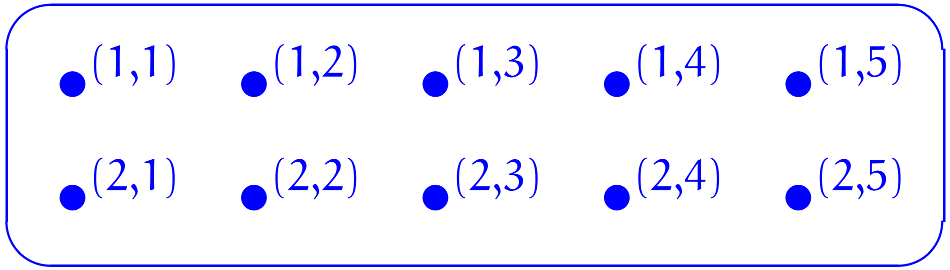
Sets

Objectives

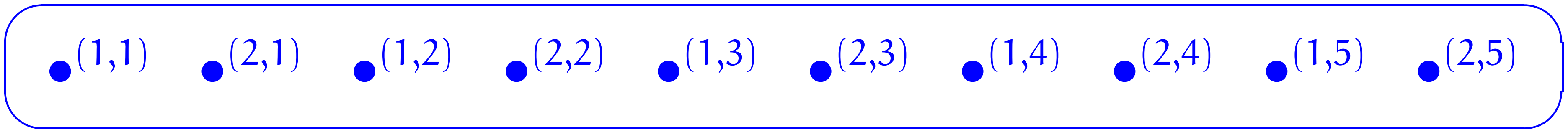
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

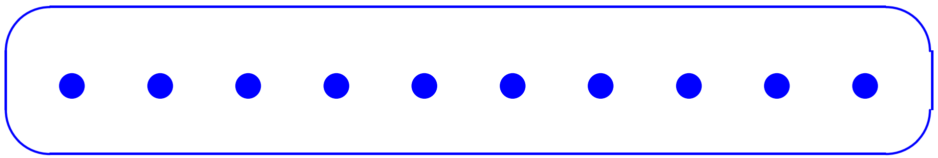
It has been said that a set is like a mental “bag of dots”, except of course that the bag has no shape; thus,



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

$x \in A$ stands for x is an element of A

We further write

$x \notin A$ for $\neg(x \in A)$

Example: $0 \in \{0,1\}$, $1 \notin \{0\}$

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:

because $1 \in \{0,1\}$ and $1 \notin \{0\}$

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

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

$$A \overset{\text{def}}{=} \{ x \in \mathbb{C} \mid x^2 - 2bx + c = 0 \}$$

$$B \overset{\text{def}}{=} \{ b + \sqrt{b^2 - c}, \; b - \sqrt{b^2 - c} \}$$

$$C \overset{\text{def}}{=} \{ b \}$$

Then,

(1) $A = B$,

and

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

(1) $\{x \in \mathbb{C} \mid x^2 - 2bx + c = 0\} \overset{\text{RTP}}{=} \{b + \sqrt{b^2 - c}, b - \sqrt{b^2 - c}\}$

equivalently

$$\forall x \in \mathbb{C}.\ x^2 - 2bx + c = 0 \iff \left(\begin{array}{l} x = b + \sqrt{b^2 - c} \\ \vee \\ x = b - \sqrt{b^2 - c} \end{array} \right).$$

(2) $b^2 = c \iff \{b + \sqrt{b^2 - c}, b - \sqrt{b^2 - c}\} = \{b\}$.

$(\Leftarrow)$ Assume $\{b + \sqrt{b^2 - c}, b - \sqrt{b^2 - c}\} \overset{\text{RTP}}{=} \{b\}$

RTP: $b^2 = c$.

By assumption $b + \sqrt{b^2 - c} = b$ hence $\sqrt{b^2 - c} = 0, \ldots$

$\boxtimes$

Subsets and supersets

$$A \subseteq B$$

A is a subset of B
or
B is a superset of A

iff$_{\text{def}}$

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

<u>NB</u>: $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$

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

Let A, B, C be sets.

Assume ② $A \subseteq B$ and $B \subseteq C$ ④

RTP: $A \subseteq C \iff (\forall x.\ x \in A \Rightarrow x \in C)$

Let x in A ①.

RTP x in C.

By ① and ②, x in B ③

By ③ and ④, $x \in C$.

$\boxtimes$

Proper subsets

We let $A \subset B$ stand for $A \subseteq B \wedge A \neq B$

Hence

$$A \subset B$$

iff

$$(\forall x.\, x \in A \Rightarrow x \in B) \wedge (\exists y.\, y \notin A \wedge y \in B)$$

Example: $\{0\} \subset \{0, 1\}$

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

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

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.

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

NB:

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

is equivalent to

$$\forall z.\, \big[(z \in A) \wedge P(z)\big] \Rightarrow \big[(z \in B) \wedge Q(z)\big]$$

Russell's paradox

$$\mathcal{U} =^{def} \{ x \mid R(x) \} \qquad R(x) =^{def} x \notin x$$

Then

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

for all x.

