Week 3-4

1 Statements

A **mathematical statement** (or **sentence** or **proposition**) is a declarative sentence that is either true or false, but not both. The **truth value** (true, false) for any statement can be determined and is not ambiguous in any sense. The true value is denoted by T and the false value is denoted by F. We also use **1** and **0** to denote T and F respectively.

Example 1.1.

- Today is 1st of July 1997.
- Math2343 of HKUST has midterm and final exams.
- There are exactly 7,523,804 people in Hong Kong.
- John is married and Mary is divorced.
- If John is divorced then Mary is married.
- $x^2 + y^2 = z^2$ has no solution for $x, y \in \mathbb{Z}$.

Example 1.2.

- How are you?
- Hong Kong is a big city.
- What a beautiful campus!
- Why mathematics is not fun?

Statements are usually denoted by lowercase letters such as p, q, r, $\ldots$, etc.

2 Connectives

We wish to set up rules by which we can decide the truth of various combinations of some given statements. New statements can be formed by using connectives ‘not’, ‘and’, ‘or’, ‘implies’, and ‘if and only if’. Statements obtained by connectives are called **compound sentences** or **compound statements.**

The **Negation** of a statement p is the statement "not p," written $\neg p$. The truth values of $\neg p$ are given by the table

p	$\neg p$
T	F
F	T

The **conjunction** of statements p and q is the statement "p and q," written $p \wedge q$. Its truth values are given by

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

The **disjunction** of statements p and q is the statement "p or q," written $p \vee q$. Its truth table is given by

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 2.1. Consider the statements

$$\begin{aligned} p &: \textit{ It is raining.} \\ q &: \textit{ I go to school.} \end{aligned}$$

Then

$$\begin{aligned} \neg p &: \quad \textit{It is not raining.} \\ p \wedge q &: \quad \textit{It is raining and I go to school.} \\ p \vee q &: \quad \textit{It is raining or I go to school.} \end{aligned}$$

The **conditional implication** from a statement p to a statement q is the statement "if p, then q", read "p implies q". The statement p is called the **hypothesis** of the implication and q the **conclusion**. The statement is denoted by $p \rightarrow q$; its truth table is defined by

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Whenever p is false, the implication is irrelevant and the argument is valid for any conclusion, thus it was assigned the true value T.

The truth of $p \rightarrow q$ is sometimes described by saying that p is a **sufficient condition** for q or that q is a **necessary condition** for p.

Example 2.2. Consider the statements

p : *It is a week day.*
q : *I go to school.*

Then

$p \rightarrow q$: *If it is a week day, then I go to school.*

Let us try to understand with this example why the truth table of $p \rightarrow q$ is defined above. Suppose it is a week day and I did go to school; there is nothing wrong; so the statement $p \rightarrow q$ is specified the true value T. Suppose it is a week day and I did not go to school; then there is something wrong; so the statement $p \rightarrow q$ is specified the false value F. However, suppose it is not a week day (say weekend or holiday); then I don't need go to school, so it is all right either I go to school or I don't go to school; thus the statement $p \rightarrow q$ is specified the true value T.

The **Biconditional Implication** of statements p and q is the statement $(p \rightarrow q) \wedge (q \rightarrow p)$. Since this compound sentence is important, we introduce a new symbol $p \leftrightarrow q$ to denote the statement, read "p if and only if q". Its truth values are given by

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Sometimes we say that q is a **necessary and sufficient condition** of p.

The **converse** of $p \to q$ is the statement

$$q \to p.$$

The **inverse** of $p \to q$ is the statement

$$\neg p \to \neg q.$$

The **contrapositive** of $p \to q$ is the statement

$$\neg q \to \neg p.$$

Example 2.3. Consider the statements

p :	*I am thinking.*
q :	*I am alive.*
$p \to q$:	*If I am thinking, then I am alive.*
$q \to p$:	*If I am alive, then I am thinking.*
$\neg p \to \neg q$:	*If I am not thinking, then I am not alive.*
$\neg q \to \neg p$:	*If I am not alive, then I am not thinking.*

Remark. Consider the two statements

"If $a = 1$, then $\frac{a}{2} = 0.5$" and *"If $a \neq 1$, then $\frac{a}{2} = 0.5$"*.

We assume presumably that a is a real number. Let us denote "$a = 1$" by p and "$\frac{a}{2} = 0.5$" by q. Then "$a \neq 1$" is denoted by $\neg p$. In notations,

$$p : a = 1; \quad q : \frac{a}{2} = 0.5; \quad \neg p : a \neq 1.$$

The sentence *"If $a = 1$, then $\frac{a}{2} = 0.5$"* becomes $p \to q$. The implication $\neg p \to q$ means the sentence *"If $a \neq 1$, then $\frac{a}{2} = 0.5$"*.

