Mohamed Boudiaf University-M'sila
First year in Computer Science

Department of Computer Science
2025-2026

Course of Algebra 1

Chapter 4

Algebraic Structures

4.1 Internal Composition Law (Binary Operation)

4.1.1 Definition and Examples

Definition 1. *Let E be a nonempty set. An* internal composition law *(or binary operation) on E is a mapping*

$$* : E \times E \longrightarrow E$$

which assigns to each ordered pair $(x, y) \in E \times E$ an element $x * y \in E$. The element $x * y$ is called the composition *of x and y under the operation $*$.*

Example 4.1.1.

- ***Addition:*** *Let $E = \mathbb{Z}$. Define addition as follows:*

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a + b$$

This is a law of internal composition on $\mathbb{Z}$.

- ***Subtraction:***

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a - b$$

Subtraction is a law of internal composition on $\mathbb{Z}$.

- ***Multiplication:***

$$\times : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a \times b$$

Multiplication is a law of internal composition on $\mathbb{Z}$.

- ***Division:***

$$\div : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a \div b$$

Division is ***not*** *a law of internal composition on $\mathbb{Z}$, because $a \div b$ is not defined for all pairs $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, especially when $b = 0$ or when the result is not an integer.*

4.1.2 Properties of Internal Composition Laws

Definition 2. *Let $*$ be a law of internal composition on a set E. Then:*

1. ***Commutativity:*** *$*$ is called* commutative *if and only if:*

$$\forall x, y \in E, \quad x * y = y * x.$$

2. ***Associativity:*** $*$ *is called* associative *if and only if:*

$$\forall x, y, z \in E, \quad (x * y) * z = x * (y * z)$$

3. ***Identity Element:*** $*$ *has an* identity element $e \in E$ *if and only if:*

$$\exists e \in E, \quad \forall x \in E, \quad e * x = x * e = x$$

4. ***Inverse Element:*** *If* $*$ *has an identity element* e*, then* $*$ *has an* inverse property *if and only if:*

$$\forall x \in E, \quad \exists x' \in E, \quad x * x' = x' * x = e,$$

an element $x' \in E$ *is called an* inverse *of* $x \in E$*.*

4.2 Groups

Definition 3. *A* group *is a set* E *together with a binary operation* $* : E \times E \to E$ *satisfying the following properties:*

1. ***Associativity:*** $\forall x, y, z \in E, \quad (x * y) * z = x * (y * z)$.
2. ***Identity element:*** *There exists an element* $e \in E$ *such that* $\forall x \in E, \quad e * x = x * e = x$.
3. ***Inverse element:*** *For every* $x \in E$*, there exists* $x' \in E$ *(or equivalently* x^{-1}*) such that* $x * x' = x' * x = e$.

If, in addition, the operation $*$ *is commutative, then* $(E, *)$ *is called a* commutative group *or* abelian group.

Example 4.2.1.

- $(\mathbb{Z}, +)$ *is a commutative group.*
- $(\mathbb{R}_+^*, \times)$ *is a commutative group.*
- $(\mathbb{R}, \times)$ *is not a group, since* 0 *does not admit an inverse element.*

4.2.1 Subgroups

Definition 4. *Let* $(G, *)$ *be a group and let* $H \subseteq G$ *be nonempty. We say that* H *is a* subgroup *of* G *if:*

1. *The identity element* e *of* G *belongs to* H.
2. H *is closed under the operation* $*$*:* $\forall x, y \in H, \quad x * y \in H$.
3. H *is closed under inverses:* $\forall x \in H, \quad x^{-1} \in H$.

Remark 4.2.2. *A practical criterion to check whether* H *is a subgroup of* G *is:*

- H *contains at least one element be the identity element* e.
- $\forall x, y \in H, \quad x * y^{-1} \in H$.

Example 4.2.3. $(\mathbb{R}_+^*, \times)$ *is a subgroup of* $(\mathbb{R}^*, \times)$*. Indeed:*

1. *The identity element* $e = 1$ *belongs to* $\mathbb{R}_+^*$

2. *For all* $x, y \in \mathbb{R}_+^*, \quad x \times y \in \mathbb{R}_+^*$.

