COURSE 1

Groups, rings and fields

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

$$\varphi : A \times A \to A\,.$$

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.
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:
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

$$a \cdot a' = a' \cdot a = e.$$

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 $(A, *)$ 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 $(A, \cdot)$ 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

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

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

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

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,

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

ii) H is a group with respect to the induced operation.

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.

$\square$