathbb{Q}$ by: $x * y = \frac{x+y}{2}$. Then $*$ is commutative, because $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$, but it is not associative,

because $(-1 * 0) * 1 = \frac{1}{4} \neq -1 * (0 * 1) = \frac{-1}{4}$.

Definition 4.4 (Neutral Element) Let E be a set equipped with an internal composition law *. Let e be an element of E. We say that e is the neutral element for the law *, if

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

Remark 4.1 If the law $*$ is commutative, the equality $x * e = e * x$ is automatically satisfied.

Example.

1. In $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, 0 is neutral for the addition law, and 1 is neutral for the multiplication law.
2. In $\mathcal{P}(E)$, the empty set $(\emptyset)$ is neutral for the union law $(\cup)$, and E is neutral for the intersection law $(\cap)$.
3. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then $e = 1$ is a neutral element, because $x * e = x \Rightarrow x + e - 1 = x$. Thus, $e = 1$.

Proposition 4.1 (Uniqueness of the Neutral Element) The neutral element of E for the law * if it exists, is unique.

Proof. Indeed, let e' be another neutral element for $*$, then $e' = e' * e = e * e' = e$. Thus, the neutral element is unique.

Definition 4.5 (Inverse Element) Let E be a set equipped with an internal composition law * and let e be a neutral element. We say that the element x of E has an inverse element x' of E, if $\forall x \in E : x * x' = x' * x = e$.

Example.

1. In $\mathbb{R}$, the invertible elements for the multiplication law $(\times)$ are the non-zero elements.
2. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then $x \in \mathbb{R}$ has an inverse element $x' = 2 - x$, because $x * x' = 1 \Rightarrow x + x' - 1 = 1$. Thus, $x' = 2 - x$.

4.1.3 Properties of internal composition laws

Definition 4.3 (Commutativity and Associativity) Let E be a set equipped with an internal composition law $*$.

We say that $*$ is commutative if $\forall(x, y) \in E^2 : x * y = y * x$.

We say that $*$ is associative if $\forall(x, y, z) \in E^3 : (x * y) * z = x * (y * z)$.

Example.

1. The addition and multiplication laws on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative and associative.

2. The union ($\cup$), intersection ($\cap$), and symmetric difference ($\triangle$) laws on $\mathcal{P}(E)$ are commutative and associative.

3. The composition law ($\circ$) on $\mathcal{F}(E)$ is associative but not commutative, because $f \circ g \neq g \circ f$ in general.

4. Let $*$ be the law defined on $\mathbb{Q}$ by: $x * y = \frac{x+y}{2}$. Then $*$ is commutative, because $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$, but it is not associative, because $(-1 * 0) * 1 = \frac{1}{4} \neq -1 * (0 * 1) = \frac{-1}{4}$.

Definition 4.4 (Neutral Element) Let E be a set equipped with an internal composition law $*$. Let e be an element of E. We say that e is the neutral element for the law $*$ if $\forall x \in E : x * e = e * x = x$.

Remark 4.1 If the law $*$ is commutative, the equality $x * e = e * x$ is automatically satisfied.

Example.

1. In $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, 0 is the neutral element for the addition law, and 1 is the neutral element for the multiplication law.

2. In $\mathcal{P}(E)$, the empty set $\emptyset$ is the neutral element for the union law $\cup$, and E is the neutral element for the intersection law $\cap$.

3. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then $e = 1$ is a neutral element, because $x * e = x + e - 1 = x$. Thus, $e = 1$.

Proposition 4.1 (Uniqueness of the Neutral Element) The neutral element of E for the law $*$, if it exists, is unique.

Proof. Indeed, let e' be another neutral element for $*$, then $e' = e' * e = e * e' = e$. Thus, the neutral element is unique.

Definition 4.5 (Inverse Element) Let E be a set equipped with an internal composition law $*$ and let e be a neutral element. We say that the element x of E has an inverse element x' of E if $\forall x \in E : x * x' = x' * x = e$.

Example.