3. $\forall x \in \mathbb{R}_+^*, \quad x^{-1} = \frac{1}{x} \in \mathbb{R}_+^*$.

Example 4.2.4. *Let*

$$H = \{\, x \in \mathbb{Z} \mid x = 2n,\ n \in \mathbb{Z} \,\}$$

be the set of even integers. We prove that H *is a subgroup of* $(\mathbb{Z}, +)$ *using the two-condition subgroup test.*

- ***Identity element:*** *In* $(\mathbb{Z}, +)$*, the identity element is* $e = 0$*. Since* $0 = 2 \cdot 0 \in H$*, we have* $e \in H$*.*
- ***Closure under*** $x + y'$***:*** *Let* $x = 2n$ *and* $y = 2m$ *with* $n, m \in \mathbb{Z}$*. The inverse of* y *in* $(\mathbb{Z}, +)$ *is* $y' = -y = -2m$*. Then*

$$x + y' = 2n + (-2m) = 2(n - m).$$

Since $n - m \in \mathbb{Z}$*, it follows that* $x + y' \in H$*.*

Therefore, H *is a subgroup of* $(\mathbb{Z}, +)$*.*

4.2.2 Group Homomorphisms

Definition 5. *Let* $(G_1, *)$ *and* (G_2, Δ) *be two groups. A* homomorphism *(or morphism) from* G_1 *to* G_2 *is a mapping*

$$f : G_1 \longrightarrow G_2$$

such that

$$\forall x, y \in G_1, \quad f(x * y) = f(x)\, \Delta\, f(y).$$

Example 4.2.5. *Define*

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times), \quad \exp(x) = e^x.$$

For all $x, y \in \mathbb{R}$*,*

$$\exp(x + y) = e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

Then exp *is a homomorphism. Thus, is a group homomorphism from* $(\mathbb{R}, +)$ *to* $(\mathbb{R}_+^*, \times)$*.*

Propoerties 4.2.6 Let $(G_1, *)$ and (G_2, Δ) be groups with identity elements e_1 and e_2, respectively, and let $f : G_1 \to G_2$ be a homomorphism. Then:

- f is an *endomorphism* if $G_1 = G_2$
- f is an *isomorphism* if it is bijective.
- f is an *automorphism* if it is an isomorphism and endomorphism.

Proposition 4.2.6. *Let* $(G_1, *)$ *and* (G_2, Δ) *be groups with identity elements* e_1 *and* e_2*. If* $f : G_1 \to G_2$ *is a homomorphism, then:*

1. $f(e_1) = e_2$.
2. $\forall x \in G_1, \quad f(x') = (f(x))'$.
3. *If* H *is a subgroup of* G_1*, then* $f(H)$ *is a subgroup of* G_2*.*
4. *If* L *is a subgroup of* G_2*, then* $f^{-1}(L)$ *is a subgroup of* G_1*.*

4.2.3 Kernel and Image of a Homomorphism

Definition 6 (Kernel of a Homomorphism). *Let $(G_1, *)$ and (G_2, Δ) be groups with identity elements e_1 and e_2. If $f : G_1 \to G_2$ is a homomorphism, the* kernel *of f is defined by*

$$\mathrm{Ker}(f) = f^{-1}(e_2) = \{\, x \in G_1 \mid f(x) = e_2 \,\}.$$

Definition 7 (Image of a Homomorphism). *Let $(G_1, *)$ and (G_2, Δ) be groups with identity elements e_1 and e_2. If $f : G_1 \to G_2$ is a homomorphism, the* image *of f is defined by*

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

Example 4.2.7.

