COURSE 1

Rings and fields

internal operation

Definition 1. By a **binary operation** on a set A we understand a map

$$\varphi : \boxed{A \times A} \to A. \quad , (x,y) \in A \times A \longmapsto \varphi(x,y)$$

Since all the operations considered in this section are binary operations, we briefly call them **operations**. Usually, we denote operations by symbols like $*$, $\cdot$, $+$, and the image of an arbitrary pair $(x, y) \in A \times A$ is denoted by $x * y$, $x \cdot y$ (multiplicative notation), $x + y$ (additive notation), respectively.

Examples 2. a) The usual addition and multiplication are operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but not on the set of irrational numbers. $(\mathbb{R} \setminus \mathbb{Q})$
b) The usual subtraction is an operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, but not on $\mathbb{N}$.
c) The usual division is an operation on $\mathbb{Q}^*, \mathbb{R}^*$, $\mathbb{C}^*$, but not on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^*$ or $\mathbb{Z}^*$.

Definitions 3. Let $*$ be an operation on A. We say that: $*: A \times A \to A$
i) $*$ is **associative** if

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3), \ \forall a_1, a_2, a_3 \in A;$$

ii) $*$ is **commutative** if

$$a_1 * a_2 = a_2 * a_1, \ \forall a_1, a_2 \in A.$$

iii) $e \in A$ is an **identity element** for $*$ if

$$a * e = e * a = a, \ \forall a \in A.$$

When using the multiplicative or additive notation, an identity element e is usually denoted by 1 or 0, respectively.

Definition 4. Let A be set and let $\cdot$ be an operation with an identity element 1. An element $a \in A$ **has an inverse** if there exists an element $a' \in A$ such that

$$a \cdot a' = a' \cdot a = 1.$$

We say that a' is an **inverse** for a.

When using the multiplicative notation, the inverse of a is denoted by a^{-1}. When using the or additive notation the inverse of a is denoted by $-a$, and it is called **the opposite of** a.

Definitions 5. A pair $\boxed{(A, *)}$ is called **monoid** if $*$ is associative and it has an **identity element**. A monoid with a commutative operation is called **commutative monoid**.

Definition 6. A pair $\boxed{(A, \cdot)}$ is called **group** if it is a monoid in which every element has an inverse. If the operation is commutative as well, the structure is called **commutative** or **Abelian group**.

Examples 7. a) $(\mathbb{N}, +)$ and $(\mathbb{Z}, \cdot)$ are commutative monoids, but they are not groups.
b) $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are commutative monoids, but they are not groups since 0 has no inverse.
c) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are Abelian groups.

Remark 8. The group definition can be rewritten: $(A, \cdot)$ is a **group** if and only if it follows the following conditions:

(i) $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3),\ \forall a_1, a_2, a_3 \in A$ ($\cdot$ is associative);

(ii) $\exists 1 \in A,\ \forall a \in A:\ a \cdot 1 = 1 \cdot a = a$ (there exists an identity element for $\cdot$);

(iii) $\forall a \in A,\ \exists a^{-1} \in A:\ a \cdot a^{-1} = a^{-1} \cdot a = 1$ (all the elements of A have inverses).

Definitions 9. Let φ be an operation on the set A and $B \subseteq A$. We say that B **is closed under** φ if

(B is closed in (B, φ))

$$b_1, b_2 \in B \Rightarrow \varphi(b_1, b_2) \in B.$$

$\boxed{\varphi': B \times B \to B}$

If B is closed under φ, one can define an operation on B as follows:

$$\varphi' : B \times B \to B,\ \varphi'(b_1, b_2) = \varphi(b_1, b_2).$$

$\varphi'(x, y) = \varphi(x, y)$

We call φ' the **operation induced** by φ on B or, briefly, the **induced operation**. Most of the time, we denote it also by φ.