Now when the statement $a = 1$ has T value, then $a \neq 1$ has F value. Hence by definition of implication →, the statement *"If $a \neq 1$, then $\frac{a}{2} = 0.5$"* has T value. For instance, let $a = 2$, we see that the sentence

"If $2 \neq 1$, then $\frac{2}{2} = 0.5$"

has T value, which seems nonsense. Can we explain what's wrong here?

Discussion: (I) When the sentence "$a = 1$" has T value, it means that a is the integer 1. So $\neg p$ is "$1 \neq 1$." This sentence has F value. So it is OK that the sentence *"If* $1 \neq 1$*, then* $\frac{1}{2} = 0.5$*"* has T value. When the sentence "$a = 1$" has F value, it means that a is not equal to 1, say, $a = 2$. Then "$2 = 1$" has F value. By definition of implication, it is OK that the sentence *"If* $2 = 1$*, then* $\frac{2}{2} = 0.5$*"* has T value. The argument is still OK. In any case there is no logical consequence that the sentence *"If* $2 \neq 1$*, then* $\frac{2}{2} = 0.5$*"* has T value in practice.

(II) Consider the sentence *"If* $2 \neq 1$*, then* $\frac{2}{2} = 0.5$*"* itself, regardless of the first sentence. When "$2 \neq 1$" is given T value (of course, this is the fact of our world), there are two situations. (i) "$\frac{2}{2} = 0.5$" has the value F, then the implication is given F value by definition; then the definition of implication is justified. (ii) "$\frac{2}{2} = 0.5$" has the value T, which is actually not the fact in our world, then the implication is given T value by definition; the T value of the implication is problematic because it is assumed that "$1 = 0.5$" has T value, which is already problematic.

However, when "$2 \neq 1$" is given F value, that is, "$2 = 1$" (of course, this is not the fact of our world; this is obviously wrong), no matter what value is given to "$\frac{2}{2} = 0.5$," the implication is given T value. The definition of implication is justified because based on a wrong fact we assume automatically that the argument is still valid when a correct or incorrect conclusion is deduced.

3 Quantifiers

Sometimes we need to consider a family of statements $P(x)$ indexed by a variable x. Such a statement form indexed by a variable is called a **predicate**. There are two quantifiers, the **universal quantifier** $\forall$ and the **existential quantifier** $\exists$.

The **universal quantification** of a predicate $P(x)$, written $\forall x\ P(x)$, is the statement

For all values of x*,* $P(x)$ *is true.*

The statement "$\forall x\, P(x)$" has the true value T when all statements $P(x)$ have the true value T, and "$\forall x\ P(x)$" has the false value F when one of $P(x)$ has the false value F.

Example 3.1. Let

$$P(x) : x + 1 < 4, \textit{ where } x \textit{ are real numbers.}$$

The statement

$$\forall x \in \mathbb{R}, P(x)$$

has the false value F because $P(4)$ is not a true statement.

Let

$$Q(x) : x(x-1) \textit{ is even, where } x \in \mathbb{Z}.$$

The statement

$$\forall x \in \mathbb{Z}, Q(x)$$

has the true value T.

Example 3.2. Let

$$\begin{aligned} P(a,b,n) :&\ \ a \equiv b \bmod n, & a,b \in \mathbb{Z}, n \in \mathbb{P} \\ Q(a,b,c,n) :&\ \ ca \equiv cb \bmod n, & a,b,c \in \mathbb{Z}, n \in \mathbb{P} \end{aligned}$$

Then the statement

$$\big(\forall a,b \in \mathbb{Z}, n \in \mathbb{P}, P(a,b,n)\big) \to \big(\forall a,b,c \in \mathbb{Z}, n \in \mathbb{P}, Q(a,b,c,n)\big)$$

means the ordinary statement:

If for arbitrary integers a, b and a positive integer n,

$$a \equiv b \bmod n$$

is valid, then for any integers a, b, c and a positive integer n, we have

$$ca \equiv cb \bmod n.$$

The **existential quantification** of a predicate $P(x)$, written $\exists x\, P(x)$, is the statement

There exists a value of x such that $P(x)$ is true.

The statement "$\exists x\, P(x)$" has the true value T when there is at least one x such that $P(x)$ has the true value T, and "$\exists x\, P(x)$" has the false value F when all statements $P(x)$ have the false value F.