- *Consider the exponential mapping*

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times), \quad \exp(x) = e^x.$$

Kernel:

$$\mathrm{Ker}(\exp) = \{x \in \mathbb{R}, e^x = 1\}.$$

The equation $e^x = 1$ holds only when $x = 0$. Therefore,

$$\mathrm{Ker}(\exp) = \{0\}.$$

Image:

$$\mathrm{Im}(\exp) = \{e^x, x \in \mathbb{R}\}.$$

Since $e^x > 0$ for every real number x, we conclude

$$\mathrm{Im}(\exp) = \mathbb{R}_+^*.$$

- *Consider the logarithm mapping*

$$\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +), \quad \ln(x) = \log(x).$$

Kernel:

$$\mathrm{Ker}(\ln) = \{x \in \mathbb{R}_+^*, \ln(x) = 0\}.$$

The equation $\ln(x) = 0$ holds only when $x = 1$. Therefore,

$$\mathrm{Ker}(\ln) = \{1\}.$$

Image:

$$\mathrm{Im}(\ln) = \{\ln(x), x \in \mathbb{R}_+^*\}.$$

Since $\ln(x)$ can take any real value as x ranges over $\mathbb{R}_+^*$, we obtain

$$\mathrm{Im}(\ln) = \mathbb{R}.$$

Theorem 4.2.8. *Let $f : (G_1, *) \to (G_2, \Delta)$ be a group homomorphism. 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* $\mathrm{Im}(f) = G_2$.

4.3 Rings

Definition 8. *Let A be a set equipped with two binary operations, denoted by $*$ and $\perp$. We say that $(A, *, \perp)$ is a* ring *if the following conditions hold:*

1. *$(A, *)$ is a commutative group.*
2. *Distributivity laws are satisfied:*

$$\forall x, y, z \in A, \quad x\perp(y * z) = (x\perp y) * (x\perp z), \quad (x * y)\perp z = (x\perp z) * (y\perp z).$$

3. *The operation $\perp$ is associative.*

Remark 4.3.1.
- *If $\perp$ is commutative, then $(A, *, \perp)$ is called a* commutative ring.
- *If $\perp$ admits a neutral element, then $(A, *, \perp)$ is called a* unitary ring.

Example 4.3.2. *The structure $(\mathbb{Z}, +, \times)$ is a commutative and unitary ring because:*

- *$(\mathbb{Z}, +)$ is a commutative group.*
- *The distributive laws hold with respect to addition and multiplication.*

Example 4.3.3. *The structure $(\mathbb{Q}, +, \times)$ is a commutative and unitary ring because:*

- *$(\mathbb{Q}, +)$ forms a commutative group.*
- *Multiplication in $\mathbb{Q}$ is associative and commutative.*
- *The distributive laws hold:*

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z), \quad (x + y) \cdot z = (x \cdot z) + (y \cdot z), \quad \forall x, y, z \in \mathbb{Q}.$$

- *The multiplicative identity is $1 \in \mathbb{Q}$, so the ring is unitary.*

4.4 Fields

Definition 9. *Let E be a set equipped with two binary operations, denoted by $+$ and $\cdot$. We say that $(E, +, \cdot)$ is a* field *if:*

1. *$(E, +, \cdot)$ is a ring with unity (i.e., a unitary ring).*
2. *Every element $x \in E$ with $x \neq 0$ admits a multiplicative inverse x', that is*

$$\forall x \in E,\ x \neq 0 \quad \exists x' \in E \quad \text{such that } x \cdot x' = 1,$$

where 1 is the multiplicative identity.

Remark 4.4.1. *Since multiplication in a field is always commutative, the term* commutative field *is redundant. Thus, by convention, all fields are commutative under multiplication.*

Example 4.4.2. 1. *The structures $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are commutative fields.*

- *$(\mathbb{R}, +, \times)$ is a commutative ring with unity.*

- *For every $x \in \mathbb{R}$ with $x \neq 0$, there exists an inverse under multiplication, namely*

$$x^{-1} = \frac{1}{x} \in \mathbb{R}.$$

- *Hence, $(\mathbb{R}, +, \times)$ satisfies all the axioms of a field.*

2. *The structure $(\mathbb{Z}, +, \times)$ is not a field:*

   - *Although $(\mathbb{Z}, +, \times)$ is a commutative ring with unity,*
   - *not every nonzero integer has a multiplicative inverse in $\mathbb{Z}$. For example, $2 \in \mathbb{Z}$ has no inverse in $\mathbb{Z}$, since $\frac{1}{2} \notin \mathbb{Z}$.*
   - *Therefore, $(\mathbb{Z}, +, \times)$ fails the field property.*