Euclid's infinitude of primes

$\{p_1, \ldots, p_k\}$ $(k \in \mathbb{N})$

Theorem 80 *The set of primes is infinite.*

PROOF: By contradiction suppose there are a finite number of primes. Consider N to be the product of all primes plus 1.

$= (p_1 \cdot p_2 \cdots p_k) + 1$

Since $N > p_i$ for all $i = 1, \ldots, k$

N is not a prime; therefore it is a product of primes.

Let p be a prime such that $p \mid N$. We have

$$p_1 \cdots p_k + 1 = N = p \cdot l \text{ for some } l \in \mathbb{N}$$

Say $p = p_i$ for some i. Hence $p_i \cdot (l - p_1 \cdots p_{i-1} p_{i+1} \cdots p_k) = 1$ $\boxtimes$

Contradiction

Sets

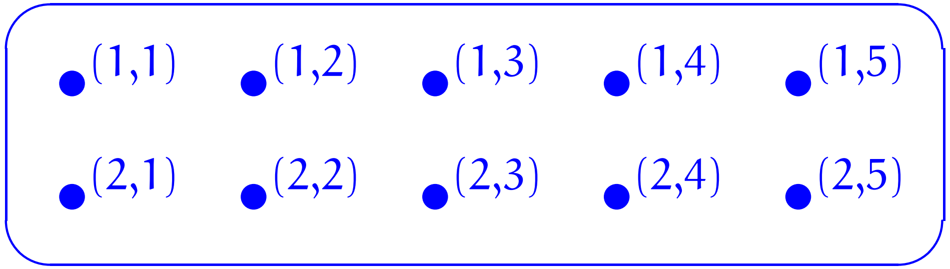
Objectives

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

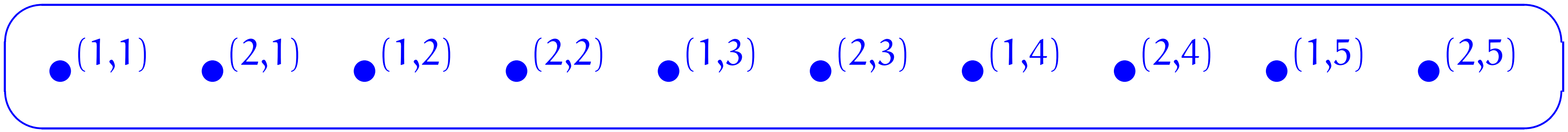
Naive Axiomatic

Abstract sets

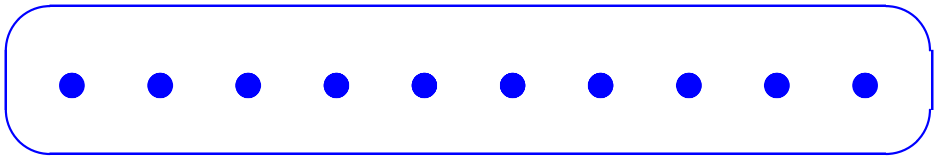
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



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.

Sets — $A, B, \ldots, X, \ldots, \mathcal{U}, \ldots$

Membership relation

$x \in P$

element set

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.

$$A \stackrel{?}{=} B$$

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:

