Binary operation

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

Examples: $+$ is a binary operation on $\mathbb{R}$; notation $(\mathbb{R}, +)$.

$+$ is a binary operation on matrices of the same order.

$\cdot$ is a binary operation on *square* matrices of the same order.

$(a, b) \to a + b - 18$ 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:

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

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

Examples: *Additive* groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}[x], +)$, $(\mathbb{R}^{m \times n}, +)$, all are Abelian. $(\mathbb{N}, +)$ is not a group.

Multiplicative groups: $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\{-1, 1\}, \cdot)$.

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

Group properties

Notation: The derived operations like subtraction/division mean the addition/multiplication with the inverse element.

Observation: The neutral element is unique.

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

Observation: Each inverse element a^{-1} is uniquely determined by a.

Proof: If b and b' were both inverse 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., $\Leftarrow$: $a = a \circ e = a \circ c \circ c^{-1} = b \circ c \circ c^{-1} = b$

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 $y = b \circ a^{-1}$.

Homework: Prove: $(a^{-1})^{-1} = a$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.