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 $\mathbb{N}.\ \Big(\ \big(\forall\, k \in [\ell..n].\ P(k)\big) \implies P(n+1)\ \Big)$

hold, then

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

Fundamental Theorem of Arithmetic

Proposition 95 *Every positive integer greater than or equal 2 is a prime or a product of primes.*

PROOF:

<u>Base case</u>: Holds because 2 is prime.

<u>Inductive step</u>: Consider $n \geq 2$.

Assume for all $k = 2, 3, \ldots, n$ $(2 \leq k \leq n)$

k is prime or a product of primes.

<u>RTP</u>: $n+1$ is prime or a product of primes.

Consider two cases:

(1) $n+1$ is prime; Then we are done.

(2) $n+1$ is composite; Then $n+1 = a \cdot b$ with $a, b \geq 2$. Observe $a, b \leq n$.

Then, by (IH), a is a prime or a product of primes and b is a prime or a product of primes. Therefore $n+1 = a \cdot b$ is a product of primes.

$\boxtimes$

Theorem 96 (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*

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

PROOF:

notation

$$\prod(\,) \stackrel{\text{def}}{=} 1$$

$$\prod(p_1, \ldots, p_{\ell+1}) \stackrel{\text{def}}{=} \prod(p_1 \ldots p_\ell) \cdot p_{\ell+1}$$

Euclid's infinitude of primes

Theorem 99 *The set of primes is infinite.*

PROOF: Assume for a contradiction that there are a finite set of primes:

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_N$ for $N \in \mathbb{N}$

Consider $\left(\prod_{i=1}^{N} p_i\right) + 1$. It is not a prime. So it is a product of primes. So there is p_k such that $p_k \mid \left(\prod_{i=1}^{N} p_i\right) + 1$. Also $p_k \mid \prod_{i=1}^{N} p_i$.

Hence, $p_k \mid \left(\prod_{i=1}^{N} p_i + 1\right) - \prod_{i=1}^{N} p_i = 1$. ↯ $\boxtimes$

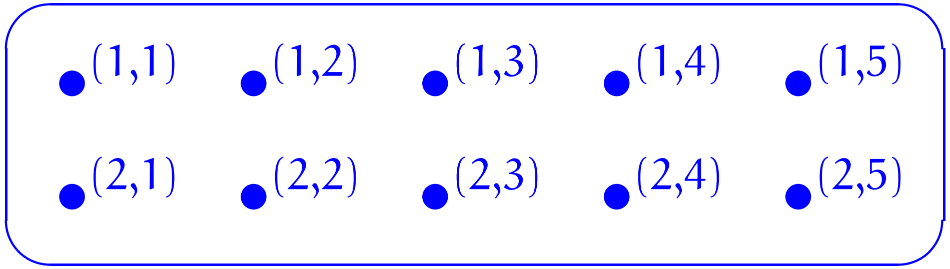
Sets

Objectives

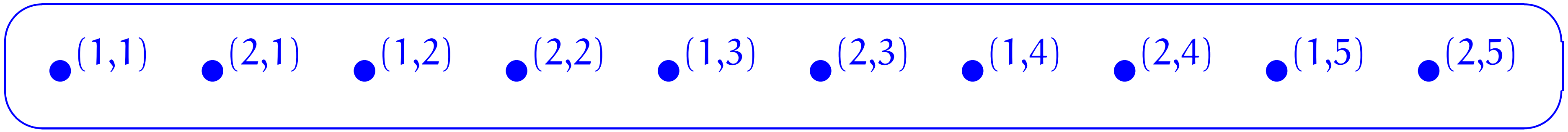
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

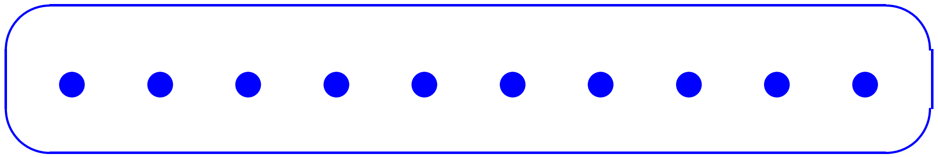
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



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.