1. In $\mathbb{R}$, the invertible elements for the multiplication law are the non-zero elements.

2. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then each $x \in \mathbb{R}$ has an inverse element $x' = 2 - x$, because $x * x' = x + x' - 1 = 1$. Thus, $x' = 2 - x$.

Proposition 4.2 Let E be a set equipped with an associative internal composition law $*$ that has a neutral element.

1. The inverse element x' of x for the law $*$ in E, if it exists, is unique.

2. If $x, y \in E$ are invertible, then $x * y$ is invertible, and its inverse is given by

$$(x * y)' = y' * x'$$

Definition 4.6 (Distributivity) Let E be a set equipped with two internal composition laws $*$ and $\top$.

We say that $*$ is left distributive with respect to $\top$ if

$$\forall (x, y, z) \in E^3 : x * (y \top z) = (x * y) \top (x * z).$$

We say that $*$ is right distributive with respect to $\top$ if

$$\forall (x, y, z) \in E^3 : (x \top y) * z = (x * z) \top (y * z).$$

Remark 4.2 If the law $*$ is commutative, then one of these properties implies the other.

Example

1. In $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, the multiplication law $\times$ is left distributive with respect to the addition law $+$.

2. In $\mathcal{P}(E)$, the laws $\cup$ and $\cap$ are left distributive with respect to each other.

3. Let $*$ be the law defined on $\mathbb{R}$ by $x * y = x + y - xy$, and let $\top$ be the law defined on $\mathbb{R}$ by $x \top y = x + y - 1$. Since the law $*$ is commutative, it suffices to demonstrate left distributivity with respect to $\top$:

$$\begin{aligned} x * (y \top z) &= x * (x + y - 1) \\ &= 2x + y + z - xy - xz - 1 \quad \ldots\ldots \quad (1) \\ (x * y) \top (x * z) &= (x + y - xy) \top (x + z - xz) \\ &= 2x + y + z - xy - xz - 1 \quad \ldots\ldots \quad (2) \end{aligned}$$

$(1) = (2)$ So the law $*$ is left distributive with respect to the law $\top$.

4.2 Algebraic Structures

4.2.1 Groups

4.2.1.1 Definitions and Examples

Definition 4.7 (Group) A group is a non-empty set equipped with an internal composition law $(G, *)$ such that:

- $*$ is associative;
- $*$ has a neutral element e;
- every element in G is invertible (has an inverse) for $*$.

Remark 4.3 If $*$ is commutative, we say that $(G, *)$ is commutative or abelian.

Example

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are abelian groups;

2. The set $\mathcal{P}(E)$ equipped with the symmetric difference $\triangle$ is an abelian group;

3. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$, $(\mathcal{P}(E), \cap)$, and $(\mathcal{P}(E), \cup)$ are not groups.

Definition 4.8 (Subgroup) Let $(G, *)$ be a group and let H be a non-empty subset of G. We say that H is a subgroup of G if:

1. H is closed under $*$, i.e., for every $(x, y) \in H^2$, $x * y \in H$;

2. H is closed under taking inverses, i.e., for every $x \in H$, x' (the inverse of x) is also in H.

Example

1. Let $(G, *)$ be a group, then e_G and G are subgroups (called trivial subgroups);

2. Let $(\mathbb{Z}, +)$ be a group. Then $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, defined by

$$3\mathbb{Z} = \{3z : z \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

3. Let $(G, \cdot)$ be a group. Then the set $Z(G) = \{x \in G : \forall y \in G, xy = yx\}$ is a subgroup of G called the center of G.

Theorem 4.1 (Characterization of Subgroups) Let $(G, *)$ be a group and let H be a non-empty subset of G. Then H is a subgroup of G if and only if

$$\forall (x, y) \in H^2, x * y' \in H$$

Proposition 4.3 (Intersection of Subgroups) Let $(G, *)$ be a group and let $\{H_i\}_{i \in I}$ be a family of subgroups of G. Then $\cap_{i \in I} H_i$ is a subgroup of G.

