0 Notation

Let X, Y be sets. Then, we introduce some simple notation: inclusion

$$x \in X$$

union

$$X \cup Y$$

intersection

$$X \cap Y$$

and the cartesian product

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

We call the Natural Numbers $\mathbb{N}$, Integers $\mathbb{Z}$, Rationals $\mathbb{Q}$ ($:= \left\{\frac{a}{b} : a, b, \in \mathbb{Z}\right\}$), Reals $\mathbb{R}$, and Complex Numbers $\mathbb{C}$. Notice that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

1 Maps

Let X, Y be two sets. A ***map*** f between X and Y denoted as

$$f : X \to Y$$

is a rule that takes *every* element of $x \in X$ to *an* element $y = f(x) \in Y$.

1.1 Composition

Let X, Y, Z be sets. Suppose $X \xrightarrow{f} Y \xrightarrow{g} Z$. Then a function $h : X \to Z$, $h(x) - g(f(x)) \in Z$ is called the ***composition*** denoted as $h = g \circ f$.

1.2 Identity

The ***identity map*** is denoted as $\mathrm{Id}_x : X \to X$, and is defined to be $\mathrm{Id}(x) = x$

1.3 Properties

Let X, Y, Z be sets.

1.3.1 Injective

A map $f : X \to Y$ is ***injective (into/one-to-one)*** if for every $x_1, x_2 \in X$, we have $f(x_1) \neq f(x_2)$ Taking the contrapositve, we get the statement: If $f(x_1) = f(x_2)$, then $x_1 = x_2$. In shorthand, it is

$$\forall x_1, x_2 \in X, f(x_1) \neq f(x_2) \iff f(x_1) = f(x_2) \implies x_1 = x_2 \forall x_1, x_2 \in X$$

1.4 Surjective

A map $f : X \to Y$ is ***surjective (onto)*** if for every $y \in Y$, there exists some $x \in X$ such that $y = f(x)$. In shorthand, it is

$$\forall y \in Y, \exists x \in X : y = f(x)$$

1.5 Bijective

A map $f : X \to Y$ is ***bijective*** if it is both *injective* and *surjective*.

1.6 Inverse Maps

Let $f : X \to Y$ be a map. A map $g : Y \to X$ is called the ***inverse of*** f if the composition is the Identity map; that is, $g \circ f = \mathrm{Id}_x$, $f \circ g = \mathrm{Id}_y$ and is denoted as $g = f^{-1}$.

Proposition

A map $f : X \to Y$ has an inverse *if and only if* f is bijective.

Proof. ($\implies$) Let $g : Y \to X$ be an inverse of f. Then $g \circ f = \mathrm{Id}_x, f \circ g = Id_y$. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Then,

$$
\begin{aligned}
x_1 &= \mathrm{Id}_x(x_1) \\
&= (g \circ f)(x_1) \\
&= g(f(x_1)) \\
&= g(f(x_2)) && f(x_1) = f(x_2) \text{ by assumption} \\
&= (g \circ f)(x_2) \\
&= \mathrm{Id}_x(x_2) \\
x_1 &= x_2
\end{aligned}
$$

so f is injective.

Take any $y \in Y$. Then $x := g(y)$ for some $x \in X$. Then,

$$f(x) = f(g(y)) = (f \circ g)(y) = \mathrm{Id}_y(y) = y$$

so f is surjective. Because f is both injective and surjective, it is bijective.

($\impliedby$) Assume f be bijective. Then let $g : Y \to X$. Take any $y \in Y$. There exists a unique $x \in X$ such that $y = f(x)$ because f is bijective. Therefore, g is an inverse of f. $\square$

2 Integers

2.1 Induction I

Let $n_0 \in \mathbb{Z}$, and $\mathrm{P}(n)$ be a statement for all $n \geq n_0$. Suppose

(i) $\mathrm{P}(n_0)$ is true.

(ii) $\mathrm{P}(n) \implies \mathrm{P}(n+1)$ for every $n \geq n_0$.

Then $\mathrm{P}(n)$ is true for all $n \geq n_0$.

Proposition

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Proof. Let $\mathrm{P}(n) := 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. We will induct on n.

(i) $\mathrm{P}(1)$ is true.

(ii) $\mathrm{P}(n) \implies \mathrm{P}(n+1)$

$$
\begin{aligned}
1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}
$$

so $\mathrm{P}(n+1)$ is true, completing the induction.