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

Subsets and supersets

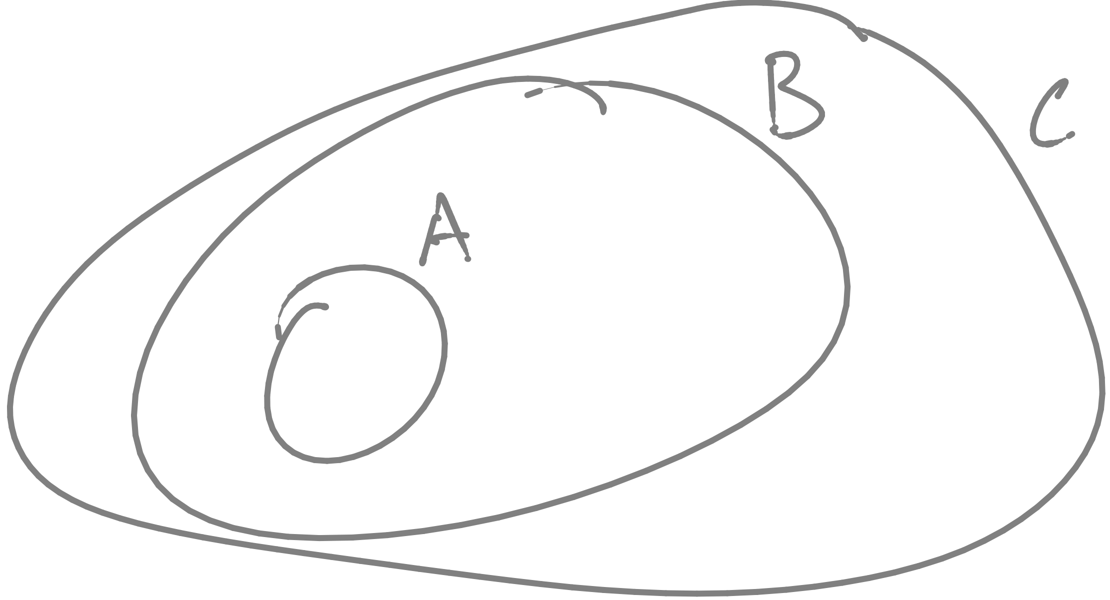
$A \subseteq B$ A a subset of B

$\overset{\Longleftrightarrow}{\text{def}} \ (\forall x.\ x \in A \Rightarrow x \in B)$

B is a superset of A

<u>Claim</u>: $(A \subseteq B \wedge B \subseteq A) \Longleftrightarrow A = B$

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

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.

<u>NB</u> : $\{x \in A \mid P(x)\} \subseteq A$

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

$$\overset{\text{def}}{\iff} [a \in A \wedge P(a)]$$

Russell's paradox

Initially Frege allowed definitions

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

So what about

$$\mathcal{U} = \{x \mid x \notin x\}$$

$\boxed{?}$ $\mathcal{U} \in \mathcal{U} \Leftrightarrow \mathcal{U} \notin \mathcal{U}$. ?

NB: $\emptyset \subseteq X$ for any set X.

Empty set

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

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:

$$\#\emptyset = 0$$

$\mathcal{P}(\emptyset) = \{\emptyset\}$ $\qquad \# \mathcal{P}(\emptyset) = 1$

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

Powerset axiom

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

$\# \mathcal{P}\mathcal{P}\mathcal{P}(\emptyset) = 4$

$\mathcal{P}(U)$

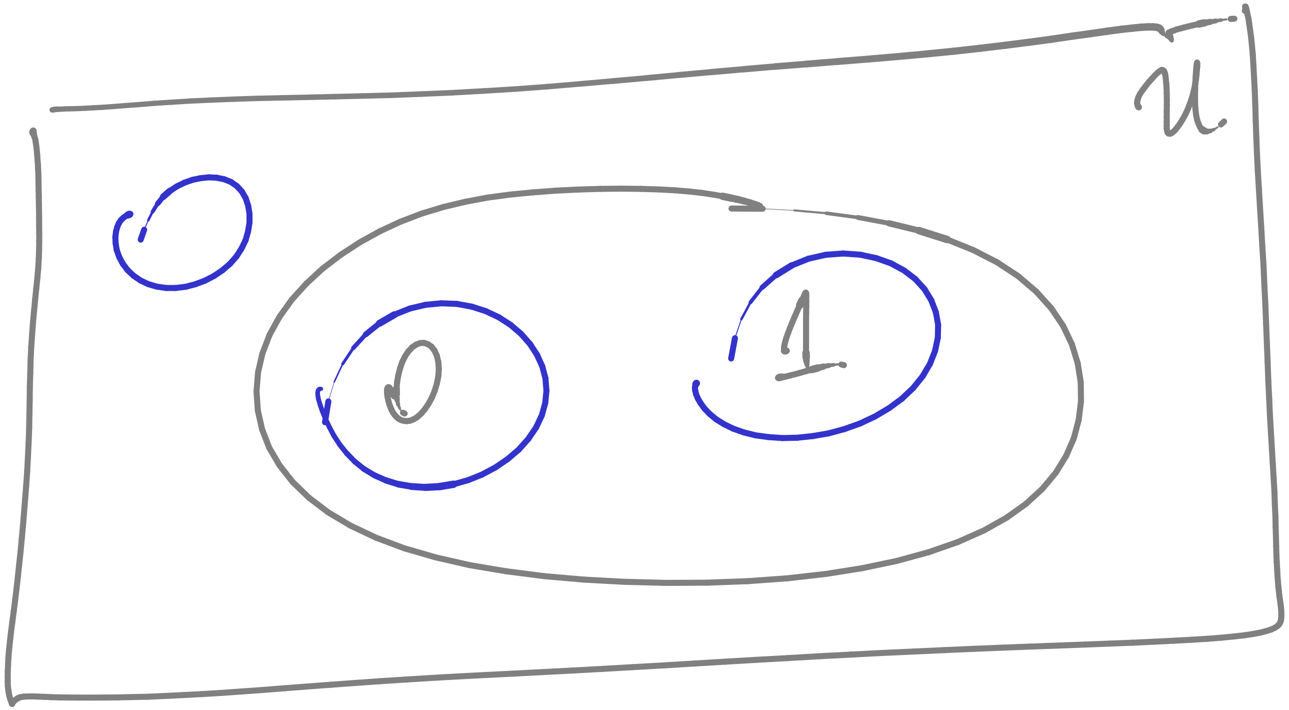
<u>NB</u>: $\emptyset \in \mathcal{P}(U)$

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

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

$S \subseteq \{\emptyset\}$

Hasse diagrams



$$\mathcal{P}\{0,1\} = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}.$$

Proposition 84 *For all finite sets* U,

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

PROOF IDEA: Say $U = \{x_1, x_2, \ldots, x_n\}$ for $n \in \mathbb{N}$

$\underline{\text{RTP}}$ $\#\mathcal{P}(U) = 2^n$.