Remark 4.4 The union of two subgroups of G is not necessarily a subgroup of G. For example, $2\mathbb{Z}$ and $3\mathbb{Z}$ are two subgroups of $(\mathbb{Z}, +)$, but their union is not a subgroup since 2 and 3 are in $2\mathbb{Z} \cup 3\mathbb{Z}$ while $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

4.2.1.2 Group Homomorphisms

Definition 4.9 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups. A group homomorphism (or simply morphism) from G_1 to G_2 is a function $f : G_1 \longrightarrow G_2$ such that for all $x, y \in G_1$,

$$f(x * y) = f(x) \perp f(y)$$

Example

Let f be defined as $\begin{array}{rcl} f: & \mathbb{R} & \longrightarrow \mathbb{R}^* \\ & x & \mapsto f(x) = 2^x \end{array}$. Then f is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^*, \times)$ because

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

Remark 4.5 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups and f be a homomorphism from G_1 to G_2. Then:

1. If f is bijective, then we say that f is an isomorphism;

2. If f is defined from $(G_1, *)$ to itself, then we say that f is an endomorphism;

3. If f is a bijective endomorphism, then we say that f is an automorphism.

Example

1. The exponential function is an isomorphism from the group $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$;

2. The natural logarithm function is an isomorphism from the group $(\mathbb{R}_+^*, \times)$ to $(\mathbb{R}, +)$.

Proposition 4.4 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups with neutral elements e_1 and e_2, respectively, and let f be a homomorphism from G_1 to G_2. Then:

1. $f(e_1) = e_2$;

2. For all $x \in G_1$, $(f(x))' = f(x')$.

Proposition 4.5 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups with neutral elements e_1 and e_2, respectively, and let f be a homomorphism from G_1 to G_2. Then:

1. If H is a subgroup of G_1, then $f(H)$ is a subgroup of G_2;

2. If H' is a subgroup of G_2, then $f^{-1}(H)$ is a subgroup of G_1.

Definition 4.10 (Kernel and Image of a Homomorphism) Let $(G_1, *)$ and $(G_2, \perp)$ be two groups, and let f be a homomorphism from G_1 to G_2. Then:

1. The kernel of f is defined as

$$\mathrm{Ker}(f) = f^{-1}(e) = \{x \in G_1 : f(x) = e_2\}$$

2. The image of f is defined as

$$\mathrm{Im}(f) = f(G_1) = \{f(x) \in G_2 : x \in G_1\}$$

Example Let f be the homomorphism given in Example 4.9. Then

$$\mathrm{Ker}(f) = \{x \in \mathbb{R} : f(x) = 1\} = \{x \in \mathbb{R} : 2^x = 1\} = \{0\}$$

and $\mathrm{Im}(f) = \{f(x) : x \in \mathbb{R}\}$. We have $f(x) = y$, which implies $2^x = y$, and this implies $x \ln 2 = \ln y$, so $x = \frac{\ln y}{\ln 2}$. Hence, $\mathrm{Im}(f) = \mathbb{R}_+^*$.

Theorem 4.2 Let f be a homomorphism from $(G_1, *)$ to $(G_2, \perp)$. Then:

1. $\mathrm{Ker}(f)$ is a subgroup of G_1;

2. $\mathrm{Im}(f)$ is a subgroup of G_2;

3. f is injective if and only if $\mathrm{Ker}(f) = \{e_1\}$;

4. f is surjective if and only if $\mathrm{Im}(f) = G_2$.

4.2.1.3 Rings

Definition 4.11 (Ring) Let A be a set equipped with two binary operations, $*$ and $\perp$. $(A, *, \perp)$ is called a ring if:

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

2. $\perp$ is associative;

3. $\perp$ is distributive over $*$.

Remark 4.6

1. If $\perp$ is commutative, then $(A, *, \perp)$ is called a commutative ring.

2. If $\perp$ has a neutral element, then $(A, *, \perp)$ is called a unitary ring.

Example

1. $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are commutative rings;

2. Let E be a set, $(\mathcal{P}(E), \triangle, \cap)$ is a commutative ring;

3. Let A be the set of functions from $\mathbb{C}$ to $\mathbb{C}$ of the form $z \mapsto \alpha z + \beta \bar{z}$. $(A, +, \circ)$ is a non-commutative ring.

