Logic and proofs

- Reading assignment:
  - Ch1: 1.1, 1.3, 1.4, 1.5, 1.7, 1.8.
  - Ch2: 2.1, Russel's paradox (p.133, exercise 50), 2.2.

Propositional logic

- Propositions: "sentences", which are either true or false

Logic operations: Let P and Q be two propositions.

- AND ($\wedge$): ($P \wedge Q$) is true if both P and Q are true.

- OR ($\vee$): ($P \vee Q$) is true if any of P and Q is true.

- NOT ($\neg$): $\neg P$ is true if P is false.

Logic operations

- Implication ($\Longrightarrow$): P$\Longrightarrow$Q is true if P is false or (P$\wedge$Q) is true.
  - If P is true, then Q is true. (若 P 則 Q)
  - Q is the necessary condition of P. (Q 為 P 的必要條件)
  - P is the sufficient condition of Q. (P 為 Q 的充分條件)
- Equivalence ($\Longleftrightarrow$): P$\Longleftrightarrow$Q is true if both (P$\Longrightarrow$Q) and (Q$\Longrightarrow$P) are true.
  - P if and only if Q (P iff Q, P 若且唯若 Q)
  - P is equivalent to Q (P 和 Q 等價)
  - Q is the necessary and sufficient condition of P (Q 為 P 的充分必要條件)

Predicate logic

- Predicate (述語): a sentence that contains a variable.
  - The truth value varies depending on the the variables.
  - e.g. $x < 10$.
- Quantifier
  - universal quantifier ($\forall \rightarrow$ for all)
  - existential quantifier ($\exists \rightarrow$ there exists some)
  - compare: $\forall x \in \mathbb{N}\ (x < 10) \quad \leftrightarrow \quad \exists x \in \mathbb{N}\ (x < 10)$

Proposition. Let n be an integer. If n is an odd number, then n^2 is also odd.

Proof:

- Since n is odd, there exists an integer k such that $n = 2k + 1$.
- Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$, which is an odd number. ∎

Proposition. Let n be an integer. If n^2 is an odd number, then n is also odd.

Proof:

Truth table

P	Q	$P \implies Q$	$\neg Q \implies \neg P$	$\neg P \implies \neg Q$	$\neg P \vee Q$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Proposition. Let n be an integer. If n^2 is an odd number, then n is also odd.

Proof: (by contraposition)

- We prove "If n is even, then n^2 is even."
- Since n is even, there exists an integer k such that $n = 2k$.
- Then, $n^2 = (2k)^2 = 4k^2$, which is even. ∎

Proof strategies (to prove $P \implies Q$)

- Direct proof
- Proof by contraposition $(\neg Q \implies \neg P)$
- Proof by contradiction (反證法)
  - To prove that a statement R is true, first assume that $\neg R$ is true.
  - We look for a statement L such that
    - $\underbrace{(\neg R \wedge \ldots)}_{\text{premise}} \implies L$ is true, and $\underbrace{(\neg R \wedge \ldots)}_{\text{premise}} \implies \neg L$ is true.
  - This implies that the premise is false, and the only statement that can be false is $\neg R$.

Proposition. $\sqrt{2}$ is irrational.

Proof: (by contradiction)

- Suppose to the contrary that $\sqrt{2}$ is rational.
  - Namely, $\sqrt{2} = \frac{a}{b}$ for some positive integers a and b, with $b \neq 0$.
  - We may assume that $\gcd(a, b) = 1$.
- It follows that $a^2 = 2b^2$.
  - Thus, a is even. There exists an integer c such that $a = 2c$.
- Since $a^2 = 2b^2$, we have $4c^2 = 2b^2$. So b is even.
- Since both a and b are even, we have $\gcd(a, b) \geq 2$, which contradicts that $\gcd(a, b) = 1$. ∎

Proposition. Show that there exists irrational numbers x and y such that x^y is rational.

Proof:

- Let $x = y = \sqrt{2}$.

- If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have the requested numbers.

- Otherwise, let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{2} = 2$. ∎

Set

- the 1st paper is given by Cantor at 1874. (the beginning of set theory)
- Set representation:
  - roster method (listing all elements in the set): e.g., {a, b, c, d, e}
  - set comprehension: S = {x | x has property P}
    - S is the set of all elements x such that x has property P.
    - e.g., $S = \{x \in \mathbb{N} \mid 0 < x < 5\}$

- Set serves as the primitive concept of most fields (in mathematics).
  - Gottlob Frege 1900s
  - Bertrand Russell
    - Russell's paradox: Let $S = \{X \mid X \text{ is a set and } X \notin X\}$.
    - Question: Is $S \in S$ or $S \notin S$?