Example 3.3. Let

$$P(x, y, z) : x^2 + y^2 = z^2,\ x, y, z \in \mathbb{R}$$

Then the statement

$$\exists x \exists y \exists z\, P(x, y, z)$$

has the true value T because $P(3, 4, 5)$ is a true statement. We often write $\exists x \exists y \exists z\, P(x, y, z)$ as

$$\exists x, y, z \in \mathbb{R}, P(x, y, z).$$

Example 3.4. Let

$$Q(a, b, x, y) :\ \gcd(a, b) = ax + by,\ a, b, x, y \in \mathbb{Z}, (a, b) \neq (0, 0).$$

Then the statement

$$\forall a, b \in \mathbb{Z}, (a, b) \neq (0, 0), \exists x, y \in \mathbb{Z}, Q(a, b, x, y)$$

means the ordinary statement:

For arbitrary integers a and b, not all zero, there exist integers x, y such that

$$\gcd(a, b) = ax + by.$$

4 Tautology

A statement (compound sentence) is called a **tautology** if it always has the true value for all possible truth values of its propositional variables (simple sentences).

A statement is called a **contradiction** if it always has the false value.

A statement is called a **contingency** if it can be either true or false, depending on the truth values of its propositional variables.

Example 4.1. $p \vee \neg p$ and $(p \rightarrow q) \vee \neg q$ are tautologies.

$(p \rightarrow q) \wedge p \wedge \neg q$ is a contradiction.

$(p \rightarrow q) \vee \neg p$ is a contingency.

Definition 4.1. For statements p and q, if $p \leftrightarrow q$ is a tautology, we say that p and q are **logically equivalent** or simply **equivalent**, written

$$p \Leftrightarrow q.$$

If $p \to q$ is a tautology, we write $p \Rightarrow q$, and say that p **logically implies** q. Indeed, when p has T value we must have that q has T value too.

Proposition 4.2. *For statements p, q, r,*

(1) $p \wedge q \Leftrightarrow q \wedge p$

(2) $p \vee q \Leftrightarrow q \vee p$

(3) $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$

(4) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

(5) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

(6) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

(7) $p \wedge p \Leftrightarrow p$

(8) $p \vee p \Leftrightarrow p$

(9) $\neg(\neg p) \Leftrightarrow p$

(10) $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

(11) $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

Proposition 4.3. *For arbitrary sets A, B, C of a universal set U,*

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

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

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

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

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

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

(7) $A \cap A = A$

(8) $A \cup A = A$

(9) $\overline{\overline{A}} = A$

(10) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

(11) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Example 4.2. Let U be a universal set and A a subset of U. Let p be a statement. Then U corresponds to $\mathbf{1}$ (tautology), the empty set $\varnothing$ corresponds to $\mathbf{0}$ (contradiction), and

$$\begin{array}{rl} A \cap U = A & \text{corresponds to } \; p \wedge \mathbf{1} = p \\ A \cap \varnothing = \varnothing & \text{corresponds to } \; p \wedge \mathbf{0} = \mathbf{0} \\ A \cup U = U & \text{corresponds to } \; p \vee \mathbf{1} = \mathbf{1} \\ A \cup \varnothing = A & \text{corresponds to } \; p \vee \mathbf{0} = p \end{array}$$

Example 4.3. $(p \to q) \leftrightarrow (\neg p) \vee q$ is a tautology, that is,

$$p \to q \Leftrightarrow \neg p \vee q$$

p	q	$p \to q$	$\neg p$	$\neg p \vee q$	$(p \to q) \leftrightarrow (\neg p \vee q)$
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

$$\begin{array}{rl} p \to q & \text{corresponds to } \; A \subset B. \\ \neg p \vee q & \text{corresponds to } \; \overline{A} \cup B. \end{array}$$

This means that the statement

"if x belongs to A then x belongs to B"

is logically equivalent to the statement

"(an element) x belongs to $\overline{A} \cup B$".

Example 4.4. $(p \to q) \leftrightarrow (\neg q \to \neg p)$ is a tautology, that is,

$$p \to q \Leftrightarrow \neg q \to \neg p$$

p	q	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$	$(p \to q) \leftrightarrow (\neg q \to \neg p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Using set notations it means that

$$\overline{A} \cup B = \overline{\overline{B}} \cup \overline{A}.$$

Example 4.5. $(p \leftrightarrow q) \leftrightarrow (p \to q) \wedge (q \to p)$ is a tautology, that is,

$$p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$$

In set notations, $p \leftrightarrow q$ corresponds to $A = B$. Note that

$$(\overline{A} \cup B) \cap (\overline{B} \cup A) = \overline{A \cup B} \cup (A \cap B).$$

This means that $A = B$ is logically equivalent to

if x belongs to $A \cup B$ then x belongs $A \cap B$.

