Lecture 6
ALGEBRAIC STRUCTURES

ENSIA 2023/2024

OUTLINE

- Binary operations
- Groups
- Subgroups
- Group homomorphisms
- Rings
- Ideals
- Fields

BINARY OPERATIONS

Definition

A **binary operation** on a set G is a function $f: G \times G \rightarrow G$.

The image $f(x, y)$ of $(x, y) \in G \times G$ will be denoted by

$$x * y, x \circ y, x \perp y, \ldots, \text{etc.}$$

Therefore, we can talk about operations $*, \circ, \perp, \ldots$, etc.

Example

The addition $+$ is a binary operation on $\mathbb{N}$.

The soustraction $-$ is a binary operation on $\mathbb{Z}$, but not on $\mathbb{N}$.

ASSOCIATIVITY AND COMMUTATIVITY

Definition

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

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

It is said to be **commutative** if

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

Example

The addition $+$ on $\mathbb{R}$ is associative and commutative.

The operation $*$ defined on $\mathbb{R}$ by $x * y = x^2 + y^2$ is commutative, but not associative.

The operation $*$ defined on $\mathbb{R}$ by $x * y = x$ is associative, but not commutative.

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

IDENTITY ELEMENT

Definition

An **identity element** (or a **neutral element**) for a binary operation $*$ on a set G is an element $e \in G$ verifying :

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

Example

- For the operation $+$ defined on $\mathbb{N}$, 0 is the identity element.
- For the operation $\times$ defined on $\mathbb{N}$, 1 is the identity element.
- The three last operations defined in Example 2 do not have identity elements.

INVERSE ELEMENT

Definition

Let G be a set equipped with a binary operation $*$ that admits an identity element e. We say that an element $x \in G$ is **invertible** if there exists an element $y \in G$ such that :

$$x * y = y * x = e.$$

We say then that y is the **inverse** of x.

Remark

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

However, for the sake of brevity, we also often use the notation x^{-1} in an arbitrary group.

INVERSE ELEMENTS EXAMPLES

Example

For the operation $+$ defined on $\mathbb{Z}$, the inverse of x is $-x$.

If we consider the same operation on $\mathbb{N}$, the inverse of $x \neq 0$ doesn't exist.

GROUPS

Definition

A group is a set G equipped with a binary operation $*$ verifying :

1) The operation $*$ is associative.

2) The operation $*$ admits an identity element.

3) Every element of G is invertible.

Notation : A group G with a binary operation $*$ is denoted by $(G,*)$. When there is no ambiguity, it is denoted simply by G.

ABELIAN GROUP, EXAMPLES

Definition

A group $(G,*)$ is commutative (or abelian) if the operation $*$ is commutative.

Example

1) $(\mathbb{Z},+), (\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$ are commutative groups.
2) $(\mathbb{N},+)$ and $(\mathbb{Z}, \times)$ are not groups.
3) Let G be the set of bijective functions from $\mathbb{R}$ to $\mathbb{R}$, and let $\circ$ be the operation of composition of functions. Then $(G, \circ)$ is a noncommutative group.

EXAMPLES FROM MODULAR ARITHMETIC

Example

Let $G = \mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of integers modulo 5. Set

$$\forall\ \bar{x}, \bar{y} \in G, \bar{x} \oplus \bar{y} = \overline{x + y}.$$

This operation is *well defined*, and $(G,\ \oplus)$ is an abelian group.

Now, consider $G' = G \backslash \{\bar{0}\}$, and set

$$\forall\ \bar{x}, \bar{y} \in G', \bar{x} \otimes \bar{y} = \overline{xy}.$$

Once again, this operation is well defined, and $(G',\ \otimes)$ is an abelian group.

PROPERTIES

Theorem

Let $(G,*)$ be a group. Then we have

1) The identity element is unique.
2) For all $a, b, x \in G$, we have the **cancellation laws**

$$a * x = b * x \Rightarrow a = b,$$

and

$$x * a = x * b \Rightarrow a = b.$$

3) For all $x \in G$, the inverse of x is unique.

4) For all $x \in G$, the inverse of x^{-1} is x.

5) For all $x, y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1}$.

SUBGROUPS

Definition

Let $(G,*)$ be a group. A **subgroup** of G is a subset $H \subseteq G$ that satisfies the following :

1) $e \in H$.
2) $\forall x, y \in H,\ x * y \in H$.
3) $\forall x \in H, x^{-1} \in H$.

Remark

A subgroup is a group under the induced binary operation, with the same identity element.

SUBGROUPS

Theorem

Let $(G,*)$ be a group, and let $H \subseteq G$. Then H is a subgroup of G if, and only if we have the following :

1) $e \in H$.
2) $\forall x, y \in H,\ x * y^{-1} \in H$.

Example

1) $(\mathbb{Z}, +), (\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are subgroups of $(\mathbb{C}, +)$.
2) $(]0, +\infty[, \times)$ is a subgroup of $(\mathbb{R}^*, \times)$.