$$\#\mathcal{P}(U) = \sum_{k=0}^{n} \#\text{subsets of } U \text{ of size } k.$$

$$= \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n. \qquad \boxtimes$$

$$\mathcal{U} = \{x_1, x_2, \dots, x_n\}$$

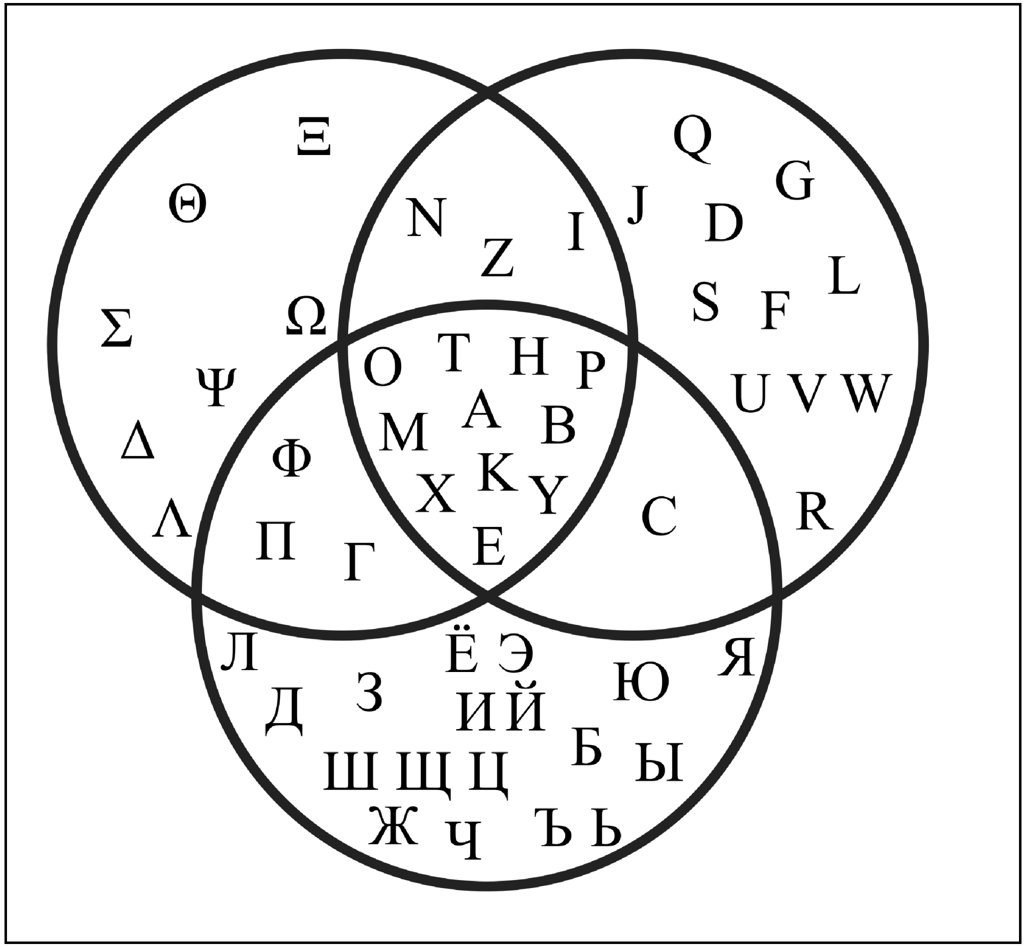
To describe a subset of $\mathcal{U}$, we need to state whether or not each x_i is in the subset. We can do this by decorating each x_i with 0 or 1.

<u>Example</u>

	x_1	x_2	$\cdots$	x_{n-1}	x_n
$\{x_1, x_n\}$	1	0	$\cdots$	0	1
$\{x_1, x_2, \dots, x_n\}$	1	1	$\cdots$	1	1

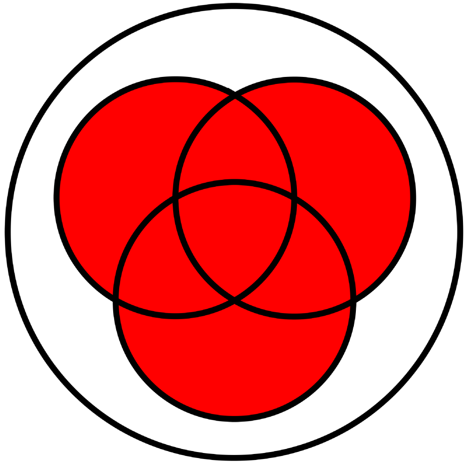
The number of sequences of length n of 0's & 1's is the number of subsets of $\mathcal{U}$, that is, 2^n. $\boxtimes$

Venn diagrams[a]