We also easily obtain

$$p \leftrightarrow q \Leftrightarrow (\neg p \vee q) \wedge (\neg q \vee p) \Leftrightarrow \neg(p \vee q) \vee (p \wedge q).$$

Example 4.6. Consider the statement

If I went to class Math2343, then I was in HKUST $(p \to q)$.

One may feel that this statement is logically equivalent to

If I wasn't in HKUST, then I didn't go to class Math2343 $(\neg q \to \neg p)$.

It is also logically equivalent to

I didn't go to class Math2343 or I was in HKUST $(\neg p \vee q)$.

It is less popular to say so in daily life.

Theorem 4.4. *1.* $\neg(\forall x\, P(x)) \Leftrightarrow \exists x\, \neg P(x)$

2. $\neg(\exists x\, P(x)) \Leftrightarrow \forall x\, \neg P(x)$

3. $\forall x\;\; P(x) \wedge Q(x) \Leftrightarrow (\forall x\, P(x)) \,\wedge\, (\forall x\, Q(x))$

4. $\exists x\;\; P(x) \vee Q(x) \Leftrightarrow (\exists x\, P(x)) \,\vee\, (\exists x\, Q(x))$

5. $(\forall x\, P(x)) \,\vee\, (\forall x\, Q(x)) \Rightarrow \forall x\;\; P(x) \vee Q(x)$

6. $\exists x\;\; P(x) \wedge Q(x) \Rightarrow (\exists x\, P(x)) \wedge\, (\exists x\, Q(x))$

7. $(\exists x\, P(x)) \rightarrow (\forall x\, Q(x)) \Rightarrow \forall x\;\; P(x) \rightarrow Q(x)$

8. $\exists x\;\; P(x) \rightarrow Q(x) \Leftrightarrow (\forall x\, P(x)) \rightarrow (\exists x\, Q(x))$

Proof. (1) Let $\neg(\forall x\, P(x)) = T$. Then $(\forall x\, P(x)) = F$. By definition, there exists an x such that $P(x) = F$, i.e., there exists an x such that $\neg P(x) = T$. So by definition again, $(\exists x\, \neg P(x)) = T$.

On the other hand, let $\neg(\forall x\, P(x)) = F$. Then $(\forall x\, P(x)) = T$. By definition, $P(x) = T$ for all x, i.e., $\neg P(x) = F$ for all x. By definition, we have $(\exists x\, \neg P(x)) = F$.

(2) Let $Q(x) = \neg P(x)$. Then $P(x) = \neg Q(x)$. Thus

$$\begin{aligned} \neg(\exists x\, P(x)) &\Leftrightarrow \neg(\exists x\, \neg Q(x)) \overset{(1)}{\Leftrightarrow} \forall x\, \neg\neg Q(x) \\ &\Leftrightarrow \forall x\, Q(x) \Leftrightarrow \forall x\, \neg P(x). \end{aligned}$$

(3) Let $(\forall x\;\; P(x) \wedge Q(x)) = T$. Then $P(x) = Q(x) = T$ for all x. Thus $(\forall x\, P(x)) = T$ and $(\forall x\, Q(x)) = T$. Therefore $(\forall x\, P(x)) \wedge (\forall x\, Q(x)) = T$.

On the other hand, let $(\forall x\;\; P(x) \wedge Q(x)) = F$. Then there exists an x such that either $P(x) = F$ or $Q(x) = F$. Thus by definition, $(\forall x\, P(x)) = F$ or $(\forall x\, Q(x)) = F$. Therefore $(\forall x\, P(x)) \wedge (\forall x\, Q(x)) = F$.

(4) Let $R(x) = \neg P(x)$, $S(x) = \neg Q(x)$. Then $P(x) = \neg R(x)$, $Q(x) = \neg S(x)$. Thus

$$\begin{aligned} \exists x\;\; P(x) \vee Q(x) &\Leftrightarrow \exists x\;\, \neg R(x) \vee \neg S(x) \\ &\Leftrightarrow \exists x\;\, \neg(R(x) \wedge S(x)) \\ &\Leftrightarrow \neg(\forall x\;\, R(x) \wedge S(x)) \\ &\Leftrightarrow \neg((\forall x\;\, R(x)) \wedge (\forall x\;\, S(x))) \\ &\Leftrightarrow \neg(\forall x\;\, R(x)) \vee \neg(\forall x\;\, S(x)) \\ &\Leftrightarrow (\exists x\;\, \neg R(x)) \vee (\exists x\;\, \neg S(x)). \end{aligned}$$

(5) If the statement $(\forall x\, P(x)) \vee (\forall x\, Q(x))$ has T value, then $(\forall x\, P(x)) = T$ or $(\forall x\, Q(x)) = T$, say $(\forall x\, P(x)) = T$. Thus $(\forall x\, P(x) \vee Q(x)) = T$. However,

$$(\forall x\, P(x)) \vee (\forall x\, Q(x)) \not\Leftarrow \forall x\ P(x) \vee Q(x)$$

Take $P(1) = T, P(2) = F$ and $Q(1) = F, Q(2) = T$. Then it shows that the converse is not true.