Definition 4.12 (Subring) Let $(A, +, \cdot)$ be a ring and B be a subset of A. B is called a subring of $(A, +, \cdot)$ if and only if:

1. $B \neq \emptyset$ $(0_A \in B)$;

2. $(B, +)$ is a subgroup of A;

3. B is closed under $\cdot$.

Alternatively,

1. $0_A \in B$

2. For all $a, b \in B$, $a - b \in B$;

3. For all $a, b \in B$, $a \cdot b \in B$.

Example

1. $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are all subrings of each other;

2. The set $\left\{r + s\sqrt{2} : (r, s) \in \mathbb{Q}^2\right\}$ is a subring of $(\mathbb{R}, +, \times)$.

Definition 4.13 (Ring Homomorphism) Let $(A, +, \cdot)$ and $(B, +, \cdot)$ be two rings. A function f from A to B is called a homomorphism if:

1. $f(1_A) = 1_B$
2. For all $a, b \in A$, $f(a + b) = f(a) + f(b)$;
3. For all $a, b \in A$, $f(a \cdot b) = f(a) \cdot f(b)$.

Remark 4.7 In particular, f is a group homomorphism from $(A, +)$ to $(A, +)$.

Definition 4.14 (Invertible Element) An element of a ring $(A, +, \cdot)$ is called invertible if it has a symmetrical element for the second operation (if it has an inverse for the operation).

Definition 4.15 (Zero Divisor) A non-zero element x of a ring A is a zero divisor if its product with another non-zero element equals zero:

$$\exists y \neq 0 \mid xy = 0 \quad \text{or} \quad yx = 0.$$

Example

1. In $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$, all non-zero elements are invertible;
2. In the set of functions from $\mathbb{R}$ to $\mathbb{R}$, any function f that vanishes is a zero divisor, and the invertible elements are the functions that do not vanish.

4.2.1.4 Ideal in a Ring

Definition 4.16 (Ideal) Let $(A, +, \cdot)$ be a ring. A non-empty subset I of A is called an ideal of A if and only if:

1. I is a subgroup of $(A, +, \cdot)$;
2. For $x \in I$ and $a \in A$, $x \cdot a \in I$ and $a \cdot x \in I$.

Example The set $\mathbb{Z}$ is not an ideal of $(\mathbb{R}, +, \times)$ because $\frac{1}{5} \in \mathbb{R}$ and $3 \in \mathbb{Z}$ while $\frac{3}{5} \notin \mathbb{Z}$.

Remark 4.8 It is easy to verify that:

1. The intersection of ideals of A is an ideal of A.
2. The image of an ideal under a surjective ring homomorphism is an ideal.
3. The kernel of a ring homomorphism is an ideal.

4.2.1.5 Rules of Calculation in a Ring

Let us recall the binomial theorem, which extends from $\mathbb{Z}$ to commutative rings, but also to arbitrary rings.

Proposition 4.6 Let $(A, +, \cdot)$ be a ring, $a, b \in A$ with $a \cdot b = b \cdot a$, and $n \in \mathbb{N}^*$. Then:

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

Proof By induction on $\mathbb{N}$ and using the Pascal's triangle.

Remark 4.9 Let $x, y \in A$ and $n \in \mathbb{N}^*$, then $x - y \mid x^n - y^n$ and more precisely:

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

* A particular case of the above: if $1-x$ is invertible, we can calculate $\sum_{k=0}^{n-1} x^k$ using the formula:

$$1 - x^n = (1-x)\sum_{k=0}^{n-1} x^k.$$

4.2.2 Fields

Definition 4.17 (Field) A field is a commutative ring in which every non-zero element is invertible for the second operation.

Remark 4.10 If the second operation is also commutative, the field $(K, +, \cdot)$ is called a commutative field.