Remarks 10. a) Let φ be an operation on the set A, $B \subseteq A$ closed under φ and let φ' be the induced operation on B. If φ is associative or commutative, then φ' is associative or commutative, respectively.

b) Let φ_1 and φ_2 be operations on A, let $B \subseteq A$ be closed under φ_1 and φ_2, and let φ_1' and φ_2' be the operations induced by φ_1 and φ_2 on B, respectively. If φ_1 is distributive with respect to φ_2, i.e.

$$\varphi_1(a_1, \varphi_2(a_2, a_3)) = \varphi_2(\varphi_1(a_1, a_2), \varphi_1(a_1, a_3)), \forall a_1, a_2, a_3 \in A,$$

then φ_1' is distributive with respect to φ_2'.

c) The existence of an identity element is not always preserved by induced operations. For instance, $\mathbb{N}^*$ is closed in $(\mathbb{N}, +)$, but $(\mathbb{N}^*, +)$ has no identity element.

Definition 11. Let $(G, \cdot)$ be a group. A subset $H \subseteq G$ is called a **subgroup of** G if:

i) H is closed under the operation of $(G, \cdot)$, that is,

$$\forall x, y \in H\,, \quad x \cdot y \in H\,;$$

ind. op.

ii) H is a group with respect to the induced operation. $(H, \cdot)$ group

Examples 12. a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$, $\mathbb{Z}$, $\mathbb{Q}$ are subgroups of $(\mathbb{R}, +)$ and $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.

b) $\mathbb{Q}^*$, $\mathbb{R}^*$ are subgroups of $(\mathbb{C}^*, \cdot)$ and $\mathbb{Q}^*$ is a subgroup of $(\mathbb{R}^*, \cdot)$.

c) $\mathbb{N}$ is closed in $(\mathbb{Z}, +)$, but it is not a subgroup.

d) Every non-trivial group $(G, \cdot)$ has two subgroups, namely $\{1\}$ and G. Any other subgroup of $(G, \cdot)$ is called **proper subgroup**.

Definition 13. Let $(G, *)$, $(G', \perp)$ be two groups. A map $f : G \to G'$ is called **homomorphism** (or **morphism**) if

$$f(x_1 * x_2) = f(x_1) \perp f(x_2),\ \forall\, x_1, x_2 \in G.$$

A bijective homomorphism is called **isomorphism**. A homomorphism of $(G, *)$ into itself is called **endomorphism** of $(G, *)$. An isomorphism al lui $(G, *)$into itself is called **automorphism** of $(G, *)$. If there exists an isomorphism $f : G \to G'$, we say that the groups $(G, *)$ and $(G', \perp)$ are isomorphic and we denote this by $G \simeq G'$ or $(G, *) \simeq (G', \perp)$.

Let us come back to the multiplicative notation.

Theorem 14. Let $(G, \cdot)$ and $(G', \cdot)$ be groups, and let 1 and $1'$, respectively, be the identity element of $(G, \cdot)$ and $(G', \cdot)$, respectively. If $f : G \to G'$ is a group homomorphism, then:

(i) $f(1) = 1'$;

(ii) $[f(x)]^{-1} = f(x^{-1})$, $\forall x \in G$.

Proof. (i) $\forall x \in G$

$x = 1 \cdot x \Rightarrow f(x) = f(1 \cdot x) = f(1) \cdot f(x) / \cdot [f(x)]^{-1} \Rightarrow 1' = f(1)$

(ii) Let $x \in G$

$$\left.\begin{array}{l} f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1) = 1' \\ f(x^{-1}) \cdot f(x) = f(x^{-1} \cdot x) = f(1) = 1' \end{array}\right\} \Rightarrow f(x^{-1}) = [f(x)]^{-1}$$

Remark: In a group, each element has a unique inverse.

proof: Let $(G, \cdot)$ be a group, $x \in G$ and x', x'' inverses of x in $(G, \cdot)$

$x' = x' \cdot 1 = x' \cdot (x \cdot x'') = (x' \cdot x) \cdot x'' = 1 \cdot x'' = x''$.

comm. ring = ring with $\cdot$ "comm.

□

Definition 15. Let R be a set. A structure $(R, +, \cdot)$ with two operations is called:

(1) **ring** if $(R, +)$ is an Abelian group, $\cdot$ is associative and the distributive laws hold (that is, $\cdot$ is distributive with respect to $+$).