In particular,

$$\mathcal{U} \in \mathcal{U} \iff \mathcal{U} \notin \mathcal{U}.$$

a contradiction. $\lightning$

Empty set

- The theory provides an empty set, with no elements
- This is,

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

- Indeed, $a \in \emptyset \Leftrightarrow \underline{false}$

That is, $\forall a.\ a \notin \emptyset$

NB: for all sets A and B,

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

NB: for all sets A,

$$\emptyset \subseteq A$$

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:

$$\#\emptyset = 0$$

In particular, $[0] = \{\}$; $[1] = \{0\}$; $[n] = \{0, 1, \ldots, n-1\}$

FINITE SETS

The finite sets are those with cardinality a natural number

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

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

is finite of cardinality n.

Powerset axiom

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

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

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

Example:

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

$$= \{ \emptyset, \qquad 0$$

$$\{x\}, \{y\}, \{z\}, \qquad 1$$

$$\{x,y\}, \{x,z\}, \{y,z\}, \qquad 2$$

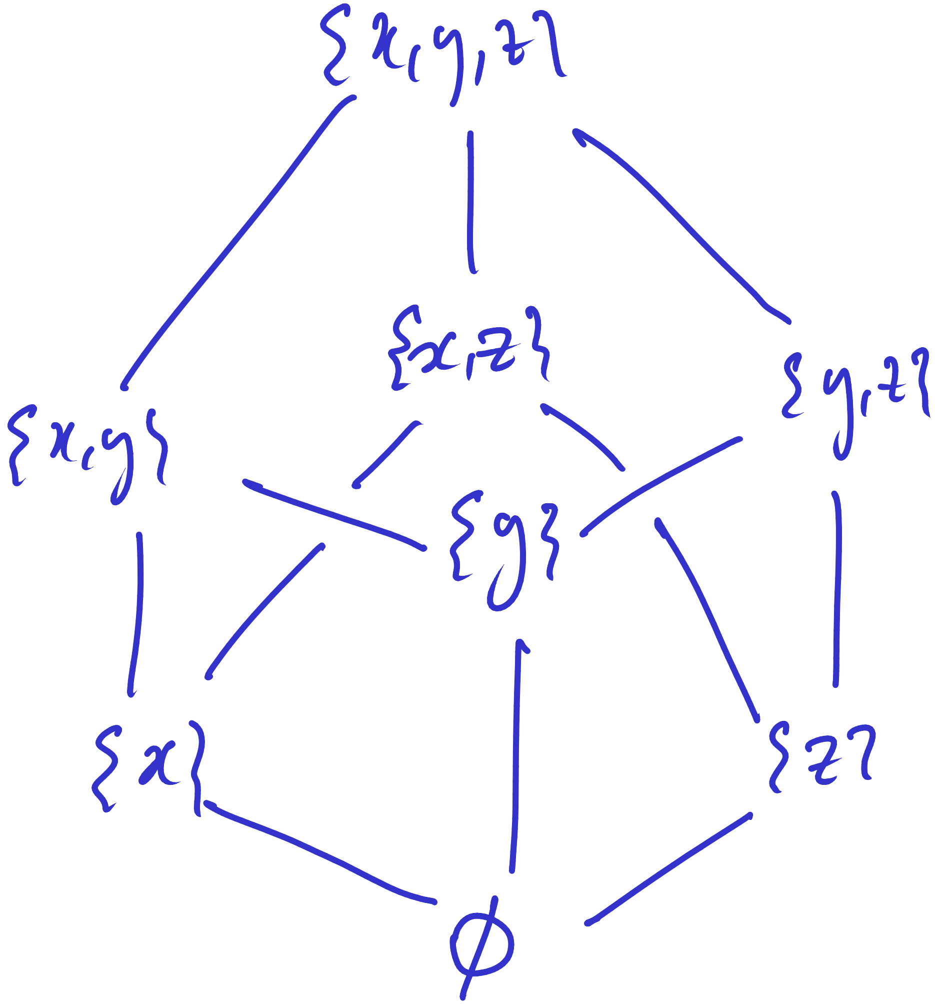
$$\{x,y,z\} \} \qquad 3$$

$$\# \mathcal{P}(\{x,y,z\}) = 8$$

NB: $\emptyset \in \mathcal{P}(\mathcal{U})$ because $\emptyset \subseteq \mathcal{U}$

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

Hasse diagrams



Proposition 84 *For all finite sets* U,

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

PROOF IDEA:

(1) $\# \mathcal{P}(U) = \sum_{k=0}^{\# U} \mathcal{P}^{(k)}(U)$

where $\mathcal{P}^{(k)}(U) = \{ S \subseteq U \mid \# S = k \}$

Since

$\# \mathcal{P}^{(k)}(U) = \binom{\# U}{k}$

$\# \mathcal{P}(U) = \sum_{k=0}^{\# U} \binom{\# U}{k} = (1+1)^{\# U} = 2^{\# U}$

(2) $\# \mathcal{P}([n])$ $\qquad$ $[n] = \{0, 1, \dots, n-1\}$

Consider $S \in \mathcal{P}([n]) \iff S \subseteq [n]$

It may be visualized as

S:

$0 \in S$	$1 \in S$		$\dots$	$(n-1) \in S$
0	1	2	$\dots$	$n-1$

$\emptyset$:

false	false		$\dots$	false
0	1	2	$\dots$	$n-1$

$\mathcal{U}$:

true	true		true.
0	1	$\dots$	$n-1$

To count

$$\#\mathcal{P}([n])$$

is to count the arrays from 0..(n-1) of Booleans. Equivalently it is to count the sequences of 0 & 1's of length n, which is 2^n.

