Binary operations

Casey Blacker
Math 300

Section 1

Properties of operations

Let $* : A \times A \to A$ be a binary operation on A.

Definition

We say that $*$ is

- *commutative* when

$$\forall a, b \in A : a * b = b * a$$

- *associative* when

$$\forall a, b, c \in A : (a * b) * c = a * (b * c)$$

Examples

i. Addition
$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$
is commutative and associative.

ii. Multiplication
$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$
is commutative and associative.

iii. Subtraction
$$- : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$
is neither commutative nor associative.

iv. The *partial operation*
$$\div : \mathbb{R} \times (\mathbb{R} \backslash \{0\}) \to \mathbb{R}$$
is neither commutative nor associative.

Examples

v. The cross product $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ is neither commutative nor associative.

vi. Union, intersection, and symmetric difference $\cup, \cap, \Delta : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ are commutative and associative for any set A.

vii. When $n \geq 2$, we have that $n \times n$ matrix multiplication $\mathrm{Mat}_{n,n}(\mathbb{R}) \times \mathrm{Mat}_{n,n}(\mathbb{R}) \to \mathrm{Mat}_{n,n}(\mathbb{R})$ is associative but *not* commutative.

viii. The midpoint operator $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by

$$x * y = \frac{x+y}{2}$$

is commutative but not associative.

Definition

The magma $(A, *)$ is called a *semigroup* when $*$ is associative.

Definition

If $(A, *)$ is such that $*$ is associative and commutative, then $(A, *)$ is called a *commutative semigroup*.

Section 2

Identity elements

Definition

We say that $e \in A$ is an *identity element* for $* : A \times A \to A$ when

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

Remarks

i. The element e is also called a *neutral element*, or simply an *identity*.

ii. When $*$ is considered as a multiplication opperation, e is sometimes written $1 \in A$. When it is considered as an addition operation, it is sometimes written $0 \in A$.

iii. If e satisfies

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

then it is called a *right identity*. It is called a *left identity* if

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

Examples

i. $0 \in \mathbb{R}$ is an identity for $(\mathbb{R}, +)$
ii. $1 \in \mathbb{R}$ is an identity for $(\mathbb{R}, \cdot)$
iii. Subtraction $- : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ does not admit an identity element $e \in \mathbb{R}$
iv. $\varnothing \in \mathcal{P}(A)$ is an identity for $(\mathcal{P}(A), \cup)$
v. $\varnothing \in \mathcal{P}(A)$ is also an identity for $(\mathcal{P}(A), \Delta)$
vi. $A \in \mathcal{P}(A)$ is an identity for $(\mathcal{P}(A), \cap)$
vii. The $n \times n$ identity matrix $I_n \in \mathrm{Mat}_{n,n}(\mathbb{R})$ is an identity for $(\mathrm{Mat}_{n,n}(\mathbb{R}), \cdot)$
viii. The midpoint operator on $\mathbb{R}$ does not admit an identity element $e \in \mathbb{R}$

Proposition

If $e \in A$ is an identity element for a binary operation $* : A \times A \to A$, then it is unique with this property.

Proof.

If $e, e' \in A$ are both identities for $*$, then

$$e = e * e' = e'.$$

□

Definition

A semigroup $(A, *)$ that admits an identity element $e \in A$ is called a *monoid*.

Section 3

Inverse elements

Let $*$ be a binary operation on A, and let $e \in A$ be an identity element.

Definition

Fix an element $a \in A$. If $b \in A$ satisfies

$$a * b = e = b * a$$

then b is called an *inverse element* of a, and we write $b = a^{-1}$.

Remark

If b satisfies $a * b = e$ (resp. $b * a = e$), then b is called a *right (resp. left) inverse* of a.

Proposition

Let $(A, *)$ be a semigroup. If $b \in A$ is an inverse of $a \in A$, then b is unique with this property.

Proof.

If $b, b' \in A$ are inverses of a, then

$$\begin{aligned} b &= e * b \\ &= (b' * a) * b \\ &= b' * (a * b) \\ &= b' * e \\ &= b'. \end{aligned}$$

$\square$

Examples

i. In $(\mathbb{R}, +)$, the inverse of $x \in \mathbb{R}$ is $-x$.

ii. In $(\mathbb{R}, \cdot)$, the inverse of $x \in \mathbb{R}\backslash\{0\}$ is $\frac{1}{x}$. The element $0 \in \mathbb{R}$ does not have an inverse.

iii. In $(\mathcal{P}(A), \cup)$, only $\varnothing \in \mathcal{P}(A)$ has an inverse.

iv. Likewise, in $(\mathcal{P}(A), \cap)$, only $A \in \mathcal{P}(A)$ has an inverse.

v. In $(\mathcal{P}(A), \Delta)$, the inverse of $S \in \mathcal{P}(A)$ is itself.

Definition

The semigroup $(A, *)$ is called a *group* when every $a \in A$ has an inverse $a^{-1} \in A$.

Definition

If $(A, *)$ is a group, and if $*$ is commutative, then $(A, *)$ is called an *abelian group*.

Examples

The following are abelian groups.

i. $(A, +)$ for $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

ii. $(A \backslash \{0\}, \cdot)$ for $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

iii. $(\mathcal{P}(A), \Delta)$ for any set A