

Functions

A **function**, or a **map** f from a set A to a set B , written as

$$\begin{aligned} f: a &\mapsto b \\ f(a) &= b, \quad \text{where } a \in A, b \in B \\ f: A &\rightarrow B \end{aligned}$$

(all forms are equivalent)

is a binary relation between elements of A and B with the property that for every $a \in A$ there is exactly one $b \in B$. i.e.:

$$f: A \rightarrow B \Leftrightarrow \forall a \in A \exists! b \in B | f: a \mapsto b$$

The **domain** of f is A

The **target** of f is B

The **range**, or the **image** of f , (sometimes written $f(A)$) is

$$\text{rng } f = \{b \in B | \exists a \in A, b = f(a)\}.$$

f is **onto**, or **surjective**, if its range is its target: $\text{rng } f = B$

f is **one-to-one** (1-1) or **injective** iff $a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)$

f is a **bijection** (f is a **bijective** function) iff it is onto and 1-1.

The **identity** function: $\iota_A = \{(a, a) \mid a \in A\}$.

The **inverse** of a function f is the set of reversed ordered pairs of f , iff it is a function:

$$f^{-1} = \{(b, a) \mid (a, b) \in f\}.$$

Propositions:

$f: A \rightarrow B$ has an inverse $f^{-1}: A \rightarrow B$, iff f is a bijection.

If $f: A \rightarrow B$ is a bijection, then $f^{-1}: A \rightarrow B$, is a bijection.

Definitions:

Sets A and B have the same cardinality, $|A| = |B|$, iff there is a **one-to-one correspondence** (i.e., a bijection) between them.

A set A is **countably infinite** iff $|A| = |\mathbb{N}|$, and **countable** iff it is either finite or countably infinite.

For any two sets A and B , $|A| \leq |B|$ iff there is a one-to-one function (injection) $A \rightarrow B$, and $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$.

Not all infinities are equal to each other!

Cardinal numbers: $|\mathbb{N}| = \aleph_0$, $|\mathbb{R}| = \aleph_1$, (?) $|\mathcal{P}(\mathbb{R})| = \aleph_2$, ...

Continuum hypothesis:

There is no set A with $\aleph_0 < |A| < |\mathbb{R}| = \aleph_1$

Schröder-Bernstein theorem:

$|A| \leq |B| \wedge |B| \leq |A| \rightarrow |A| = |B|$. (useful to prove that $|A| = |B|$)

Integers

For the following 3 sets:

- Set of integer numbers \mathbb{Z}
- Set of natural numbers \mathbb{N}
- Set of real numbers \mathbb{R}

\leq is a partial order, because it is reflexive, antisymmetric, transitive

Two binary operations: multiplication, ab , and addition, $a+b$

For each operation on the above 3 sets we have

Operation	+			×			
	Set	\mathbb{N}	\mathbb{Z}	\mathbb{R}	\mathbb{N}	\mathbb{Z}	\mathbb{R}
Closure	✓	✓	✓	✓	✓	✓	✓
Associativity	✓	✓	✓	✓	✓	✓	✓
Commutativity	✓	✓	✓	✓	✓	✓	✓
Identity exists	✗	✓	✓	✓	✓	✓	✓
Inverse exists for each element	✗	✓	✓	✗	✗	✗	✗
Distributivity: $a(b+c) = ab+ac$	✓	✓	✓	✓	✓	✓	✓

Properties:

$$a \leq b \Rightarrow a + c \leq b + c$$

$$a \leq b \wedge c \geq 0 \Rightarrow ac \leq bc$$

$$a \leq b \wedge c \leq 0 \Rightarrow ac \geq bc$$

smallest element

Well-ordering principle:

Any nonempty set of natural numbers has a smallest element.

Theorem: (here and below the symbol “ \exists ” means “such that”)

$$\forall a, b \in \mathbb{N} \exists! q, r \in \mathbb{Z}, 0 \leq q, 0 \leq r < b \ni a = qb + r$$

Theorem (division algorithm):

$$\forall a, b \in \mathbb{Z}, b \neq 0 \exists! q, r \in \mathbb{Z}, 0 \leq r < |b| \ni a = qb + r,$$

where q is called the **quotient** and r is called the **remainder**:

$$q = \begin{cases} \left\lfloor \frac{a}{b} \right\rfloor & \text{if } b > 0, \\ \left\lceil \frac{a}{b} \right\rceil & \text{if } b < 0. \end{cases}$$

Recall (page 77) that $\lfloor x \rfloor$, the **floor** of x , is the greatest integer that is less or equal to x , and $\lceil x \rceil$, the **ceiling** of x , is the smallest integer that is greater or equal to x .

As a generalization of decimal representations, one can define **base b** representations $(a_0, a_1, \dots, a_n)_b$: binary, octal, hexadecimal
example: $6 \times 9 = (42)_{13}$

Definition:

$\forall a, b \in \mathbb{Z}, b \neq 0$, b is a **divisor** or **factor** of a , write $b \mid a$, iff
 $\exists q \in \mathbb{Z} \ni a = qb$

Facts:

$$1 \mid n \quad \forall n \in \mathbb{N},$$

$$a \mid a \quad \forall a \in \mathbb{N},$$

$$n \mid 0 \quad \forall n \neq 0, n \in \mathbb{N},$$

$$b \mid a \text{ is a partial order,}$$

greatest common divisor (gcd), $a \wedge b$, is the glb,

least common multiple (lcm), $a \vee b$, is the lub,

the poset (\mathbb{N}, \mid) is a lattice.

Euclidean algorithm (of computing gcd):

$\forall a, b \in \mathbb{Z}, b < a$, write

$$a = q_1 b + r_1,$$

$$b = q_2 r_1 + r_2,$$

$$r_1 = q_3 r_2 + r_3, \dots$$

then $\gcd(a, b)$ is the last nonzero remainder.

Definition:

a, b are *relatively prime* $\Leftrightarrow \forall a, b \in \mathbb{Z}, a, b \neq 0, \gcd(a, b) = 1$.

Theorem:

$$\forall a, b \in \mathbb{Z} \exists m, n \in \mathbb{Z} \ni \gcd(a, b) = ma + nb$$

Exercise: prove that

$$\gcd(a, b) \operatorname{lcm}(a, b) = |ab|$$