Numbers

- **Set:** a collection of objects called **elements.**
- We write x ∈ S to mean that element x is in set S.
- A set is **nonempty** if it has at least one element.
- The empty set is denoted by ∅
- **Subset:** A subset of S is a set T with the property $x \in T \Rightarrow x \in S$.
- Every element of T is an element of S.
- Trivially, S ⊆ S and ∅ ⊆ S
- The subset symbol is denoted by ⊆.
- The set of Natural Numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ is useful for counting and for ordering.
- The order symbols are $<, \leq, \geq, >$

Set Algebra

- An **operation** on a set S is a rule for combining elements of S.
- **Binary operations:** combines pairs of elements to prove another.

A binary operation $*$ is **closed** if:

Definition

$$\boldsymbol{x, y \in S \Rightarrow x * y \in S}$$

- Four common operations on numbers are $+, -, \cdot, /$.

Exercise:

Are +, -, ·, / closed on ℕ? Prove or disprove

$+)\ a, b \in \mathbb{N} \Rightarrow a+b \in \mathbb{N}$ (Closed)

$-)\ 1, 5 \in \mathbb{N} \Rightarrow 1-5 = -4 \notin \mathbb{N}$ (Not closed)

$\cdot)$ Closed on $\mathbb{N}$

$/)\ 5, 3 \in \mathbb{N} \Rightarrow \frac{5}{3} \notin \mathbb{N}$ (Not closed)

An element e ∈ S is called an **identity** if:

Definition

$$\boldsymbol{x * e = x \text{ AND } e * x = x\ \forall\ x \in S}$$

Exercise:

Does ℕ have an identity under $+$? Under $\cdot$?

+) $e + x = x \wedge x + e = x$

Let $x = 1$, $e = 2$

$1 + 2 \neq 1 \wedge 2 + 1 \neq 1$

$\therefore$ Under $+$ binary operations on set of $\mathbb{N}$, there is NO identity.

•) $e \cdot x = x \wedge x \cdot e = x$

Let $e = 1$, $x = 2$,

$1 \cdot 2 = 2 \wedge 2 \cdot 1 = 2$.

$\therefore$ Under $\cdot$ binary operations, $e = 1$ is the identity.

If $\exists\ e$ identity of S, an element $x \in S$ is called **invertible** when $\exists\ y \in S \ni$:

> *Definition*
>
> $\boldsymbol{x * y = e\ AND\ y * x = e}$

Then **y** is called the **inverse** of **x.**

Exercise:

What are the invertible elements of ℕ under $+, \cdot$?

+) No identity $\therefore$ no invertible elements

•) $x \cdot y = e \wedge y \cdot x = e$

Let $x = 1$, $y = 1$

$1 \cdot 1 = 1 \wedge 1 \cdot 1 = 1$

$\therefore$ Under $\cdot$ for the set of $\mathbb{N}$. 1 is an inverse of itself.

A binary operation $*$ on S is **commutative** if:

> *Definition*
>
> $\boldsymbol{x * y = y * x\ \forall\ x, y \in S}$

It is **associative** if:

> *Definition*
>
> $\boldsymbol{(x * y) * z = x * (y * z)\ \forall\ x, y, z \in S}$

- The operations $+, \cdot$ are associative and commutative on ℕ.

Exercise:

Rock-Paper-Scissors.

Let M = {r, p, s} and consider the binary operation that gives the winner of the game.

$$\left.\begin{aligned} r * p &= p * r = p \\ s * p &= p * s = s \\ r * s &= s * r = r \end{aligned}\right\} \text{Commutative.}$$

$$p * p = s * s = r * r = \text{TIE}$$

Is $*$ associative?

$$(r * p) * s \neq r * (p * s) \quad \square$$

$\therefore$ Rock-paper-Scissors is not associative.

A binary operation $*$ is **distributive** over another $\cdot$ if for all $a, b, c \in S$.

