# Binary operation

Definition: A *binary operation* on a set $X$ is a map $X \times X \to X$.

Examples: Binary operations on $\mathbb{R}$ are $+$, $-$ and $\cdot$; notation $(\mathbb{R}, +)$.

Division $:$ is a binary operation on $\mathbb{R} \setminus 0$, or on $\mathbb{R}^+$, but not on $\mathbb{R}$. Formally $:$ is a mapping $\mathbb{R} \times (\mathbb{R} \setminus 0) \to \mathbb{R}$. We can restrict it to $\mathbb{R} \setminus 0$ or to $\mathbb{R}^+$. Extensions that allow dividing by $0$ make little sense.

On $\mathbb{N}$, $+$ and $\cdot$ are binary operations, but $-$ is not.

Matrix sum is a binary operation on matrices of the same order.

Product is a binary operation on *square* matrices of the same order.

$(a, b) \to a^2 - b + 18$ is a binary operation on $\mathbb{R}$ but not on $\mathbb{N}$.

$(a, b) \to b$ is a binary operation on any set.

$(p, q) \to r$, where $\forall x \in \mathbb{R} : r(x) = p(x) + q(x)$, is a binary operation on the set of real functions $\mathbb{R}[x]$, we write $r = p + q$.

A binary operation on a finite set can be described by a table, e.g.

$(a, b) \to \neg a \wedge b$

| | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 0 | 0 |

# Group

Definition: A group $(G, \circ)$ is a set $G$ together with a binary operation $\circ$ on $G$ satisfying axioms:

- $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$
  ... the operation $\circ$ is *associative*,
- $\exists e \in G \; \forall a \in G : a \circ e = e \circ a = a$
  ... $e$ is called the *neutral element*,
- $\forall a \in G \; \exists b \in G : a \circ b = b \circ a = e$
  ... $b$ is called the *inverse element* for $a$, denoted by $a^{-1}$

When the operation $\circ$ is *commutative*, i.e. $\forall a, b \in G : a \circ b = b \circ a$, then $(G, \circ)$ is called an *Abelian* group.

Examples: The smallest group is $(\{e\}, \circ)$, where $e \circ e = e$.
For $G = \{e, a, b\}$ and $\circ$ defined by the table we get the group $(G, \circ)$, with the neutral element $e$, $e$ is the inverse of itself, and the elements $a$ and $b$ are inverses of each other. This group is Abelian.

| | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

Fact: The smallest nonabelian group $S_3$ has 6 elements.

# Additive and multiplicative groups

Groups $(G, \circ)$ where $\circ$ is derived from addition are called *additive*, e.g. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}[x], +)$, $(\mathbb{R}^{m \times n}, +)$.
These examples are Abelian. $(\mathbb{N}, +)$ is not a group.

On additive groups the neutral element is called *null element* or *zero* and denoted by $0$, $\mathbf{0}$, $\mathbf{0}_{m,n}$, etc. The inverse is often called the *opposite* element and is denoted by $-a$ instead of $a^{-1}$.
One can introduce the binary operation *difference* as the sum with the opposite element, formally: $a - b = a + (-b)$.

*Multiplicative* groups have $\circ$ derived from product, like in Abelian groups $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\{-1, 1\}, \cdot)$ and $(\{z \in \mathbb{C} : |z| = 1\}, \cdot)$.

Regular matrices of order $n$ with $\cdot$ form a group that is *not Abelian*.
The neutral element is $\mathbf{I}_n$. The inverse element for $\boldsymbol{A}$ is $\boldsymbol{A}^{-1}$.

In multiplicative groups, the neutral element is often denoted by $1$.
Similarly, *division* can be defined as $a : b = a \cdot b^{-1}$.

# Group properties

Observation: The neutral element is unique.

Proof: If $e$ and $e'$ were both neutral then $e = e \circ e' = e'$.

Observation: Each $a$ uniquely determines its inverse element $a^{-1}$.

Proof: If $b$ and $b'$ were both inverse elements for $a$ then
$b = b \circ e = b \circ (a \circ b') = (b \circ a) \circ b' = e \circ b' = b'$.

Observation: The equivalent transformations are:
$a = b \iff a \circ c = b \circ c \iff c \circ a = c \circ b$

Proof: $\Rightarrow$ triv., $\Leftarrow$: $a = a \circ e = a \circ c \circ c^{-1} = b \circ c \circ c^{-1} = b \circ e = b$

Observation: Equations: $a \circ x = b$, $y \circ a = b$ have unique solutions.

Proof: $x = e \circ x = a^{-1} \circ a \circ x = a^{-1} \circ b$; analogously $y = b \circ a^{-1}$.

Exercise: Prove on your own: $(a^{-1})^{-1} = a$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.
$a \neq b \implies a^{-1} \neq b^{-1}$.

# Questions to understand the lecture topic

- The literature sometimes mentions so-called axioms of *closure*, e.g. $\forall a, b \in G : a \circ b \in G$. Why we omit these as axioms?
- Can the axiom of the existence of an inverse element be shortened to $\forall a \in G \; \exists b \in G : a \circ b = e$ and the relation $b \circ a = e$ be derived from it similarly to the statement about the inverse matrix?
- Can the axiom on the neutral element be simplified analogously?
- Which properties of binary operations guarantee the correctness of equivalent equation transformations in a group?