# Euclid's infinitude of primes

**Theorem 80** *The set of primes is infinite.*

PROOF: Suppose the set of primes is finite, and let

$p_1, p_2, \ldots, p_N$ be all the primes.

Consider $q = (p_1 \cdot p_2 \cdot \cdots \cdot p_N) + 1$

Since $q$ is not in the list of primes then

there is some prime, say $p_i$, such that $p_i \mid q$

Also $p_i \mid (p_1 \cdots p_N)$. So $p_i \mid [q - (p_1 \text{—} p_N)] = 1$

which is a contradiction. $\otimes$

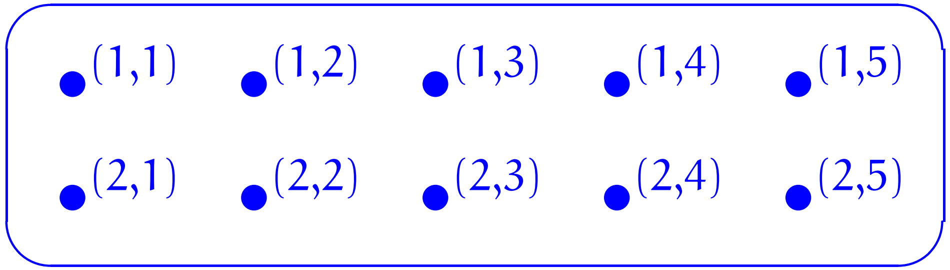
# Sets

# Objectives

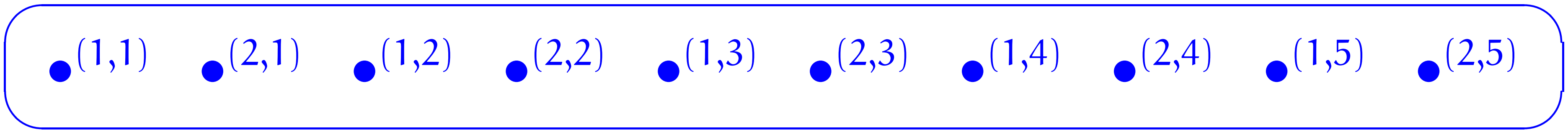
To introduce the basics of the theory of sets and some of its uses.

# Abstract sets

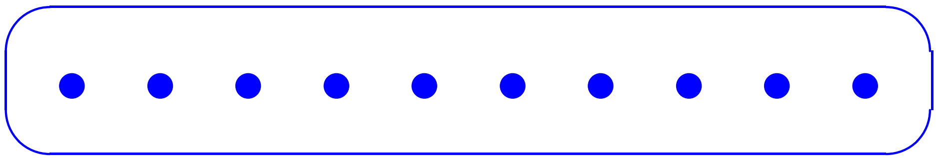
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,




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.

The most important structure of a set is its membership relation ($\in$).

# Extensionality axiom

| Two sets are equal if they have the same elements. |
|---|

Thus,

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

Recall the notation $\{a_1, a_2, \ldots, a_n\}$ is the set whose elements are precisely the $a_i$'s.

**Example:**

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

# Subsets and supersets

We say that $A$ is a subset of $B$, denoted $A \subseteq B$, whenever

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

Also $B$ is a superset of $A$.

**Lemma 83**

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* $A$, $B$, $(A \subseteq B \wedge B \subseteq A) \implies A = B$.

an expression of the extensionality axiom.

# 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.

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

by def $\iff$

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

# Russell's paradox

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

allowing unbounded comprehension

By def

$$\forall X .\ X \in R \Leftrightarrow X \notin X$$

By univ. instantiation

$$R \in R \Leftrightarrow R \notin R$$

Giving inconsistency!

# Empty set

$$\emptyset \quad \text{or} \quad \{\,\}$$

defined by

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

or, equivalently, by

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

# 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:**

$$\#\emptyset = 0$$

## Powerset axiom

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

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

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

| | $\mathcal{P}(\mathcal{U})$ | # |
|---|---|---|
| $\mathcal{U} = \emptyset$ | $\{\emptyset\}$ | 1 |
| $\mathcal{U} = \{1\}$ | $\{\emptyset, \{1\}\}$ | 2 |
| $\mathcal{U} = \{1,2\}$ | $\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ | 4 |