Set membership

We write $\in$ for the *membership predicate*; so that

$$x \in A \text{ stands for } x \text{ is an element of } A \quad .$$

We further write

$$x \notin A \text{ for } \neg(x \in A) \quad .$$

Example: $0 \in \{0, 1\}$ and $1 \notin \{0\}$ are true statements.

Extensionality axiom

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

Thus,

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

Example:

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

$$B = C \iff \left(b = b + \sqrt{b^2 - c} \ \land \ b = b - \sqrt{b^2 - c} \right)$$

exo.

Proposition 100 *For* $b, c \in \mathbb{R}$, *let*

$$\begin{aligned} A &= \{\, x \in \mathbb{C} \mid x^2 - 2b\overset{x}{c} + c = 0 \,\} \\ B &= \{\, b + \sqrt{b^2 - c} \,,\ b - \sqrt{b^2 - c} \,\} \\ C &= \{\, b \,\} \end{aligned}$$

Then,

$$\forall x. \left(x \in \mathbb{C} \land x^2 - 2bc + c = 0 \right) \iff \left(x = b + \sqrt{b^2 - c} \ \lor \ x = b - \sqrt{b^2 - c} \right)$$

1. $A = B$, *and*

2. $B = C \iff b^2 = c$.

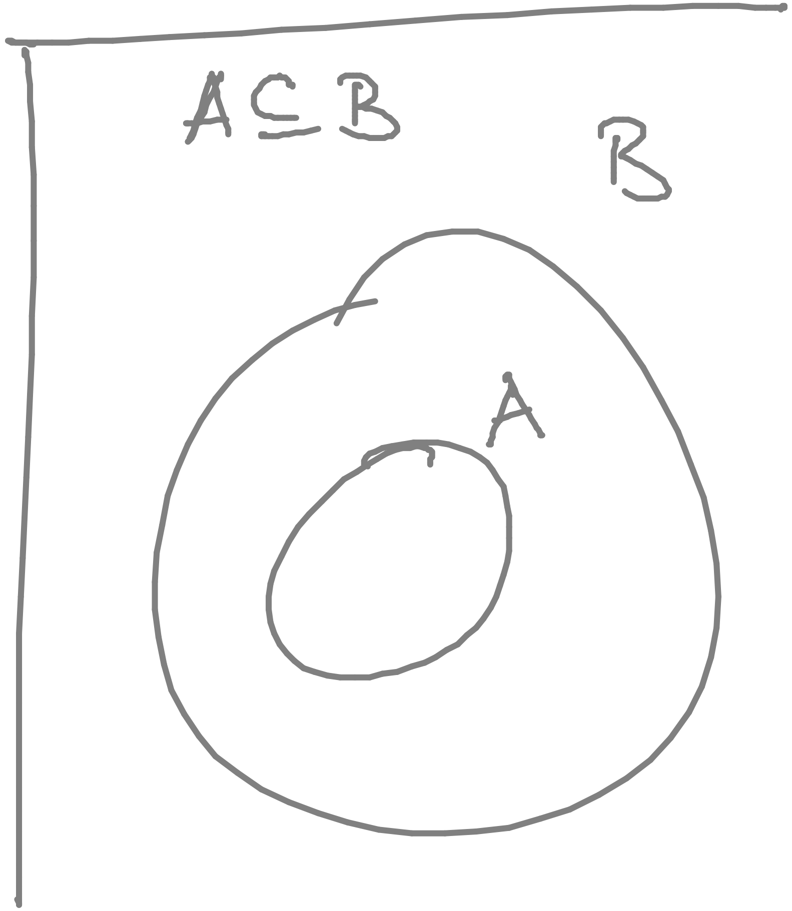
Subsets and supersets

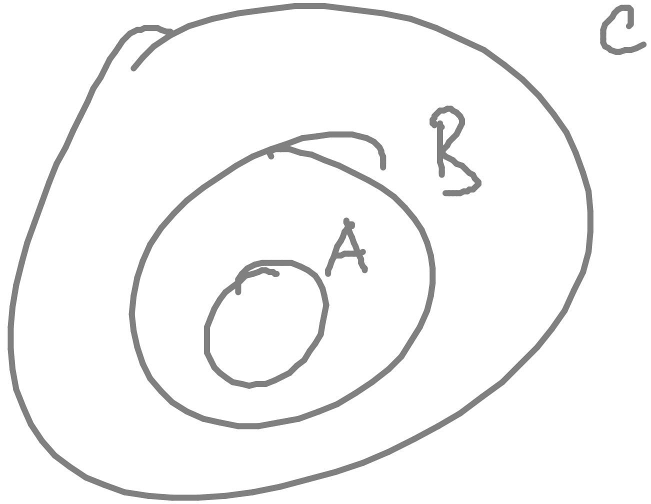
$$A = B \overset{\text{def}}{\iff} \forall x.\,(x \in A \iff x \in B)$$

$$\iff \forall x.\,(x \in A \implies x \in B) \wedge (x \in B \implies x \in A)$$

$$A \subseteq B \overset{\text{def}}{\iff} \forall x.\,(x \in A \implies x \in B)$$

$$A = B \iff (A \subseteq B) \wedge (B \subseteq A)$$





Lemma 103

1. *Reflexivity.*

   For all sets A, $A \subseteq A$.

2. *Transitivity.*

   For all sets A, B, C, $(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$.

3. *Antisymmetry.*