INTERSECTION OF SUBGROUPS

Theorem

Let G be a group, and let H and K be two subgroups of G. Then $H \cap K$ is a subgroup of G.

GROUP HOMOMORPHISMS

Definition

Let $(G,*)$ and $(G',\perp)$ be two groups. A function $f: G \to G'$ is said to be a **group homomorphism** if

$$\text{For all } x, y \in G, f(x * y) = f(x) \perp f(y).$$

A homomorphism which is bijective is called an **isomorphism.** Two groups are **isomorphic** if there exists an isomorphism between them. A homomorphism from a group to itself is called an **endomorphism**. When the endomorphism is bijective, it is called an **automorphism**.

EXAMPLE OF HOMOMORPHISM

Example

The function $f: \mathbb{R} \to]0, +\infty[$ defined by $f(x) = e^x$ is an isomorphism from the group $(\mathbb{R}, +)$ to the group $(]0, +\infty[, \times)$.

Indeed, we have

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

Then f is a group homomorphism. Furthermore, for all $y \in]0, +\infty[$, there exists a unique $x = lny \in \mathbb{R}$ such that $y = f(x)$. This shows that f is bijective and completes the proof.

PROPERTIES OF HOMOMORPHISMS

Theorem

Let $(G,*)$ and $(G',\perp)$ be two groups with respective identity elements e and e', and let $f: G \to G'$ be a group homomorphism. Then we have :

1) $f(e) = e'$.
2) For all $x \in G, f(x^{-1}) = (f(x))^{-1}$.

IMAGE AND KERNEL OF HOMOMORPHISMS

Definition

Let $f: G \to G'$ be a group homomorphism. We define the **image** of f by

$$Im(f) = \{y \in G' \colon \exists x \in G \text{ such that } y = f(x)\},$$

and we define the **kernel** of f by

$$Ker(f) = \{x \in G : f(x) = e'\}.$$

OTHER PROPERTIES OF HOMOMORPHISMS

Theorem

Let $f: G \to G'$ be a group homomorphism. Then we have :

1) The image of f, $Im(f)$, is a subgroup of G'.
2) The kernel of f, $Ker(f)$, is a subgroup of G.
3) The homomorphism f is injective if, and only if, $Ker(f) = \{e\}$.

RINGS

Definition

Let R be a nonempty set endowed with two binary operations denoted by $+$ (addition) and $\cdot$ (multiplication) that satisfy the following :

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

2) The multiplication is associative and admits an identity element.

3) The multiplication is distributive with respect to addition, that is

$$\forall a, b, c \in R, (a + b) \cdot c = a \cdot c + b \cdot c \text{ and } c \cdot (a + b) = c \cdot a + c \cdot b.$$

Then $(R, +, \ \cdot)$ is called a **ring.**

A ring R is called a **commutative ring** when the multiplication is commutative.

RINGS EXAMPLES

Example

$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$ are commutative rings with usual operations of addition and multiplication.

Let $R = \{f : \mathbb{R} \to \mathbb{R}\}$, and define for all $f, g \in R$:

$$(f+g)(x) = f(x) + g(x), \forall x \in \mathbb{R},$$
$$(f.g)(x) = f(x)g(x), \forall x \in \mathbb{R}.$$

Then $(R,+,\cdot)$ is a commutative ring.

NOTATION

Notation

For brevity, when there is no ambiguity, we denote

$$R \coloneqq (R,+,\ \cdot)$$
$$ab \coloneqq a \cdot b$$
$$a - b \coloneqq a + (-b).$$

NOTATION

Notation

By associativity, the following notations make sense :

$$a^n := \begin{cases} a \cdot a \cdots a \ (n \, times) & if \ n > 0 \\ 1 & if \ n = 0 \\ a^{-1} \cdot a^{-1} \cdots a^{-1} \ \ (-n \, times) & if \ n < 0 \end{cases}$$

$$na := \begin{cases} a + a + \cdots + a \ (n \, times) & if \ n > 0 \\ 0 & if \ n = 0 \\ (-a) + (-a) + \cdots + (-a) \ \ (-n \, times) & if \ n < 0 \end{cases}$$

THE RING $\mathbb{Z}/n\mathbb{Z}$

Let n be a positive integer. Recall that the relation $\mathcal{R}$ defined on $\mathbb{Z}$ by

$$\forall x, y \in \mathbb{Z}, \qquad x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z}, x - y = nk,$$

is an equivalence relation, and the quotient set is given by :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}.$$

We define the two binary operations :

$$\forall\ \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}, \bar{x} \oplus \bar{y} = \overline{x+y} \text{ and } \bar{x} \otimes \bar{y} = \overline{xy}.$$

Theorem

$(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ is a commutative ring.

INTEGRAL DOMAINS

Definition

Let R be a ring and let $a \in R\backslash\{0\}$. If there exists $b \in R\backslash\{0\}$ such that $ab = 0$ or $ba = 0$, then a is said to be a **zero-divisor**.