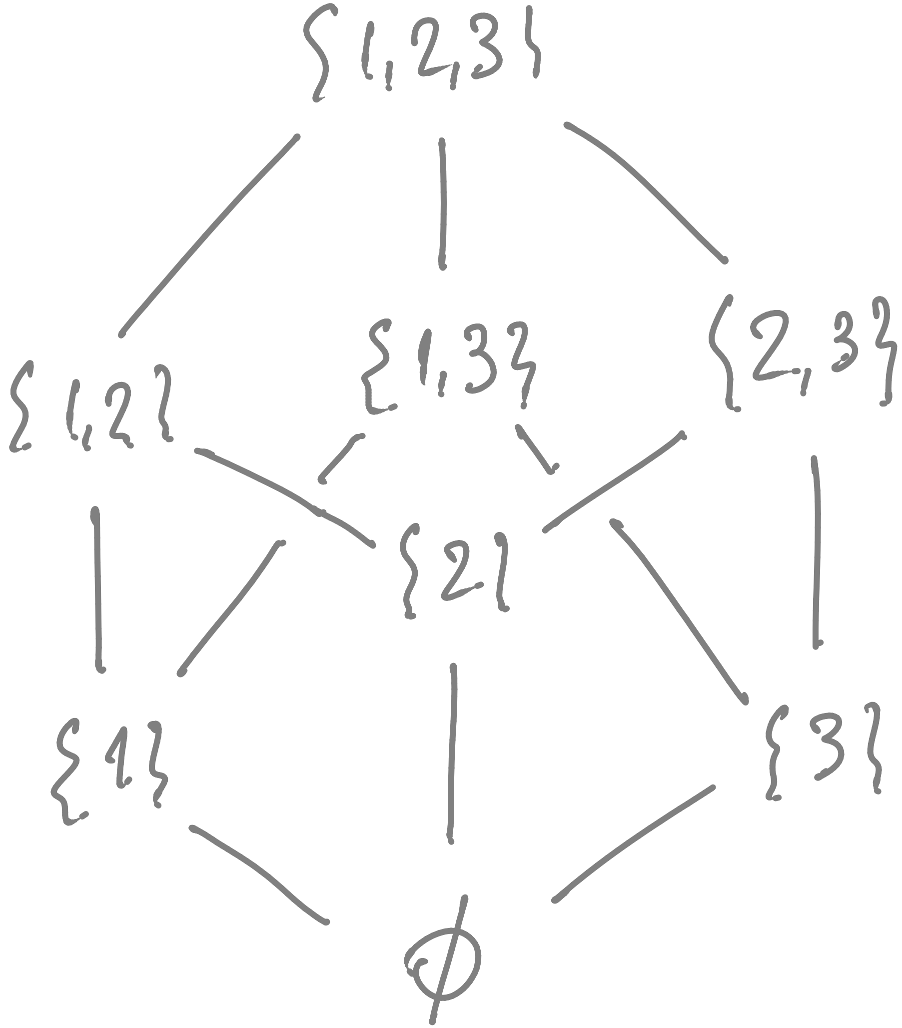
$$\begin{tikzcd} \{1\} \arrow[d, dash] \\ \emptyset \end{tikzcd}$$

$$\begin{tikzcd} & \{1,2\} \arrow[dl, dash] \arrow[dr, dash] & \\ \{1\} \arrow[dr, dash] & & \{2\} \arrow[dl, dash] \\ & \emptyset & \end{tikzcd}$$

$$\# \mathcal{U} = n \Rightarrow \# \mathcal{P}(\mathcal{U}) = ?$$

# Hasse diagrams for $\mathcal{P}(\mathcal{U})$

$\mathcal{U} = \{1, 2, 3\}$



**Proposition 84** *For all finite sets* $U$*,*

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

PROOF IDEA: Let $U$ be a set with $n$ elements, say $u_1, u_2, \ldots, u_n$. We need to count all the subsets of $U$.

E.g. $\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^{i} = (1+1)^{n} = 2^{n}$.

Every subset $S \subseteq U$ can be encoded as a sequence of 0's and 1's of length $n$ with 0 in position $i$ if $u_i \notin S$ and 1 otw.

Eg $S = \{u_1, u_3, u_4, u_n\}$

$$\begin{array}{ccccccc} 1 & 0 & 1 & 1 & 0 & \cdots 0 \cdots & 1 \\ 1 & 2 & 3 & 4 & 5 & \cdots\cdots & n \end{array}$$

So $\# \mathcal{P}(U) =$ The number of sequences of 0's and 1's of length $n$, which is $2^n$. $\boxtimes$