Euclid's infinitude of primes

Theorem 80 *The set of primes is infinite.*

PROOF: By contradiction assume that there are a finite number of primes, say $p_1, p_2, \dots, p_N$ (for $N \in \mathbb{N}$).

Consider
$$(p_1 \cdot p_2 \cdot \dots \cdot p_N) + 1 \in \mathbb{N}$$

Since it is not prime, as it is bigger than all the p_i, it is a product of primes. Hence it is divisible by a prime say p_i. So:

$$p_1 \cdot p_2 \cdots p_N + 1 = p_i \cdot k \quad \text{for some } k \in \mathbb{N}$$

Then

$$p_i \cdot k + (-1)\, p_1 \cdot p_2 \cdots p_N = 1$$

<u>Lemma</u>: If $ax + by = 1$ for a, b positive integers and x, y are integers then $\underline{\gcd}(a,b) = 1$.

$$p_i \cdot k + p_i \cdot l = 1 \qquad l = (-1) \cdot p_1 \cdots p_{i-1}\, p_{i+1} \cdots p_N$$

$\Downarrow$ by Lemma

$$\underline{\gcd}(p_i, p_i) = 1 \quad \text{a contradiction}$$

$\gcd(p_i,p_i) = p_i$

$\square$

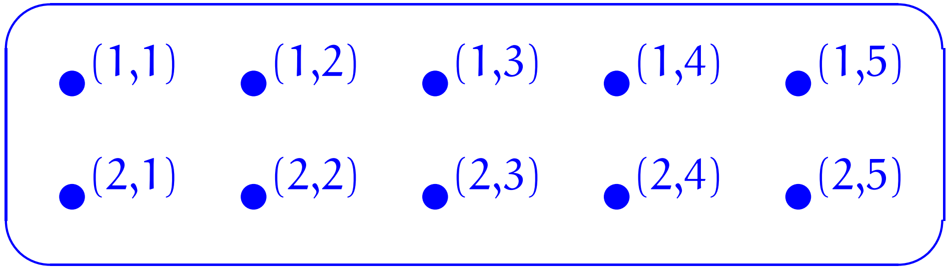
Sets

Objectives

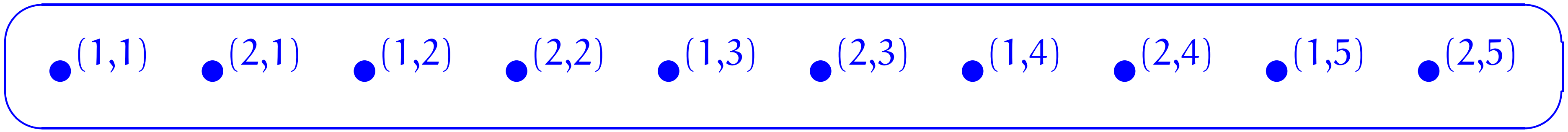
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

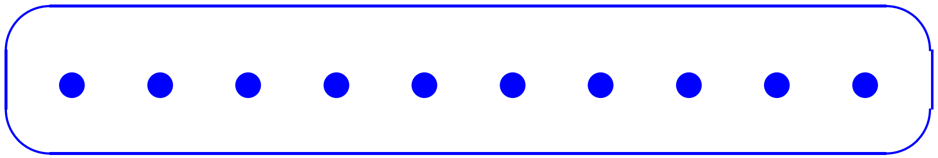
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



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.

NB: The crucial predicate of set theory is

$$x \in A$$

Extensionality axiom

Two sets are equal if they have the same elements.

Thus,

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

Example:

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

Example

$$\underline{CD}(m,n) \overset{\text{def}}{=} \{d \in \mathbb{N} \mid d|m \wedge d|n\}$$

$$\underline{CD}(m,n) = \underline{D}(\underline{gcd}(m,n))$$

$$\underline{D}(\underline{gcd}(m,n)) \overset{\text{def}}{=} \{k \in \mathbb{N} \mid k \mid \underline{gcd}(m,n)\}$$

$$\forall i \in \mathbb{N}.\ (i|m \wedge i|n) \iff i \mid \underline{gcd}(m,n)$$

Subset inclusion

Subsets and supersets

A is a subset of B

equiv.

$$A \subseteq B \iff (\forall x.\ x \in A \Rightarrow x \in B)$$

B is a superset of A

NB: $A = B \Rightarrow A \subseteq B$

Example We can have $A \subseteq B$ with $A \neq B$; e.g.

$$A = \{0\},\ B = \{0, 1\}$$

NB: We have given ourselves various sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$

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.

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

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

Russell's paradox

$\boxed{?}$ What about a more liberal way to construct subsets by separation as follows:

$$\{x \mid P(x)\}$$

?

Suppose the above is allowed, then define

$$R = \{x \mid x \notin x\}$$

Consider whether or not R is in R?

if $R \in R$ then $R \in \{x \mid x \notin x\}$ so $R \notin R$

if $R \notin R$ then $\neg(R \in \{x \mid x \notin x\})$ so $R \in R$

Notation

$a \notin A$

$=$

$\neg(a \in A)$

NB:
$$\emptyset = \{x \in A \mid \underline{false}\}$$

Empty set

$\emptyset$ or $\{\}$

defined by

$$\forall x.\, x \notin \emptyset$$

or, equivalently, by

$$\neg(\exists x.\, x \in \emptyset)$$

Example: for all sets A,

$$\emptyset \subseteq A$$

That is,

$$\forall x.\, x \in \emptyset \Rightarrow x \in A$$

equivalently

$$\underbrace{\forall x.\, false \Rightarrow x \in A}_{\text{which is true.}}$$

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:

$$\#\emptyset = 0$$

Examples: $\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$ $\quad \#\mathcal{P}(\emptyset) = 1$

$\mathcal{P}(\{*\}) = \{\emptyset, \{*\}\}$ $\quad \#\mathcal{P}(\{*\}) = 2$

Powerset axiom

For any set, there is a set consisting of all its subsets.

$\mathcal{P}(U)$ — powerset of U

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

In general if $\#U = n$ then $\#\mathcal{P}(U) = 2^n$

Remark $\emptyset \in \mathcal{P}(U)$.