Euclid’s infinitude of primes

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.

\[
N = (p_1 \cdot p_2 \cdots p_k) + 1
\]

Since \( N > p_i \) for all \( i \in \{1, \ldots, k\} \), \( N \) is not a prime. There fore it is a product of primes. Let \( p \) be a prime such that \( p \mid N \). We have

\[
p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1 = N = p \cdot l \text{ for some } l \in \mathbb{Z}
\]

Say \( p = p_i \) for some \( i \). Hence \( p_i \cdot (l - p_1 \cdot p_2 \cdot \cdots \cdot p_{i-1} - p_{i+1} \cdots p_k) = 1 \).
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,

\[
\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5)
\end{array}
\]

may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as

\[
\begin{array}{cccccccc}
(1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) & (1,4) & (2,4) & (1,5) & (2,5)
\end{array}
\]

or even simply as

\[
\begin{array}{cccccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet
\end{array}
\]

for other considerations.
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.

\[ A = B \]
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:

\[ \{0\} \neq \{0, 1\} = \{1, 0\} \neq \{2\} = \{2, 2\} \]
Subsets and supersets

\( A \subseteq B \quad \text{A a subset of B} \)

\( \iff \quad (\forall x. x \in A \Rightarrow x \in B) \)

\( \text{B is a superset of A} \)

Claim: \( (A \subseteq B \land B \subseteq A) \iff A = B \)
Lemma 83

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 \(A, B, (A \subseteq B \land B \subseteq A) \implies A = B\).
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.

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

$\forall x \in A \mid P(x)$

$\exists a \in A \mid P(a)$

$\exists a \in \{ x \in A \mid P(x) \}$
Russell’s paradox

Initially, Frege allowed definitions

\[ \{ x \mid P(x) \} \]

so what about

\[ U = \{ x \mid x \notin x \} \]

? \[ \forall U \ (U \notin U \leftrightarrow U \notin U) \]?
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

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

\[
\begin{align*}
P(\emptyset) &= \{ \emptyset \} & \# P(\emptyset) &= 1 \\
P(P(\emptyset)) &= P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} & \# P(P(\emptyset)) &= 2
\end{align*}
\]

\[
\forall X. X \in P(U) \iff X \subseteq U.
\]

\[
S \subseteq \{\emptyset\}
\]
Hasse diagrams

\[ \mathcal{P}\{0,1\} = \{\emptyset, \{0\}, \{1\}, \{0,1\} \} . \]
Proposition 84  For all finite sets \( \mathbb{U} \),

\[
\# \mathcal{P}(\mathbb{U}) = 2^{\# \mathbb{U}}.
\]

**Proof Idea:** Say \( \mathbb{U} = \{x_1, x_2, \ldots, x_n\} \) for \( n \in \mathbb{N} \).

\[
\# \mathcal{P}(\mathbb{U}) = 2^n.
\]

\[
\# \mathcal{P}(\mathbb{U}) = \sum_{k=0}^{n} \# \text{subset of } \mathbb{U} \text{ of size } k.
\]

\[
= \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.
\]

\[\Box\]
\[ U = \{ x_1, x_2, \ldots, x_n \} \]

To describe a subset of \( U \), 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.

**Example**

\[
\begin{align*}
\{ x_1, x_n \} & \quad 1 \quad 0 \quad \cdots \quad 0 \quad 1 \\
\{ x_1, x_2, \ldots, x_n \} & \quad 1 \quad 1 \quad \cdots \quad 1 \quad 1
\end{align*}
\]

The number of sequences of length \( n \) of 0's and 1's is the number of subsets of \( U \), that is, \( 2^n \).
Venn diagrams


---

The powerset Boolean algebra

\[ ( \mathcal{P}(\mathcal{U}), \emptyset, \cup, \cap, (\cdot)^c ) \]

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

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

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

\[ A^c = \{ x \in \mathcal{U} \mid \neg(x \in A) \} \in \mathcal{P}(\mathcal{U}) \]
The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

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

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

cf. $p \lor q = q \lor p$
The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

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

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

The empty set $\emptyset$ is a neutral element for $\cup$ and the universal set $U$ is a neutral element for $\cap$.

$$\emptyset \cup A = A = U \cap A$$
The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $U$ is an annihilator for $\cup$.

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

$$U \cup A = U$$
The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $U$ is an annihilator for $\cup$.

\[ \emptyset \cap A = \emptyset \]
\[ U \cup A = U \]

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

\[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \]
\[ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \]

\[ P \lor (P \land Q) = P \]
\[ A \cup (A \cap B) = A = A \cap (A \cup B) \]
The complement operation \((\cdot)^c\) satisfies complementation laws.

\[ A \cup A^c = U, \quad A \cap A^c = \emptyset \]