Euclid's infinitude of primes

Theorem 99 *The set of primes is infinite.*

PROOF: Suppose by contradiction that there are finite prime numbers. Let $p_1, p_2, \dots, p_N$ be the prime numbers for N a natural number.

Consider $(p_1 \cdot p_2 \cdot \dots \cdot p_N) + 1$.

which is not prime. So there is p_i such that $p_i \mid (p_1 \dots p_N) + 1$. Also $p_i \mid (p_1 \dots p_N)$ and so $p_i \mid [(p_1 \dots p_N) + 1] - (p_1 \dots p_N) = 1$. which is a contratiction.

$\boxtimes$

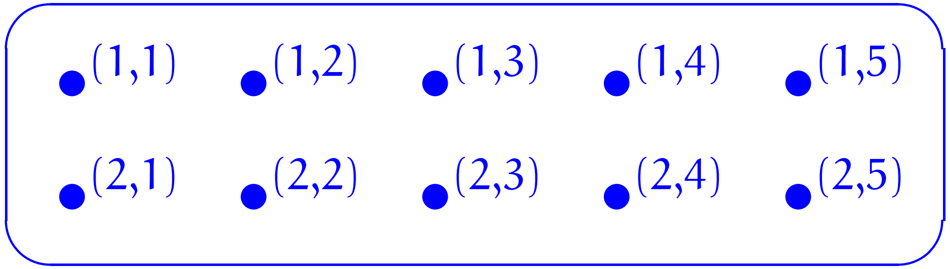
Sets

Objectives

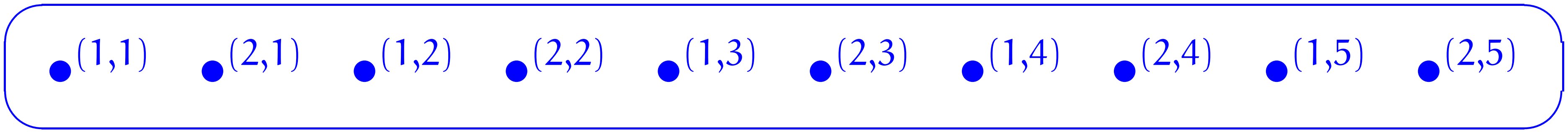
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

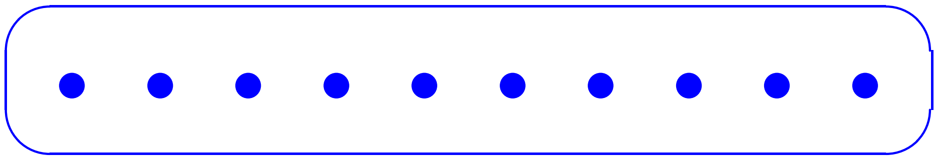
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



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

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

We further write

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

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:

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

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

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

(2) ($\Rightarrow$) Assume $B = C$; i.e.

$$\{ b + \sqrt{b^2 - c}, \, b - \sqrt{b^2 - c} \} = \{ b \}$$

Then,

1. $A = B$, *and*
2. $B = C \iff b^2 = c$.

$\rightarrow \quad b \in \{b\} = \{b+\sqrt{b^2-c},\ b-\sqrt{b^2-c}\}$

$\Rightarrow \quad b \in \{b+\sqrt{b^2-c},\ b-\sqrt{b^2-c}\}$

So $b = b+\sqrt{b^2-c}$ or $b = b-\sqrt{b^2-c}$

In both case, it follows that $b^2 = c$.

($\Leftarrow$) Assume $b^2 = c$

RTP: $\{b+\sqrt{b^2-c},\ b-\sqrt{b^2-c}\}$

$= \{b+0,\ b-0\} = \{b, b\} = \{b\}$.

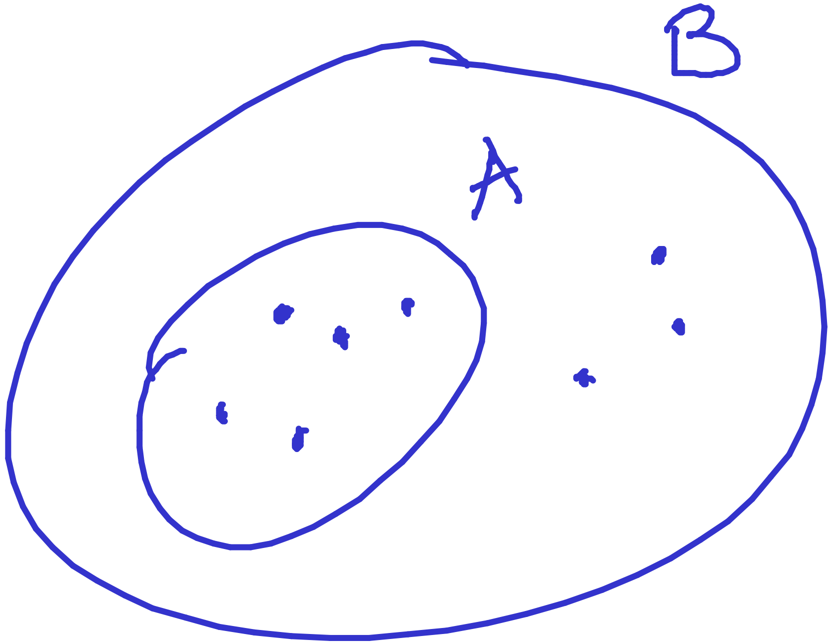
$\boxtimes$

Subsets and supersets

A is a <u>subset</u> of B, write $A \subseteq B$, whenever

$$\forall x.\ x \in A \Rightarrow x \in B.$$

Also, B is a <u>superset</u> of A.