Definition

$$\boldsymbol{a * (b \cdot c) = (a * b) \cdot (a * c) \;\; AND \;\; (a \cdot b) * c = (a * c) \cdot (b * c)}$$

For example, multiplication distributes over addition on $\mathbb{N}$.

Exercise:

Prove that addition does not distribute over multiplication on $\mathbb{N}$.

$$a + (b \cdot c) = (a + b) \cdot (a + c) \wedge (a \cdot b) + c = (a + b) \cdot (b + c) \;\; \forall a, b, c \in \mathbb{N}$$

Let $a = 1, b = 2, c = 3 \in \mathbb{N}$

$$1 + (2 \cdot 3) = (1 + 2) \cdot (1 + 3)$$

$$7 \neq 6 \quad \square$$

$\therefore$ + does not distribute over $\cdot$ $\forall a, b, c \in \mathbb{N}$

Exercise:

Let a, b ∈ ℕ. Simplify the following expression, giving reasons for each step. [8(a + b)] + 2a

$$\begin{aligned} &= [8a + 8b] + 2a && \text{(distribution)} \\ &= [8a + 2a] + 2b && \text{(association)} \\ &= (8 + 2)a + 2b && \text{(distribution)} \\ &= 10a + 2b && \square \end{aligned}$$

A set S with order $\leq$ is called **well-ordered** if every nonempty subset T of S has at least one smallest element.

Definition

That is, if $\boldsymbol{T} \subseteq \boldsymbol{S}, \boldsymbol{T} \neq \emptyset$, then $\exists\ \mathbf{s_0} \leq \mathbf{s}\ \forall\ \mathbf{s} \in \mathbf{T}$

The set $\mathbb{N}$ with the usual order $\leq$ is well-ordered.

The set of integers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ can be constructed from $\mathbb{N}$:

- It is the set of differences $\{m-n\}\ \forall\ m, n \in \mathbb{N}$.
- The order $\leq$ on $\mathbb{N}$ extends to $\mathbb{Z}$.

Exercise:

a) Are $+, -, \cdot, /$ closed on $\mathbb{Z}$?
b) Does $\mathbb{Z}$ has identities under $+, \cdot$?
c) What are the invertible elements of $\mathbb{Z}$ under $+, \cdot$?

a) $x, y \in \mathbb{Z} \Rightarrow x * y \in \mathbb{Z}$
+) Yes, closed.
-) Yes, closed.
$\cdot$) Yes, closed
/) Not closed, $1, 0 \in \mathbb{Z} \not\Rightarrow 1/0 \notin \mathbb{Z}$

b) $x * e = x \wedge e * x = x\ \forall x \in \mathbb{Z}$
+) $e = 0$
$\cdot$) $e = 1$

c) $x * y = e \wedge y * x = e$
+) If $\exists e$, x is invertible if
$\exists y \ni x + y = 0 \wedge y + x = 0$
Let $x < 0$, then $y = -x$
$\therefore x + (-y) = 0 \wedge -y + x = 0\ \forall x \in \mathbb{Z}$
$\cdot$) Proof: $x \neq \pm 1 \Rightarrow \frac{1}{x} \notin \mathbb{Z}$

- On $\mathbb{Z}$, $+$ and $\cdot$ are commutative and associative.
- On $\mathbb{Z}$, - and / are **not** commutative and associative.
- However, if we define a **– b = a + (-b)** and **a/b = a · 1/b**, then we have commutativity and associativity.

$\boldsymbol{a - b \neq b - a, BUT\ a + (-b) = -b + a}$ (associativity)

$\boldsymbol{\frac{a}{b} \neq \frac{b}{a}, BUT a \cdot \frac{1}{b} = \frac{1}{b} \cdot a}$ (distribution)

- Multiplication distributes over addition and subtraction on $\mathbb{Z}$:

$$\boldsymbol{a} \cdot (\boldsymbol{b} \pm \boldsymbol{c}) = (\boldsymbol{a} \cdot \boldsymbol{b}) \pm (\boldsymbol{a} \cdot \boldsymbol{c})$$
$$(\boldsymbol{a} \pm \boldsymbol{b}) \cdot \boldsymbol{c} = (\boldsymbol{a} \cdot \boldsymbol{c}) \pm (\boldsymbol{b} \cdot \boldsymbol{c})$$

Exercise:
Is $\mathbb{Z}$ well-ordered?