   For all sets A, B, $(A \subseteq B \wedge B \subseteq A) \implies A = B$.

$$a \in \{x \in A \mid P(x)\} \iff (a \in A \wedge P(a))$$

Separation principle

For any set A and any definable property P, there is a set containing precisely those elements of A for which the property P holds.

$$\{x \in \underbrace{A}_{} \mid \mathrm{P}(x)\} \subseteq A$$

Russell's paradox

$$\mathcal{U} = \{ x \mid R(x) \} \qquad R(x) \overset{\text{def}}{\Longleftrightarrow} x \notin x$$

For arbitrary x:

$$x \in \mathcal{U} \Longleftrightarrow R(x) \Longleftrightarrow x \notin x$$

$$\boxed{x \in \mathcal{U} \Longleftrightarrow x \notin x}$$

Then

$$\mathcal{U} \in \mathcal{U} \Longleftrightarrow \mathcal{U} \notin \mathcal{U} \quad \lightning$$

$\forall x. \neg(x \in \emptyset) \iff \forall x. (x \in \emptyset \Rightarrow \underline{false})$

Empty set

Set theory has an

empty set ,

typically denoted

$\emptyset$ or $\{\}$,

with no elements.

Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set S are $\#S$ or $|S|$.

Example:

$$\#\emptyset = 0$$

Finite sets

The *finite sets* are those with cardinality a natural number.

Example: For $n \in \mathbb{N}$,

$$[n] = \{x \in \mathbb{N} \mid x < n\}$$

is finite of cardinality n. $= \{0, 1, 2, \ldots, n-1\}$

Powerset axiom

$\boxed{\text{For any set, there is a set consisting of all its subsets.}}$

$$\mathcal{P}(U)$$

$$\forall X.\ X \in \mathcal{P}(U) \iff X \subseteq U \quad .$$

$$\mathcal{P}(\{x,y,z\})$$

$$= \Big\{ \begin{array}{ll} \{\}, & 0 \\ \{x\}, \{y\}, \{z\}, & 1 \\ \{x,y\}, \{x,z\}, \{y,z\}, & 2 \\ \{x,y,z\} & 3 \end{array} \Big\}$$

$$\# \mathcal{P}(\underbrace{\{x,y,z\}}_{3}) = 8 = 2^3$$