

Definition 3.1

A *group* is set G equipped with an operation that assigns to each pair of elements $a, b \in G$ an element $a \cdot b \in G$ in such way, that the following conditions are satisfied:

- 1) For any $a, b, c \in G$ we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(associativity).

- 2) There exists an element $e \in G$ such that

$$e \cdot a = a \cdot e = a$$

for all $a \in G$. The element e is called the *identity element* or the *trivial element*.

- 3) For each element $a \in G$ there exists an element $b \in G$ such that

$$a \cdot b = b \cdot a = e$$

Such element b is called the *inverse* of a and it is denoted by a^{-1} .

Note. The first condition in the definition of a group implies that if we want to multiply several elements, then it does not matter how we place parentheses. E.g.:

$$((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d) = (a(bc))d$$

Definition 3.2

A *abelian group* is a group G where the multiplication is commutative:

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

Notation

Multiplicative:

- $a \cdot b, a \times b, a * b, a \circ b, a \odot b, \dots$
- Inverse element: a^{-1} .
- The identity element: $e, 1, \dots$

Additive:

- $a + b$
- Inverse element: $-a$.
- The identity element: 0 .

Note: The additive notation is only used for abelian groups.

Some examples of groups

- \mathbb{Z} – the group of integers (with addition)
- \mathbb{Q} – the group of rational numbers (with addition)
- \mathbb{R} – the group of real numbers (with addition)
- \mathbb{C} – the group of complex numbers (with addition)
- \mathbb{Q}^* – the group of non-zero rational numbers (with multiplication)
- \mathbb{R}^* – the group of non-zero real numbers (with multiplication)
- \mathbb{C}^* – the group of non-zero complex numbers (with multiplication)
- \mathbb{Q}^+ – the group of positive rational numbers (with multiplication)
- \mathbb{R}^+ – the group of positive real numbers (with multiplication)
- The trivial group $\{e\}$.

Example: General linear groups $GL(n, \mathbb{R})$.

- Elements of $GL(n, \mathbb{R})$: invertible $n \times n$ matrices with real entries.

- **Group operation:** matrix multiplication.
- **The identity element:** the identity matrix I_n .

Example: Groups \mathbb{Z}_n

Notation: Let $n > 0$ be an integer. For any integer m we have

$$m = qn + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then we write

$$m \bmod n = r$$

For an integer $n \geq 2$ the group \mathbb{Z}_n is defined as follows:

- **Elements of \mathbb{Z}_n :** numbers $0, 1, \dots, n-1$
- **Group operation \oplus :** For $k, l \in \mathbb{Z}_n$ we set

$$k \oplus l := (k + l) \bmod n$$

- **The identity element:** 0.
- **Inverses:** The inverse of an element $k \in \mathbb{Z}_n$ is the element $n - k$.

Example: Groups $U(n)$

Recall:

- If m, n are integers then $\gcd(m, n)$, is the greatest integer that divides both m and n .
- For any $m, n \neq 0$ there exists $a, b \in \mathbb{Z}$ such that

$$am + bn = \gcd(m, n)$$

Moreover, $\gcd(m, n)$ is the smallest positive integer that can be obtained for any choice of a and b .

For an integer $n \geq 2$ the group $U(n)$ is defined as follows:

- **Elements of $U(n)$:** integers $1 \leq k < n$ such that $\gcd(k, n) = 1$
- **Group operation \odot :** For $k, l \in U(n)$ we set

$$k \odot l := (k \cdot l) \bmod n$$

- **The identity element:** 1.
- **Inverses:** If k is an element of $U(n)$, then we can find $p, q \in \mathbb{Z}$ such that $pk + qn = \gcd(k, n) = 1$. Let $\bar{p} = p \bmod n$. Notice that we have $\gcd(p, n) = 1$, so also $\gcd(\bar{p}, n) = 1$. Also,

$$(\bar{p} \cdot k) \bmod n = (pk) \bmod n = (pk + qn) \bmod n = 1$$

This means that $\bar{p} = k^{-1}$ in the group $U(n)$.