<u>NB</u>: $A = B$ 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, $(A \subseteq B \land B \subseteq C) \implies A \subseteq C$.

3. *Antisymmetry.*

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

(2) Let A, B, C be sets.
Assume $A \subseteq B$ and $B \subseteq C$. i.e.
(1) $(\forall x.\ x \in A \Rightarrow x \in B)$ and (2) $(\forall x.\ x \in B \Rightarrow x \in C)$

RTP: $A \subseteq C$, i.e. $\forall x.\ x \in A \Rightarrow x \in C$.

Let x be arbitrary.

Suppose $x \in A$. By 1, we have $x \in B$. Then, by 2, $x \in C$.

$\boxtimes$

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

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.

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

$\overset{def}{\iff}$

$[a \in A \wedge P(a)]$

$\{x \in A \mid P(x)\} \equiv \{x \in A : P(x)\}$

Russell's paradox

$\boxed{?}$ Can one <u>arbitrarily</u> define sets by comprehension?

which relying on already constructed sets.

Should we allow definition of sets $\{x \mid P(x)\}$?

If $U = \{x \mid \neg(x \in x)\}$ is a set.

Then $U \in U \Leftrightarrow \neg(U \in U)$.

$x \in \emptyset \iff \underline{\text{false}}$

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

$\underline{\text{NB}}: \emptyset \subseteq A$

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 $n \in \mathbb{N}$,

$$[n] = \{x \in \mathbb{N} \mid x < n\} = \{0, 1, \ldots, n-1\}$$

is finite of cardinality n.

$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$

$\mathcal{P}\emptyset = \{\emptyset\}$

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

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

Powerset axiom

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

$\#\mathcal{P}\{a\} = 2$

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

$\#\mathcal{P}\emptyset = 1$

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

$\#\mathcal{P}\{a,b\} = 4$

$\mathcal{P}\{a,b\} = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

NB: The powerset construction can be iterated. In particular,

$$\mathcal{F} \in \mathcal{P}\big(\mathcal{P}(\mathcal{U})\big) \iff \mathcal{F} \subseteq \mathcal{P}(\mathcal{U}) \quad ;$$

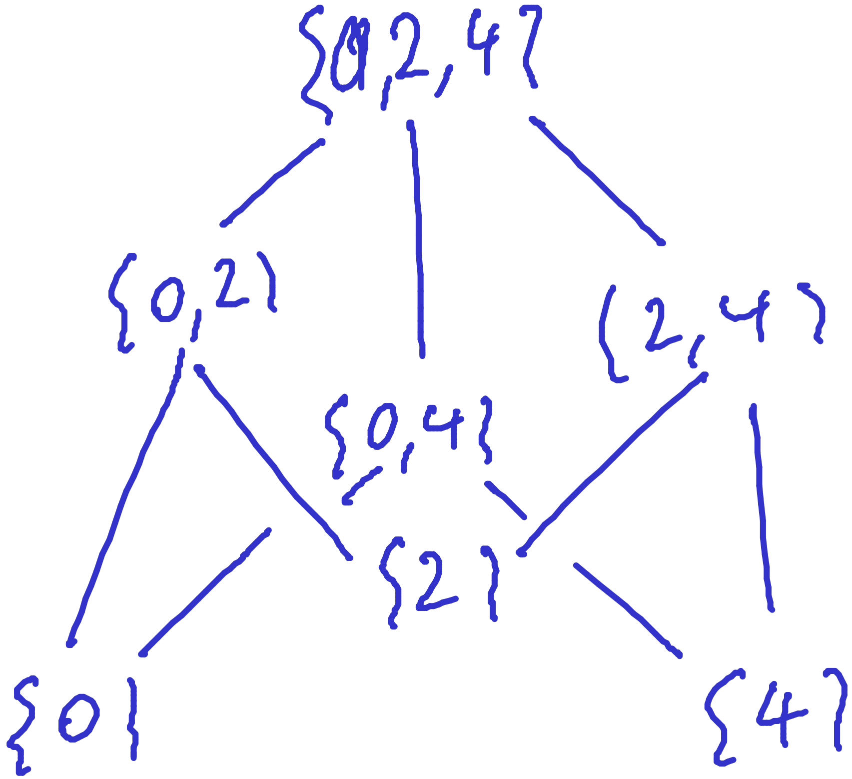
that is, $\mathcal{F}$ is a set of subsets of $\mathcal{U}$, sometimes referred to as a *family*.

$= \{0,1,2,3,4\}$

Example: The family $\mathcal{E} \subseteq \mathcal{P}\big([5]\big)$ consisting of the non-empty subsets of $[5] = \{0, 1, 2, 3, 4\}$ whose elements are even is

$$\mathcal{E} = \big\{ \{0\}, \{2\}, \{4\}, \{0,2\}, \{0,4\}, \{2,4\}, \{0,2,4\} \big\} \ .$$

Hasse diagrams



Proposition 104 *For all finite sets* U,

$$\# \mathcal{P}(U) = 2^{\# U} \quad .$$

PROOF IDEA:

$$\# \mathcal{P}(U) = \# \{ X \mid X \subseteq U \}$$

$$= \sum_{i=0}^{\# U} \underbrace{\# \{ X \mid X \subseteq U \wedge \# X = i \}}_{\binom{\# U}{i}}$$

$$= \sum_{i=0}^{\# U} \binom{\# U}{i} = \sum_{i=0}^{\# U} \binom{\# U}{i} 1^{\# U - i} 1^{i}$$

$$= (1+1)^{\# U} = 2^{\# U} ,$$