(6) It is an equivalent form of (5). The proof is similar to that of (4).

(7)
$$\begin{aligned}
(\exists x\, P(x)) \to (\forall x\, Q(x)) &\Leftrightarrow \neg(\exists x\, P(x)) \vee (\forall x\, Q(x)) \\
&\Leftrightarrow (\forall x\, \neg P(x)) \vee (\forall x\, Q(x)) \\
&\overset{(5)}{\Rightarrow} \forall x\ \neg P(x) \vee Q(x) \\
&\Leftrightarrow \forall x\ P(x) \to Q(x)
\end{aligned}$$

Let $P(1) = T, P(2) = F$ and $Q(1) = T, Q(2) = F$, then it shows that the converse is not true.

(8)
$$\begin{aligned}
\exists x\ P(x) \to Q(x) &\Leftrightarrow \exists x\ \neg P(x) \vee Q(x) \\
&\overset{(4)}{\Leftrightarrow} (\exists x\, \neg P(x)) \vee (\exists x\, Q(x)) \\
&\Leftrightarrow \neg(\forall x\, P(x)) \vee (\exists x\, Q(x)) \\
&\Leftrightarrow (\forall x\, P(x)) \to (\exists x\, Q(x))
\end{aligned}$$

□

Example 4.7. Given a universal set U. A predicate $P(x)$ corresponds to a family A_i of subsets of U, and

$$\forall x \in X, P(x) \ \text{ corresponds to } \ \textstyle\bigcap_{i\in I} A_i,$$

$$\exists x \in X, P(x) \ \text{ corresponds to } \ \textstyle\bigcup_{i\in I} A_i,$$

$$\neg(\forall x \in X, P(x)) \Leftrightarrow \exists x \in X, \neg P(x)$$

$$\text{corresponds to}$$

$$\overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i},$$

$$\neg(\exists x \in X, P(x)) \Leftrightarrow \forall x \in X, \neg P(x)$$

$$\text{corresponds to}$$

$$\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A_i}.$$

5 Methods of Proof

Let p and q be statements, usually p and q are compound sentences. If $p \to q$ is a tautology, we say that p **implies logically** q or q **follows logically** from p, written $p \Rightarrow q$. The statement $p \Rightarrow q$ is also called a **theorem**. For statements $p_1, p_2, \ldots, p_n$, if

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q,$$

we say that $p_1, p_2, \ldots, p_n$ **imply logically** q or q **follows logically** from $p_1, p_2, \ldots, p_n$, written

$$\begin{array}{c} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline q \end{array}$$

The statements p_1, p_2, …, p_n are called the **hypothesis** (or **premises**) and q the **conclusion**.

To prove a theorem $p \Rightarrow q$, it means to show that the implication $p \to q$ is a tautology. Arguments based on tautology are called **rules of inference**. The true of rules of inference is universal, and is independent of the context of the truth values of the simple statements involved. We only need to check that when p has T value, the sentence q has T value, regardless of whether p has F value.

Remark. Let $P \to Q$ be a statement in real mathematics. Then there is a valid proof for the mathematical statement $P \to Q$ if and only if $P \to Q$ is a tautology in propositional calculus.

Method of Affirming (**Modus Ponens**, **Rule of Detachment**) is the inference

$$\begin{array}{l} p \\ p \to q \\ \hline q \end{array}$$

This means the tautology

$$p \wedge (p \to q) \Rightarrow q$$

p	q	$p \to q$	$p \wedge (p \to q)$	$(p \wedge (p \to q)) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Example 5.1. Correct or incorrect argument? (valid)

Premisses: *If I have one billion, then I have a car.*
I have one billion.
Conclusion: *I have a car.*

Example 5.2. Correct or incorrect argument? (not valid)

Premisses: *If I have one billion, then I have a car.*
I have one billion.
Conclusion: *I have a bike.*

Chain Rule (**Law of Syllogism**) is the inference

$$\begin{array}{l} p \to q \\ q \to r \\ \hline p \to r \end{array}$$

This means the tautology

$$(p \to q) \wedge (q \to r) \Rightarrow p \to r$$

In fact, the statement has F value if and only if $(p \to q) \wedge (q \to r)$ has T value but $p \to r$ has F value. Then both $p \to q$ and $q \to r$ have T value, and p has

T value and r has F value. Thus q must have T value because $p \to q$ has T value. Since $q \to r$ has T value, then r must have T value, This is contradict to that r has F value.