$\boxtimes$

NB: The powerset construction can be iterated.

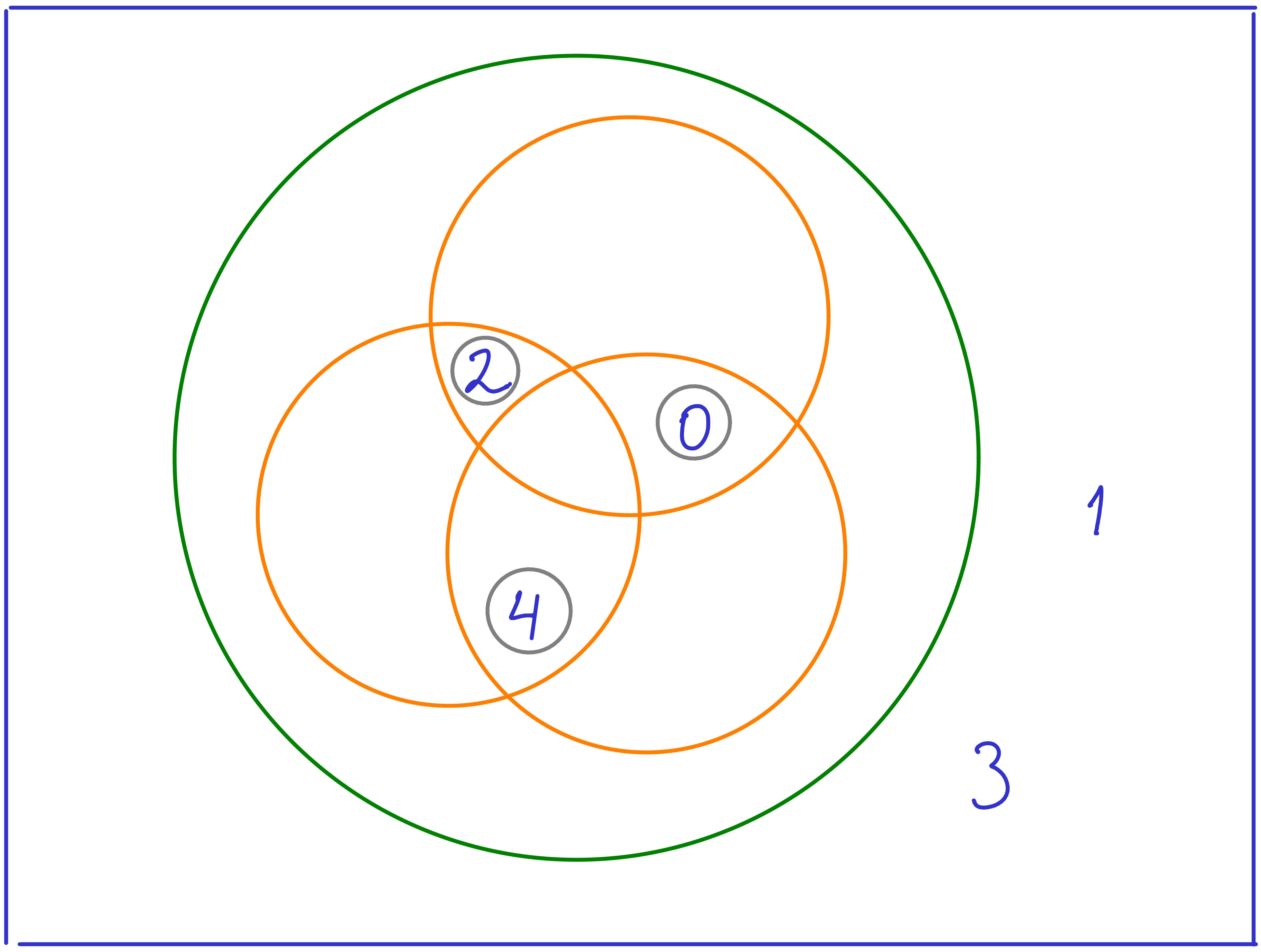
In particular,

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

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

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

$$\mathcal{E} = \Big\{ \{0\}, \{2\}, \{4\}, \\ \{0,2\}, \{0,4\}, \{2,4\}, \\ \{0,2,4\} \Big\}$$


2
0
4
1
3

Exercise: Explicitly describe the family

$\mathcal{S} = \left\{ S \subseteq [5] \;\middle|\; \begin{array}{l}\text{the sum of the elements} \\ \text{of } S \text{ is } 6\end{array} \right\}$

and depict its Hasse and Venn diagrams.