(2) **unitary ring** if $(R, +, \cdot)$ is a ring and there exists a multiplicative identity element. (high-school rings)

"unital

Definition 16. Let $(R, +, \cdot)$ be e unital ring. An element $x \in R$ which has an inverse $x^{-1} \in R$ is called **unit**. The ring $(R, +, \cdot)$ is called **division ring** if it is a unitary ring, $|R| \geq 2$ and any $x \in R^*$ is a unit. A commutative division ring is called **field**. corp

"$R \setminus \{0\}$

Definition 17. Let $(R, +, \cdot)$ be a ring. An element $x \in R^*$ is called **zero divisor** if there exists $y \in R^*$ such that

$$x \cdot y = 0 \text{ or } y \cdot x = 0.$$

We say that R is an **integral domain** if $R \neq \{0\}$, R is unitary, commutative and has no zero divisors.

Remarks 18. (1) Notice that $x \in R^*$ is not a zero divisor iff

$$y \in R\,,\ x \cdot y = 0 \text{ or } y \cdot x = 0\ \Rightarrow\ y = 0\,.$$

(2) A ring R has no zero divisors if and only if

$$x, y \in R\,,\ x \cdot y = 0 \Rightarrow x = 0 \text{ or } y = 0\,.$$ ($x \neq 0$ and $y \neq 0 \Rightarrow xy \neq 0$)

(3) $(R, +, \cdot)$ is a division ring if and only if it satisfies the following conditions:
i) $(R, +)$ is an Abelian group;
ii) R^* is closed in $(R, \cdot)$ and $(R^*, \cdot)$ is a group;
iii) $\cdot$ is distributive with respect to $+$.
(4) The fields have no zero divisors. Moreover, every field is an integral domain.

Examples 19. (a) $(\mathbb{Z}, +, \cdot)$ is an integral domain, but it is not a field. Its units are -1 and 1.
(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields.
(c) Let $\{0\}$ be a single element set and let both $+$ and $\cdot$ be the only operation on $\{0\}$, defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$. Then $(\{0\}, +, \cdot)$ is a commutative unitary ring, called the **trivial ring** (or **zero ring**). The multiplicative identity element is, of course, 0, hence we can write $1 = 0$. As matter of fact, this equality characterize the trivial ring.

COURSE 2

(d) Let $n \in \mathbb{N}$, $n \geq 2$. Let us remind **the Division Algorithm in** $\mathbb{Z}$: *For any integers a and b, with $b \neq 0$, there exists only one pair $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that*

$$a = b \cdot q + r \textit{ and } 0 \leq r < |b|.$$

The Division Algorithm gives us a partition of $\mathbb{Z}$ in classes determined by the remainders one can find when dividing by n :

$$\{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\},$$

where $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$ $(r \in \mathbb{Z})$. We use the following notations

$$\widehat{r} = r + n\mathbb{Z}\ (r \in \mathbb{Z}) \text{ şi } \mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\} = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}.$$

Let us notice that for $a, r \in \mathbb{Z}$,

$$\widehat{a} = \widehat{r} \Leftrightarrow a + n\mathbb{Z} = r + n\mathbb{Z} \Leftrightarrow a - r \in n\mathbb{Z} \Leftrightarrow n | a - r.$$

The operations

$$\widehat{a} + \widehat{b} = \widehat{a + b},\ \ \widehat{a}\,\widehat{b} = \widehat{ab}$$

are well defined, i.e. if one considers another representatives a' and b' for the classes $\widehat{a}$ and $\widehat{b}$, respectively, the operations provide us with the same results. Indeed, from $a' \in \widehat{a}$ şi $b' \in \widehat{b}$ it follows that

$$n | a' - a,\ n | b' - b \Rightarrow n | a' - a + b' - b \Rightarrow n | (a' + b') - (a + b) \Rightarrow \widehat{a' + b'} = \widehat{a + b}$$

and

$$a' = a + nk,\ b' = b + nl\ (k, l \in \mathbb{Z}) \Rightarrow a'b' = ab + n(al + bk + nkl) \in ab + n\mathbb{Z} \Rightarrow \widehat{a'b'} = \widehat{ab}.$$

One can easily check that the operations $+$ and $\cdot$ are associative and commutative, $+$ has $\widehat{0}$ as identity element, each class $\widehat{a}$ has an opposite in $(\mathbb{Z}_n, +)$, $-\widehat{a} = \widehat{-a} = \widehat{n-a}$, $\cdot$ has $\widehat{1}$ as identity element and $\cdot$ is distributive with respect to $+$. Thus, $(\mathbb{Z}_n, +, \cdot)$ is a unitary ring, called $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, called the **residue-class ring modulo** n.