Definition

An **integral domain** is a commutative ring without zero-divisor.

In other words, a commutative ring R is an integral domain if, and only if,

$$\forall a, b \in R, ab = 0 \Rightarrow a = 0 \; or \; b = 0.$$

Example

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are integral domains.

The ring $\mathbb{Z}/6\mathbb{Z}$ is **not** an integral domain since we have

$$\bar{2} \otimes \bar{3} = \bar{6} = \bar{0}.$$

ELEMENTARY PROPERTIES

Theorem

Let R be a ring, a, b and c three elements in R and $n \in \mathbb{Z}$. Then we have the following properties :

1) $a \cdot 0 = 0 \cdot a = 0.$
2) $If\ card(R) > 1$, *then* $0 \neq 1.$
3) $(-a)b = a(-b) = -(ab).$
4) $(-1)a = -a$ and $(-a)(-b) = ab.$
5) $a(b - c) = ab - ac$ and $(b - c)a = ba - ca.$
6) $(na)b = a(nb) = n(ab).$

BINOMIAL FORMULA

Theorem

Let R be a ring. If a and b are elements in R which commute $(ab = ba)$, then we have for all $n \in \mathbb{N}$:

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

UNITS OF A RING

Definition

Let R be a ring. An element $a \in R$ is said to be **invertible**, or a **unit**, if there exists $b \in R$ such that $ab = ba = 1$.

The set of units in R is denoted by $U(R)$.

Theorem

The set of units $U(R)$ forms a group under multiplication.

Example

$U(\mathbb{Z}) = \{1, -1\}$.

$U(\mathbb{Z}/8\mathbb{Z}) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

SUBRINGS

Definition

Let $(R, +, \ \cdot)$ a ring. A subset S of R is a **subring** of $(R, +, \ \cdot)$ if we have :

1) $1 \in S$.
2) $(S, +)$ is a subgroup of $(R, +)$.
3) S is closed under multiplication : $\forall a, b \in S, ab \in S$.

SUBRINGS EXAMPLES

Example

1) $\mathbb{Z}$ is the only subring of $\mathbb{Z}$.

2) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$ …

3) $\mathbb{Z}[i] \coloneqq \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ is a subring of $\mathbb{C}$. It's called the ring of **Gaussian integers.**

RING HOMOMORPHISMS

Definition

Let R and R' be two rings. A function $f: R \to R'$ is said to be a **ring homomorphism** if it satisfies the following :

1) $f(1) = 1'$.
2) $\forall x, y \in R, f(x + y) = f(x) + f(y)$.
3) $\forall x, y \in R, f(xy) = f(x)f(y)$.

Isomorphisms, endomorphisms and automorphisms are defined similarly to those of groups.

PROPERTIES OF RING HOMOMORPHISMS

Theorem

Let $f: R \to R'$ be a ring homomorphism. Then we have :

1) $f(0) = 0'$.
2) $f(na) = nf(a), \forall a \in R, \forall n \in \mathbb{Z}$.
3) $f(a^n) = f(a)^n, \forall a \in R, \forall n \in \mathbb{N}$.
4) $f(a^n) = f(a)^n, \forall a \in U(R), \forall n \in \mathbb{Z}$.
5) $f(A)$ is a subring of R', for all subring A of R.
6) $f^{-1}(B)$ is a subring of R, for all subring B of R'.

IDEALS

Definition

Let R be a *commutative* ring. A subset I of R is said to be an **ideal** of R if it satisfies the two following conditions :

1) $(I,+)$ is a subgroup of $(R,+)$.

2) $\forall a \in R, \forall x \in I, ax \in I$.

Example

For all $n \in \mathbb{Z}, n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

QUOTIENT RING

Let R be a commutative ring, and let I be an ideal of R. The relation $\mathcal{R}$ defined on R by

$$\forall x, y \in R, \qquad x\mathcal{R}y \Leftrightarrow x - y \in I,$$

is an equivalence relation. The quotient set will be denoted by R/I.

We define on A/I the two binary operations :

$$\forall\ \bar{x}, \bar{y} \in A/I, \bar{x} + \bar{y} = \overline{x+y} \text{ and } \bar{x} \cdot \bar{y} = \overline{xy}.$$

Theorem

R/I is a commutative ring under the operations defined above. It is called the **quotient ring.**

FIELDS

Definition

A **field** is a commutative ring in which every nonzero element is invertible.

A **subfield** of a field is a subring which is itself a field.

Example

$\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, endowed with usual operations, are fields.

$\mathbb{Z}$ is **not** a field.

THE FIELD $\mathbb{Z}/p\mathbb{Z}$, p PRIME

Theorem

The ring $\mathbb{Z}/p\mathbb{Z}$ is a field if, and only if, p is prime.

Theorem

Let $a, b \in \mathbb{Z}/p\mathbb{Z}$, where p is prime, and let $k \in \mathbb{N}$. Then we have

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}.$$