Previously.

- Disjoint Cycles
- Transpositions
- Even vs Odd Permutations

This Section.

- Binary Operations
- Monoids

Definition. A `binary operation`, $*$ on a set S is a function that associates to each ordered pair $(a, b) \in S \times S$ an element of S which we call $a * b$.

Note. Since we know that $a * b \in S$ for all $a, b \in S$, we say that the binary operation is `closed under` $*$.

Note. Sometimes we write $(S, *)$ to mean $*$ is a binary operation on S.

Definition. A binary operation $*$ on S is `associative` if

$$a * (b * c) = (a * b) * c,$$

for all $a, b, c \in S$.

Definition. A binary operation $*$ on S is `commutative` if

$$a * b = b * a,$$

for all $a, b \in S$.

Definition. An element $e \in S$ is called an `identity` (or `unity`) for the binary operation $*$ if

$$a * e = e * a = a,$$

for all $a \in S$.

Theorem 2.1.1. If a binary operation $*$ on a set S has an identity, then it is unique.

Definition. A set S along with a binary operation $*$ is called an `monoid` if $*$ is associative and has an identity.

If $(S, *)$ is also commutative, then we say S is a `commutative monoid`.

Example. Here are two monoids:

- $(\mathbb{Z}, \cdot)$
- $(S_n, \circ)$

Exercise 1. Let $*$ be the binary operation on $\mathbb{N}$ given by

$$a * b := a^b.$$

(a) Associative?

(b) Identity?

(c) Commutative?

Therefore, $(\mathbb{N}, \hat{})$ is $\boxed{\text{commutative}}$ $\boxed{\text{a monoid}}$ $\boxed{\text{not a monoid}}$. (cross out those that do not apply)

Exercise 2. Let $*$ be the binary operation on $\mathbb{Z}$ given by

$$a * b := a - b.$$

(a) Associative?

(b) Identity?

(c) Commutative?

Therefore, $(\mathbb{Z}, -)$ is $\boxed{\text{commutative}}$ $\boxed{\text{a monoid}}$ $\boxed{\text{not a monoid}}$. (cross out those that do not apply)

Exercise 3. Let $*$ be the binary operation on $GL_2(\mathbb{R})$given by

$$A * B := AB.$$

(a) Associative?

(b) Identity?

(c) Commutative?

Therefore, $(GL_2(\mathbb{R}), \cdot)$ is is $\boxed{\text{commutative}}$ $\boxed{\text{a monoid}}$ $\boxed{\text{not a monoid}}$. (cross out those that do not apply)

Definition. Let $(M, *)$ be a monoid.
If $x \in M$, we call $y \in M$ an `inverse of` x if

$$xy = e = yx.$$

An element that has an inverse is called a `unit`.

Exercise 4. A nice table of monoids and their units.

Monoid	Identity Element	Set of Units
$(\mathbb{Z}, +)$		
$(\mathbb{R}, +)$		
$(\mathbb{Z}_n, +)$		
$(M_n(\mathbb{R}), +)$		
$(M_n(\mathbb{R}), \cdot)$		
$(\mathbb{R}, \cdot)$		
$(\mathbb{Z}_4, \cdot)$		
$(\mathbb{Z}_n, \cdot)$		
$(\mathbb{Z}_p, \cdot)$		
$(S_3, \circ)$		