$\square$

2.2 Induction II (Strong Induction)

Let $n_0 \in \mathbb{Z}$, and $\mathrm{P}(n)$ be a statement for all $n \geq n_0$. Suppose

(i) $\mathrm{P}(n)$ is true.

(ii) For every $n > n_0$, if $\mathrm{P}(k)$ is true for every $n_0 \leq k \leq n$, then $\mathrm{P}(n)$ is true.

Then $\mathrm{P}(n)$ is true for all $n \geq n_0$.

Proposition

Every positive integer can be written in the form

$$n = 2^{K_1} + 2^{K_2} + \cdots + 2^{K_m}$$

where $K_i \in \mathbb{Z}$ and $0 \leq K_1, < K_2, \cdots < K_m$.

Proof. We will induct on n.

(i) $\mathrm{P}(1)$ is true.

(ii) We know that $\mathrm{P}(k)$ is true for $k = 1, 2, \ldots, n-1$. Then for n, we find the largest s such that $2^s \leq n$. There are two cases:

  (i) $n = 2^s$. Then $\mathrm{P}(n)$ is true.

  (ii) $2^s < n$, $p := n - 2^s > 0$.
  Apply $\mathrm{P}(p)$: $p = 2^{K_1} + \cdots 2^{K_m}$, $0 \leq K_1, < K_2 < \cdots K_m$.
  $\implies n = 2^{K_1} + \cdots 2^{K_m} + 2^s$ Then, $p > 2^{K_m}$, so $2^s > 2^{K_m}$
  $\implies s > k_m$, completing the induction.

□

2.3 Division of Integers

Let $n, m \in \mathbb{Z}, m \neq 0$. Then, n is divisible by m if there exists some $q \in \mathbb{Z}$ such that $n = mq(\iff \frac{n}{m} \in \mathbb{Z})$ and we denote this as $m \mid n$, read as "m divides n".

2.3.1 Properties

(i) $1 \mid n$ for every $n \in \mathbb{Z}$ and $m \mid 0$ for every $m \neq 0$.

(ii) If $m \mid n_1$ and $m \mid n_2$, then $m \mid (n_1 \pm n_2)$.

  Proof. $n_1 = mq_1$ and $n_2 = mq_2$
  $\implies n_1 \pm n_2 = mq_1 \pm mq_2 = m(q_1 + q_2) \implies m \mid (n_1 \pm n_2)$ since $q_1 + q_2 \in \mathbb{Z}$. □

(iii) If $m \mid n$, then $m \mid an$ for all $a \in \mathbb{Z}$.

  Proof. $n = m \cdot q, q \in \mathbb{Z}$, $an = m \cdot (aq), aq \in \mathbb{Z} \implies m \mid an$. □

(iv) If $m \mid n_1$ and $m \mid n_2$, then $m \mid a_1 n_1 + a2_n 2$ for every $a_1, a_2 \in \mathbb{Z}$.

  Proof. By *(iii)*, $m \mid a_1 n_1$ and $m \mid a_2 n_2$. By *(ii)*, $m \mid a_1 n_1 + a_2 n_2$. □

(v) If $m \mid n, n \neq 0$, then $|m| \leq |n|$.

  Proof. $n = m \cdot q, q \in \mathbb{Z}, q \neq 0, |n| = |m| \cdot |q| \geq |m|$. □

(vi) If $m \mid n$ and $n \mid m$, then $n = \pm m$.

  Proof. By *(v)*, $|m| \leq |n| \leq |m| \implies n = \pm m$. □

2.3.2 Division Algorithm

Theorem

Let $n, m \in \mathbb{Z}, m \neq 0$. Then, there are *unique* $q, r \in \mathbb{Z}$ such that

$$n = m \cdot q + r,\ 0 < r < m$$

where q is the partial quotient and r is the remainder on dividing n by m.

Proof. ***Existence*** Define an infinite set $S = \{n - mx, x \in \mathbb{Z}\}$ containing nonnegative integers. Take $S \cap \mathbb{Z}^{\geq 0} \neq \emptyset$, so S is non-empty. Then by the well ordering principle, every non-empty set of $\mathbb{Z}^{\geq 0}$ has a least element, $n - mx \in S \cap \mathbb{Z}^{\geq 0}$. Call $q = x$, $r := n - mx \geq 0$. Then $n = mx + r = mq + r$. To show that $r < m$, take $r - m = (n - mq) - m = n - m(q + 1) \in S$. This shows that $r - m < r$, but since we chose r to be the *least* element in $S \cap \mathbb{Z}^{\geq 0}$, $r - m \notin S$. So $r - m < 0 \implies r < m$. $\square$