Example 5.3. Consider the sentences:

If I am attending the class Math2343, then I am in HKUST;

and if I am in HKUST, then I am in Hong Kong.

This is logically equivalent to saying:

If I am attending the class Math2343, then I am in Hong Kong.

Example 5.4. Correct or incorrect argument? (valid)

Premisses:	*If today is weekend, then I am in Macau.*
	Today is Sunday.
Conclusion:	*I am in Macau.*

Solution. Let us define

p :	*Today is weekend.*
q :	*I am in Macau.*
r :	*Today is Sunday.*

Note that $r \to p$ is automatically a tautology. Since $p \to q$ is true, then by Law of Syllogism, $r \to q$ has true value. Since r and $r \to q$ have true value, then by Method of Affirming, q has true value. So the conclusion is a logical result of the premisses.

Example 5.5. Correct or incorrect argument? (not valid)

Premisses:	*If today is weekend, then I am in Macau.*
	Today is Thursday.
Conclusion:	*I am not in Macau.*

Example 5.6. Correct or incorrect argument? (not valid)

Premisses:	*If today is weekend, then I am in Macau.*
	Today is Thursday.
Conclusion:	*I am in Hong Kong.*

Example 5.7. If two integers a and b are even, then their sum $a+b$ is even.

Statement	**Reason**
1. $a = 2a'$, $b = 2b'$.	Hypothesis & defn of even
2. $a + b = 2a' + 2b'$.	Step 1 & defn of addition
3. $a + b = 2(a' + b') = 2c$.	Algebraic manipulation
4. $a + b$ is even.	Step 3 & defn of even

Note that we did not prove that $a + b$ is even. We simply proved *"If a and b are even, then $a+b$ is even."* The above argument can be made into the following formal argument (factorization).

Symbol	**Statement**	**Reason**
1. p	a & b are even.	Hypothesis
2. $p \rightarrow q$	If a & b are even, then $a = 2a'$ & $b = 2b'$.	Definition of even
3. $q \rightarrow r$	If $a = 2a'$ & $b = 2b'$, then $a + b = 2a' + 2b'$.	Doing algebra
4. $p \rightarrow r$	If a & b are even, then $a + b = 2a' + 2b'$	Steps 2 & 3; Law of Syllogism
5. $r \rightarrow s$	If $a + b = 2a' + 2b'$, then $a + b = 2(a' + b') = 2c$.	Factorizing
6. $p \rightarrow s$	If a & b are even, then $a + b = 2c$.	Steps 4 & 5; Law of Syllogism
7. $s \rightarrow t$	If $a + b = 2c$, then $a + b$ is even.	Definition of even
8. $p \rightarrow t$	If a & b are even, then $a + b$ is even	Steps 6 & 7; Law of Syllogism
9. t	$a + b$ is even.	Steps 1 & 8; Rule of Detachment

Example 5.8. If $a \equiv b \bmod n$, then $ca \equiv cb \bmod n$ for all $c \in \mathbb{Z}$.

Method of Denying (**Modus Tollens**, **Contrapositive Proof**) is the inference

$$\begin{array}{l} p \to q \\ \underline{\neg q \qquad} \\ \neg p \end{array}$$

This means the tautology

$$(p \to q) \wedge \neg q \Rightarrow \neg p$$

Example 5.9. Correct or incorrect argument? (valid)

Premisses:	*If today is weekend, then I am in Macau.*
	I am not in Macau.
Conclusion:	*Today is not weekend.*

Example 5.10. Correct or incorrect argument? (not valid)

Premisses:	*If today is weekend, then I am in Macau.*
	I am in Hong Kong.
Conclusion:	*Today is a weekday.*

(We don't have "*If I am in Hong Kong then I am not in Macau*" in pure logic, but we do have it valid in our physical life so far. Let p denote "*today is weekend*", q denote "*I am in Macau*", and r denote "*I am in Hong Kong*". The statement $(p \to q) \wedge r \to \neg p$ is not a tautology.)

Example 5.11. Correct or incorrect argument? (not valid)

Premisses:	*If today is weekend, then I am in Macao.*
	Today is Monday.
Conclusion:	*I am not in Macao.*

Example 5.12. Correct or incorrect argument? (not valid)

Premisses:	*If today is weekend, then I am in Macao.*
	Today is Monday.
Conclusion:	*I am in Hong Kong or Beijing or New York.*

Example 5.13. If n^2 is even, then n is even ($p \to q$).