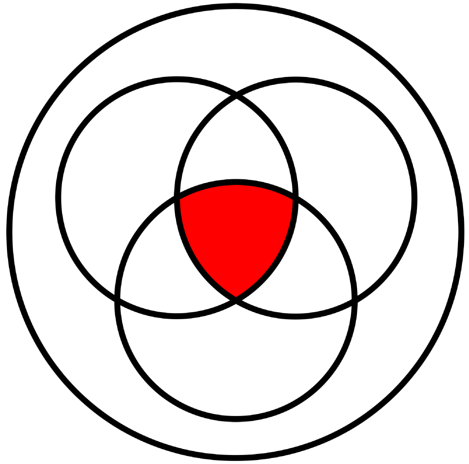


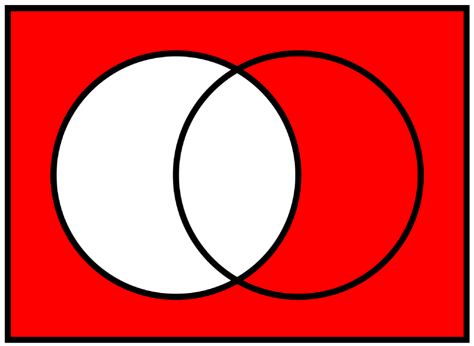
[a]From http://en.wikipedia.org/wiki/Intersection_(set_theory) .

Union



Intersection





Complement

The powerset Boolean algebra

$$\left(\mathcal{P}(U),\ \overbrace{\underset{\text{false}}{\emptyset},\ \underset{\text{true}}{U}}^{\in \mathcal{P}(U)!},\ \cup,\ \cap,\ (\cdot)^c \right)$$

For all $A, B \in \mathcal{P}(U)$,

$$A \cup B = \{x \in U \mid x \in A \lor x \in B\} \in \mathcal{P}(U)$$

$$A \cap B = \{x \in U \mid x \in A \land x \in B\} \in \mathcal{P}(U)$$

$$A^c = \{x \in U \mid \neg(x \in A)\} \in \mathcal{P}(U)$$

cf. $P \vee Q = Q \vee P$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

$$(A \cup B) \cup C = A \cup (B \cup C) \ , \quad A \cup B = B \cup A \ , \quad A \cup A = A$$

$$(A \cap B) \cap C = A \cap (B \cap C) \ , \quad A \cap B = B \cap A \ , \quad A \cap A = A$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

$$(A \cup B) \cup C = A \cup (B \cup C) \ , \quad A \cup B = B \cup A \ , \quad A \cup A = A$$

$$(A \cap B) \cap C = A \cap (B \cap C) \ , \quad A \cap B = B \cap A \ , \quad A \cap A = A$$

- The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* $\mathcal{U}$ is a neutral element for $\cap$.

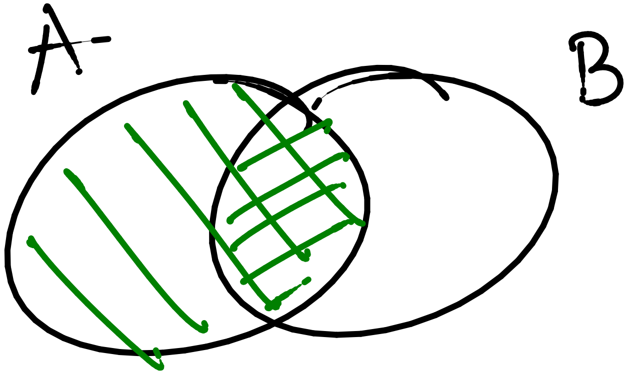
$$\emptyset \cup A \ = \ A \ = \ \mathcal{U} \cap A$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

$$\emptyset \cap A = \emptyset$$

$$\mathcal{U} \cup A = \mathcal{U}$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.



$$\emptyset \cap A = \emptyset$$

$$\mathcal{U} \cup A = \mathcal{U}$$

$\underline{NB}$ $S \subseteq A$

$\Rightarrow A \cup S = A$

$A \cap B \subseteq A$

- With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are distributive and absorptive.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad , \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$P \vee (P \wedge Q) = P$

$$A \cup (A \cap B) = A = A \cap (A \cup B)$$

- The complement operation $(\cdot)^{c}$ satisfies complementation laws.

$$A \cup A^{c} = \mathcal{U} \ , \quad A \cap A^{c} = \emptyset$$