Principle of Strong Induction

from basis ℓ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If both

BASE CASE

- $P(\ell)$ and

INDUCTIVE STEP

- $\forall\, n \geq \ell$ in $\mathbb{N}.\ \Big(\overbrace{\big(\forall\, k \in [\ell..n].\, P(k)\big)}^{P(\ell) \wedge P(\ell+1) \wedge \cdots \wedge P(n-1) \wedge P(n)} \implies P(n+1) \Big)$

hold, then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\, P(m)$ holds.

Fundamental Theorem of Arithmetic

Proposition 76 *Every positive integer greater than or equal* 2 *is a prime or a product of primes.*

PROOF: $\forall n \geq 2.\ P(n)$

$P(n) =_{def}$ n is a prime or n is a product of primes.

<u>BASE CASE</u>:

<u>RTP</u>: 2 is a prime or 2 is a product of primes.

Which holds because 2 is prime.

INDUCTIVE STEP Let $n \geq 2$.

Assume $P(i)$ for all $2 \leq i \leq n$ (IH)

RTP: $P(n+1)$; that is, $(n+1)$ is prime or $(n+1)$ is a product of primes.

Case (1): $(n+1)$ is prime.
and we are done.

Case (2): $(n+1)$ is not prime
Hence $(n+1) = p.q$ for p and q not 1.
So we have $2 \leq p, q \leq n$

Thus, by (I.H), p is prime or a product of primes and q is prime or a product of primes.

Therefore, $p \cdot q$ is a product of primes.

and we are done $\boxtimes$

uniqueness of prime decomp.

Theorem 77 (Fundamental Theorem of Arithmetic) *For every positive integer n there is a unique finite ordered sequence of primes $(p_1 \leq \cdots \leq p_\ell)$ with $\ell \in \mathbb{N}$ such that*

$$n = \prod(p_1, \ldots, p_\ell) \quad .$$

$$\| \text{def}$$

$$p_1 \cdot p_2 \cdot \cdots \cdot p_{\ell-1} \cdot p_\ell$$

PROOF:

By convention:

$$\Pi(\,) = 1$$

uniqueness.

Proof idea :

$$\Pi(p_1, \dots, p_\ell) = \Pi(q_1, \dots, q_k)$$

p_i are ordered primes
q_j are ordered primes

$\implies$ $\ell = k$
$p_1 = q_1$
$\vdots$
$p_\ell = q_\ell$

Suppose $\Pi(p_1 \dots p_\ell) = \Pi(q_1 \dots q_k)$.

$\implies p_1$ equals some $q_j \implies q_1 \leq p_1$
$\implies q_1$ equals some $p_i \implies p_1 \leq q_1$
$\implies p_1 = q_1$

By cancellation, $\Pi(p_2, \dots, p_\ell) = \Pi(q_2, \dots, q_k)$

Analogously we have

$$\Pi(p_3, \dots p_\ell) = \Pi(q_3 \dots q_k)$$

and continuing like this, say wlog for $\ell > k$, we have

$$\Pi(p_{k+1}, \dots, p_\ell) = \Pi() = 1$$

$$\Rightarrow (p_{k+1}, \dots, p_\ell) = ()$$

$$\Rightarrow \ell = k \text{ and } p_i = q_i$$

$\boxtimes$

informal argument by iteration has a formal counter-part by induction.

Euclid's infinitude of primes

Theorem 80 *The set of primes is infinite.*

PROOF: By contradiction, assume the set of primes is finite; say $p_1, p_2, \ldots\ldots, p_N$

Consider $p = (p_1 \cdot p_2 \cdot \ldots \cdot p_N) + 1$

Then $p > p_i \ \forall i$, so p is not prime.

Hence there is p_k such that $p_k \mid p$.

But then since $p_k \mid (p_1 \cdots p_k \cdots p_N)$ we have

$p_k \mid p - (p_1 \cdots p_N)$. That is, $p_k \mid 1$: a contradiction $\boxtimes$

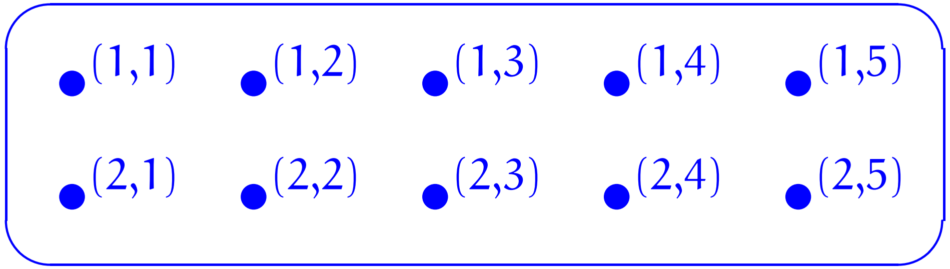
Sets

Objectives

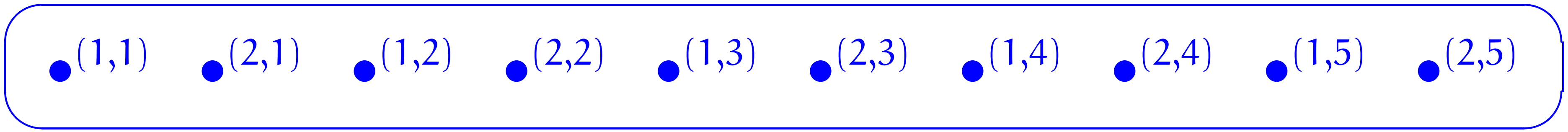
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

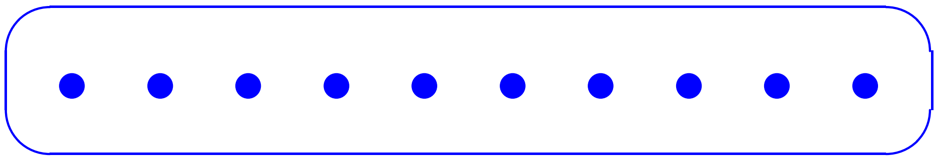
It has been said that a set is like a mental “bag of dots”, except of course that the bag has no shape; thus,



may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as



or even simply as



for other considerations.

Naive Set Theory

We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquitous structures that are available within it.

$\boxed{?}$ When are two sets equal?

Extensionality axiom

$\boxed{\text{Two sets are equal if they have the same elements.}}$

Thus,

$$\forall \text{ sets } A, B.\ A = B \iff (\forall x.\, x \in A \iff x \in B)\ .$$

$\{ p/q \mid p, q \in \mathbb{Z} \wedge q \neq 0 \} = \{ m/n \mid m \in \mathbb{Z}, n \in \mathbb{N}_{\geq 1}, \underline{gcd}(m,n) = 1 \}$

Example:

$$\{0\} \neq \{0,1\} = \{1,0\} \neq \{2\} = \{2,2\}$$