Statement	**Reason**
1. $n = 2k + 1$	Defenition of odd
2. $n^2 = (2k + 1)^2$	Doing algebra
$= 4k^2 + 4k + 1$	
$= 2l + 1$	
3. n^2 is odd	Definition of odd

Let p denote that n^2 *is even* and q denote that n *is even*. The above argument can be made into the formal argument.

Symbol	**Statement**	**Reason**
1. $\neg q$	n is not even.	Denying
2. $\neg q \to r$	If n is not even, then n is odd, i.e., $n = 2k + 1$.	Meaning of not even
3. $r \to \neg p$	If $n = 2k + 1$,then $n^2 = (2k + 1)^2$. $= 2l + 1$	Doing algebra
	i.e., n^2 is not even.	
4. $\neg q \to \neg p$	If n is not even, then n^2 is not even.	Law of Syllogism
5. $\neg p$	n^2 is not even.	Rule of Detachment

Example 5.14. If $\gcd(a, n) \nmid b$, then $ax \equiv b \bmod n$ has no solution.

Proof. Let $d = \gcd(a, n)$. Suppose there is a solution, say $x = u$ is a solution. Then $au \equiv b \bmod n$, i.e., $b - au$ is a multiple of n, say $b - au = kn$. Thus $b = au + kn$. Since $d \mid a$ and $d \mid n$, we have $d \mid b$. This contradicts $d \nmid b$. □

Define the predicates

$$\begin{aligned} P(a, b, n):&\quad \gcd(a, n) \mid b, \quad a, n \in \mathbb{P}, b \in \mathbb{Z} \\ Q(a, b, n, x):&\quad ax \equiv b \bmod n, \quad a, n \in \mathbb{P}, n, x \in \mathbb{Z} \end{aligned}$$

Then to prove the above result is to show that

$$\forall a \in \mathbb{P}, b \in \mathbb{Z}, n \in \mathbb{P}, \ \neg P(a, b, n) \to \exists x \in \mathbb{Z}, Q(a, b, n, x)$$

is a tautology.

Proposition 5.1. *If* $\gcd(c, n) = 1$ *and* $ca \equiv cb \bmod n$*, then* $a \equiv b \bmod n$*.*

Define the predicates

$$\begin{array}{lll} P(c,n): & \gcd(c,n) = 1, & c \in \mathbb{Z}, n \in \mathbb{P} \\ Q(a,b,c,n): & ca \equiv cb \bmod n, & a,b,c \in \mathbb{Z}, n \in \mathbb{P} \\ R(a,b,n): & a \equiv b \bmod n, & a,b \in \mathbb{Z}, n \in \mathbb{P} \end{array}$$

Then to prove the above result is to show that

$$\forall a, b, c \in \mathbb{Z}, n \in \mathbb{P},\ P(c,n) \wedge Q(a,b,c,n) \to R(a,b,n)$$

is a tautology.

Proof. Since $ca \equiv cb \bmod n$, it means that $n \mid (cb - ca)$, that is, $n \mid c(b - a)$. Since $\gcd(c, n) = 1$, by properties of divisibility, we have $n \mid (b - a)$. Thus $a \equiv b \bmod n$. □

Proposition 5.2. *Show that if* $c|n$ *then*

$$ca \equiv cb \bmod n \quad \textit{if and only if} \quad a \equiv b \bmod \frac{n}{c}.$$

Proof. By definition $ca \equiv cb \bmod n$ is logically equivalent to $ca = cb + kn$ for an integer k, which is $ca = cb + k \cdot \frac{n}{c} \cdot c$. Clearly, $ca = cb + k \cdot \frac{n}{c} \cdot c$ is equivalent to $a = b + k \cdot \frac{n}{c}$, i.e., $a \equiv b \bmod \frac{n}{c}$. □

Example 5.15. If $ax \equiv b \bmod n$, then for any $k, l \in \mathbb{Z}$.

$$(a + kn)x \equiv b + ln \bmod n.$$

Let $P(a, b, n, k, l)$ denote $(a + kn)x \equiv b + ln \bmod n$. Then $P(a, b, n, 0, 0)$ is $ax \equiv b \bmod n$. The above statement can be written as

$$\forall a, b, n \in \mathbb{Z}, P(a, b, n, 0, 0) \to (\forall k, l \in \mathbb{Z}, P(a, b, n, k, l)).$$

The job is to show that the above statement is a tautology.