Since $\widehat{2} \cdot \widehat{3} = \widehat{0}$, both $\widehat{2}$ and $\widehat{3}$ are zero divisors in the ring $(\mathbb{Z}_6, +, \cdot)$. Thus $(\mathbb{Z}_n, +, \cdot)$ is not a field in the general case. Actually, $\widehat{a} \in \mathbb{Z}_n$ is a unit if and only if $(a, n) = 1$. Thus $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is a prime number.

Remark 20. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a group and $\cdot$ is associative, so that we may talk about multiples and positive powers of elements of R.

Definition 21. Let $(R, +, \cdot)$ be a ring, let $x \in R$ and let $n \in \mathbb{N}^*$. Then we define

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ terms}}, \ 0 \cdot x = 0\,, \ (-n) \cdot x = -n \cdot x\,,$$

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ factors}}.$$

If R is a unitary ring, then we may also consider $x^0 = 1$. If R is a division ring, then we may also define negative powers of nonzero elements x by

$$x^{-n} = (x^{-1})^n\,.$$

Remark 22. Notice that in the definition $0 \cdot x = 0$, the first 0 is the integer zero and the second 0 is the zero element of the ring R, i.e., the identity element of the additive group $(R, +)$.

Theorem 23. Let $(R, +, \cdot)$ be a ring and let $x, y, z \in R$. Then:
(i) $x \cdot (y - z) = x \cdot y - x \cdot z$, $(y - z) \cdot x = y \cdot x - z \cdot x$;
(ii) $x \cdot 0 = 0 \cdot x = 0$;
(iii) $x \cdot (-y) = (-x) \cdot y = -x \cdot y$.

Proof.

□

Definition 24. Let $(R, +, \cdot)$ be a ring and $A \subseteq R$. Then A is a **subring of** R if:
(1) A is closed under the operations of $(R, +, \cdot)$, that is,

$$\forall x, y \in A\,,\ x + y\,,\ x \cdot y \in A\,;$$

(2) $(A, +, \cdot)$ is a ring.

Remarks 25. (a) If $(R, +, \cdot)$ is a ring and $A \subseteq R$, then A is a subring of R if and only if A is a subgroup of $(R, +)$ and A is closed in $(R, \cdot)$.

This follows directly from subring definition and Remark 10 b).

(b) A ring R may have subrings with or without (multiplicative) identity, as we will see in a forthcoming example.

Definition 26. Let $(K, +, \cdot)$ be a field and let $A \subseteq K$. Then A is called a **subfield of** K if:
(1) A is closed under the operations of $(K, +, \cdot)$, that is,

$$\forall x, y \in K\,,\ x + y\,,\ x \cdot y \in K\,;$$

(2) $(A, +, \cdot)$ is a field.

Remarks 27. (a) From (2) it follows that for a subfield A, we have $|A| \geq 2$.
(b) If $(K, +, \cdot)$ is a field and $A \subseteq K$, then A is a subfield if and only if A is a subgroup of $(K, +)$ and A^* is a subgroup of $(K^*, \cdot)$.
(c) f $(K, +, \cdot)$ is a field and $A \subseteq K$, then A is a subfield if and only if A is a subring of $(K, +, \cdot)$, $|A| \geq 2$ and for any $a \in A^*$, $a^{-1} \in A$.

Examples 28. (a) Every non-trivial ring $(R, +, \cdot)$ has two subrings, namely $\{0\}$ and R, called the **trivial subrings**.
(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$, $\mathbb{Q}$ is a subfield of $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$, $\mathbb{R}$ is a subfield of $(\mathbb{C}, +, \cdot)$.
(c) If K is a field, then $\{0\}$ is a subring of K which is not a subfield.