Well Ordered: if $T \in S$, $T \neq \emptyset$, then $\exists s_0 \leq s \ \forall s \in T$
Given $T = \{x \in T \ni -x\}$
$= \{\mathbb{Z}^-\}$

Some Common Rules

An integer $m \in \mathbb{Z}$ is **even** if $m = 2k$ for some $k \in \mathbb{Z}$.
An integer $m \in \mathbb{Z}$ is **odd** if $m = 2k + 1$ for some $k \in \mathbb{Z}$
An integer $m > 1$ is **prime** if whenever $m = rs$ for $r, s \in \mathbb{N}$, either $r = 1$ or $s = 1$
An integer $m > 1$ is **composite** if it is not prime (i.e. $m = ab$ with $a, b > 1$ AND $a, b < m, a, b \in \mathbb{N}$)

- The set of Rationals $\mathbb{Q}$ is the set of numbers q that can be written $q = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$
- $\mathbb{Q}$ can be constructed from $\mathbb{Z}$.

Dedekind Cuts

- To construct the Real Numbers $\mathbb{R}$, we can use $\mathbb{Q}$ and the Dedekind Cuts.
- A Dedekind Cut of $\mathbb{Q}$ is a pair of subsets (A, B) of $\mathbb{Q}$ that satisfy the following:
  - A and B are nonempty
  - $A \cup B = \mathbb{Q}$
  - A is closed downwards: If $q \in A$ and $r < q$, then $r \in A$
  - B is closed upwards: if $q \in B$ and $r > q$, then $r \in B$
  - A contains no greatest element: $\forall\, q \in A\ \exists\, r \in A \ni q < r$

- Given $q \in Q$, we can form a Dedekind Cut (A,B) where:

  $A = \{x \in Q : x < q\}$ AND $B = \{x \in Q : x \geq q\}$

- That is the Dedekind-Cut identification of all rational numbers $q \in \mathbb{Q}$
- But we can make such cuts at non-rational numbers as well.
- An irrational number is one that cannot be written as $\frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$.
  - An example is $\sqrt{2}$

Exercise:

Prove that $\sqrt{2} \notin \mathbb{Q}$

?

- The following Dedekind Cut defines $\sqrt{2}$:

  $\boldsymbol{A = \{x : x < 0 \text{ } OR \text{ } x^2 < 2\}, B = \{x : x > 0 \text{ } AND \text{ } x^2 \geq 2\}}$

- The numbers defined by <u>ALL</u> Dedekind Cuts of $\mathbb{Q}$ make up the set of Real Numbers $\mathbb{R}$.
- The usual order $\leq$ on $\mathbb{R}$ is inherited from $\mathbb{N}$.

Exercise:

a) Which of $+, -, \cdot, /$ are closed on $\mathbb{R}$?
b) Does $\mathbb{R}$ have identities under $+, \cdot$?
c) What are the invertible elements of $\mathbb{R}$ under $+, \cdot$?

a) $*$ is closed on S if $\forall a, b \in S$, $a * b \in S$
$+, -, \cdot$ are closed on $\mathbb{R}$
$/$ is not closed on $\mathbb{R}$ e.g. $1, 0 \in \mathbb{R}$, $\frac{1}{0} \notin \mathbb{R}$

b) Under $+$, $\mathbb{R}$ has the identity $e = 0$
Under $\cdot$, $\mathbb{R}$ has the identity $e = 1$

c) Under $+$, all values are invertible in $\mathbb{R}$
Under $\cdot$, all values except 0 are invertible.

- As in $\mathbb{Q}$, the operations $+, \cdot$ are commutative and associative.
- In $\mathbb{R}$, $-, /$ are not commutative and associative, unless you define them as we did in $\mathbb{Q}$.