Proof. Since $ax \equiv b \bmod n$, i.e., $n \,|\, (b - ax)$, we then have

$$(b + ln) - (a + kn)x = (b - ax) + (l - kx)n.$$

It is clear that $n \mid \big((b + ln) - (a + kn)x\big)$. Hence

$$(a + kn)x \equiv b + ln \bmod n.$$

□

Remark. Since $(\forall k, l \in \mathbb{Z}, P(a,b,n,k,l) \Rightarrow P(a,b,n,0,0))$ is obviously true, we thus have $ax \equiv b \bmod n$ if and only if

$$\forall k, l \in \mathbb{Z},\ (a+kn)x \equiv b + ln \bmod n.$$

Writing in propositional sentences, we have

$$\big(\forall a, b \in \mathbb{Z}, n \in \mathbb{P}, P(a,b,n,0,0)\big) \Leftrightarrow \big(\forall k, l \in \mathbb{Z}, P(a,b,n,k,l)\big).$$

Example 5.16. Let $a, b \in \mathbb{Z}, n \in \mathbb{P}$, $d = \gcd(a,n)$. If $d \mid b$ and $d = au + nv$, then

$$ax \equiv b \bmod n \quad \Leftrightarrow \quad x \equiv \frac{ub}{d} \bmod \frac{n}{d}.$$

Proof. Note that

$$ax \equiv b \bmod n \quad \Leftrightarrow \quad \frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}.$$

Since $d = au + nv$, dividing both sides by d, we have

$$1 = \frac{au}{d} + \frac{nv}{d},$$

which is equivalent to $\frac{a}{d}u \equiv 1 \bmod \frac{n}{d}$. (This means that u is the inverse of $\frac{a}{d}$ modulo $\frac{n}{d}$.) Multiplying u to both sides of

$$\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d},$$

we have

$$\frac{au}{d}x \equiv \frac{bu}{d} \bmod \frac{n}{d}.$$

Since $\frac{au}{d} = 1 - \frac{nv}{d}$, then $\frac{au}{d}x = x - \frac{n}{d}vx \equiv x \bmod \frac{n}{d}$. We thus obtain

$$x \equiv \frac{bu}{d} \bmod \frac{n}{d}, \quad \text{i.e.,} \quad x = \frac{bu}{d} + \frac{kn}{d}, \quad k \in \mathbb{Z}.$$

□

Example 5.17. $15x \equiv 6 \bmod 56$.

Note that $56 = 3 \cdot 15 + 11$, $15 = 11 + 4$, $11 = 2 \cdot 4 + 3$, $4 = 3 + 1$. Then

$$\begin{aligned}\gcd(15,56) = 1 &= 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\ &= 3(15 - 11) - 11 = 3 \cdot 15 - 4 \cdot 11 \\ &= 3 \cdot 15 - 4(56 - 3 \cdot 15) = 15 \cdot 15 - 4 \cdot 56.\end{aligned}$$

Thus the solutions are given by

$$x \equiv 6 \cdot 15 \bmod 56, \quad \text{i.e.,} \quad x = 34 + 56k,\ k \in \mathbb{Z}.$$

Example 5.18. $45x \equiv 60 \bmod 75$. This is equivalent to

$$9x \equiv 12 \bmod 15 \quad \Leftrightarrow \quad 3x \equiv 4 \bmod 5 \quad \Leftrightarrow \quad x \equiv 8 \bmod 5.$$

The solution is $x = 3 + 5k$, $k \in \mathbb{Z}$. Since $75 = 45 + 30$, $45 = 30 + 15$, then $15 = 45 - 30 = 45 - (75 - 45) = 2 \cdot 45 - 75$. So

$$x \equiv \frac{2 \cdot 60}{15} \bmod \frac{75}{15}, \quad \text{i.e.,} \quad x = 8 + 5k,\ k \in \mathbb{Z}.$$

6 Mathematical Induction

Mathematical Induction (MI) is an inference about a family of statements $P(k)$, indexed by positive integers k,

$$\begin{array}{l} P(1) \\ \forall k \in \mathbb{P},\ P(k) \to P(k+1) \\ \hline \forall k \in \mathbb{P},\ P(k) \end{array}$$

Mathematical Induction is a consequence of applying the Modus Ponens and the Law of Syllogism again and again. This means that the statement

$$P(1) \wedge (\forall k \in \mathbb{P}, P(k) \to P(k+1)) \to (\forall k \in \mathbb{P}, P(k))$$

is a tautology.

Second Form of Mathematical Induction

$$\begin{array}{l} P(1) \\ \forall k \in \mathbb{P},\ P(1) \wedge P(2) \wedge \cdots \wedge P(k) \to P(k+1) \\ \hline \forall k \in \mathbb{P},\ P(k) \end{array}$$

This means that the statement

$$P(1) \wedge (\forall k \in \mathbb{P}, P(1) \wedge P(2) \wedge \cdots \wedge P(k) \to P(k+1)) \\ \to (\forall k \in \mathbb{P}, P(k))$$

is a tautology.