Example

$\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not (2 is not invertible).

Definition 4.18 (Subfield) Let $(K, +, \cdot)$ be a field, a subfield of K is a subset K_1 of K such that $(K_1, +, \cdot)$ is a field, i.e., for all x, y in K_1, we have $x - y \in K_1$ and $xy^{-1} \in K_1$.

Example

1. $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are all subfields of each other;

2. The set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a commutative field that contains $\mathbb{Q}$ as a subfield.

4.3 Solved Exercises

Exercise 1. We define on $\mathbb{R}$ an internal composition law $*$ as follows:

$$\forall a, b \in \mathbb{R} : a * b = \ln\left(e^a + e^b\right)$$

1. Is the law $*$ commutative? Associative? Does it have a neutral element?

2. Let $a, b \in \mathbb{R}$. We define an internal composition law $\perp$ on $\mathbb{R}$ as follows:

$$\forall x, y \in \mathbb{R} : x \perp y = ax + by$$

Determine a, b such that the law $\perp$ is: (1) associative, (2) has a neutral element.

Exercise 2. Let $G = \mathbb{R}^* \times \mathbb{R}$ and $*$ be the internal composition law defined on G as follows:

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

1. Show that $(G, *)$ is a non-commutative group.

2. Show that the set $H = \mathbb{R}_+^* \times \mathbb{R}$ is a subgroup of $(G, *)$.

Exercise 3. Let $\left(\mathbb{R}_+^*, \times\right)$ and $(\mathbb{R}, +)$ be two groups, and let $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ be the function defined as follows:

$$f(x) = \ln(x)$$

1. Show that f is a homomorphism from $\left(\mathbb{R}_+^*, \times\right)$ to $(\mathbb{R}, +)$.

2. Calculate $Ker(f)$. What can you conclude?

3. Is f surjective?

Exercice4. We equip the set $A = \mathbb{Z}^2$ with two operations defined by:

$$(x, y) + (x', y') = (x + x', y + y') \text{ and } (x, y) \star (x', y') = (xx', xy' + x'y)$$

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

2. Show that the operation $\star$ is commutative and associative.

3. Determine the neutral element for the operation $\star$.

4. Show that $(A, +, \star)$ is a commutative unitary ring.

5. Show that $B = \{(a, 0) \mid a \in \mathbb{Z}\}$ is a subring of $(A, +, \star)$.

6. We equip the set $K = \mathbb{R}$ with the usual addition and multiplication.

(a) Why is $(K, +, \cdot)$ a field?

(b) Let $L = \{x \in \mathbb{R}, \exists \alpha, \beta \in \mathbb{Q} \mid x = \alpha + \beta\sqrt{3}\}$ be a subset of $\mathbb{R}$.

Show that $(L, +, .) isasubfieldof$(K,+,.).

Exercice5.

(1) Consider a set E defined by $E = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$ and define on E a composition law $*$ by

$$\forall (a_1, b_1), (a_2, b_2) \in E : (a_1, b_1) * (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1)$$

(a) Verify that $*$ is an internal law on E and find $(2, 0) * (1, 1)$

(b) Show that $(E, *)$ is a non-commutative group.

(c) Determine the set $H = \{(x, y) \in E, \forall (a, b) \in E : (x, y) * (a, b) = (a, b) * (x, y)\}$

(2) Let $F = \{(a, b) \in E : b = 0\}$ be a subset of E.

(a) Show that F is a subgroup of E.

(3) Consider a function f defined by

$$f : (E, *) \longrightarrow (\mathbb{R}^*, .)$$

$$(a, b) \longmapsto f((a, b)) = a$$

(a) Show that f is a group homomorphism from $(E, *)$ to the group $(\mathbb{R}^*, .)$

(b) Determine the kernel of f.

(4) Let $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2}, m, n \in \mathbb{Z}\}$ be a subset of $\mathbb{R}$.

(a) Show that $\mathbb{Z}[\sqrt{2}]$ equipped with addition and multiplication of real numbers is a subring of $\mathbb{R}$.

4.3.1 Solutions

Exercise 1.

(1)

- $\forall a, b \in \mathbb{R},\ b * a = \ln\left(e^b + e^a\right) = \ln\left(e^a + e^b\right) = a * b.$

  Therefore, $*$ is commutative.

- $$\begin{aligned} \forall a, b, c \in \mathbb{R},\ (a * b) * c \quad & \ln\left(e^{a*b} + e^c\right) = \ln\left(e^a + e^b + e^c\right) \\ &= a * (b * c). \end{aligned}$$

  Therefore, $*$ is associative.

- $a * e = a \Leftrightarrow \ln\left(e^a + e^e\right) = a \Leftrightarrow e^e = 0.$

  Thus, there is no neutral element.

(2)

- $\perp$ is associative $\Leftrightarrow \forall x, y, z \in \mathbb{R},\ (x \perp y) \perp z = x \perp (y \perp z).$

  $\Leftrightarrow \forall x, y, z \in \mathbb{R},\ a^2x + aby + bz = ax + aby + b^2z.$

  Therefore, $a^2 = a$ and $ab = ba$ and $b = b^2$.

  Hence, $(a = 0$ or $a = 1)$ and $(b = 0$ or $b = 1)$.

- $\perp$ has a neutral element $e \in \mathbb{R}$ if $\forall x \in \mathbb{R},\ x \perp e = e \perp x = x.$

  $\Leftrightarrow \forall x \in \mathbb{R},\ ax + be = ae + bx = x.$

  $\Leftrightarrow a = 1$ and $e = 0$ and $b = 1$.

Exercise 2.

(1)

- $$\begin{aligned} ((x, y) * (x', y')) * (x'', y'') &= (xx', xy' + y) * (x'', y'') \\ &= (xx'x'', xx''y' + xy'' + y) \text{ and} \end{aligned}$$

  $(x, y) * ((x', y') * (x'', y'')) = (x, y) * (x'x'', x'y'' + y') = (xx'x'', xx''y' + xy'' + y).$

  Thus, $*$ is associative.

- $(x, y) * (1, 0) = (x, y)$ and $(1, 0) * (x, y) = (x, y)$.

  Hence, $(1, 0)$ is the neutral element.

- $(x, y) * \left(\frac{1}{x}, \frac{-y}{x}\right) = (1, 0)$ and $\left(\frac{1}{x}, -\frac{y}{x}\right) * (x, y) = (1, 0)$.

Therefore, every element is symmetrizable. Thus, $(G, *)$ is a group.

- $(1, 2) * (3, 4) = (3, 6)$ and $(3, 4) * (1, 2) = (3, 10)$.

Therefore, the group is not commutative.

(2) $H = \mathbb{R}_+^* \times \mathbb{R}$ is a subset of G.

- $(1, 0) \in H$,
- $\forall (x, y), (x', y') \in H$, $(x, y) * (x', y') \in H$ since $x\bar{x} > 0$,
- $\forall (x, y) \in H$, $(x, y)^{-1} = \left(\frac{1}{x}, \frac{-y}{x}\right) \in H$ since $\frac{1}{x} > 0$.

Therefore, H is a subgroup of G.

Exercise 3.

(1) f is a homomorphism from $\left(\mathbb{R}_+^*, \cdot\right)$ to $(\mathbb{R}, +)$. Let:

$$\begin{aligned} x_1, x_2 \in \mathbb{R}_+^* : f(x_1 \cdot x_2) &= \ln(x_1 \cdot x_2) = \ln x_1 + \ln x_2 \\ &= f(x_1) + f(x_2) \end{aligned}$$

(2)

$$\begin{aligned} \ker(f) &= \left\{x \in \mathbb{R}_+^* : f(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : \ln x = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : e^{\ln(x)} = e^0 = 1\right\} \\ &= \left\{x \in \mathbb{R}_+^* : x = 1\right\} \\ &= \{1\} \end{aligned}$$

Thus, f is injective.

(3) f is surjective because:

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

Exercise 4.

(1) $(*)$