Chapter 2 Methods of Proofs

We are now prepared to begin our main topic: mathematical proofs. It is essential to know what methods are available to us if we wish to verify the truth of a mathematical statement.

Section 2.1 Rules for Proving

Using a truth table is one of the methods of proving but it is not convenient when we have to prove the statement that combines many statements together. To solve this problem we use the *Rules for Proving* instead of the truth table.

In proving, we use the following principle.

1. The truth value of the given statement is always true.
2. Use the given statements, laws of tautology, rules for proving, and the statements that have been proved to prove the given conclusion that its truth value is true.

Note that we will only write the statements that truth value is true and we will write only "*p*" when we want to say "*the truth value of p is true.*"

Rules for Proving

2.1.1 Rule of Modus Ponens or Rule of Implication

If $p \to q$ and p, then q

Proof:

2.1.2 Rule of Substitution

There are two types of using Rule of Substitution.

1) Substitute the statement that is tautology (or contradiction) with the other statement
2) Substitute the statement with its equivalent statement.

Proof: By the theorem of tautology, theorem of contradiction, and the theorem of equivalence.

For example,

2.1.3 Definition of Conjunction

There are two types of using Definition of Conjunction.

1) If $p \wedge q$, then p and q.
2) If p and q, then $p \wedge q$

2.1.4 Rule of Modus Tollens

If $p \rightarrow q$ and $\sim q$, then $\sim p$

Proof:

2.1.5 Disjunctive Syllogism

There are two types of using Disjunctive Syllogism.

1) If $p \vee q$ and $\sim p$, then q.

2) If $p \vee q$ and $\sim q$, then p.

Proof:

2.1.6 Constructive Dilemma

If $(p \to q) \wedge (r \to s)$ and $p \vee r$, then $q \vee s$

Section 2.2 Direct Proof

The direct proof is the proof that start with what is given then use the rules for proving, axioms, theorems, laws of tautology, or the statements that have been proved to make a conclusion.

Example 1: Prove that if $u \vee (r \to t)$ and $\sim u \wedge \sim t$, then $\sim r$.

Example 2: Prove that if $x \to (y \to z)$, $\sim y \to \sim x$, and x, then z.

Example 3: Prove that if $\sim p \to \sim q$, $\sim u$, $p \to t$, and $q \vee u$, then t.

Example 4: Show $\sim t$ if $\left[r \to (s \to \sim t)\right] \wedge \left[(\sim s \to \sim r) \wedge r\right]$.

Section 2.3 Indirect Proof or Proof by Contradiction

The direct proof is sometimes not very easy to do use the other method of proof which is called indirect proof or proof by contradiction.

To use the method of indirect proof, we assume that the statement we want to proof is false then we try to show that it contradicts with the given statement.

Example 1: Prove that if $(\sim x \vee \sim y) \rightarrow (z \wedge w)$, $z \rightarrow t$, and $\sim t$, then x.

Example 2: Prove that if $(\sim a \vee b) \rightarrow c$, $\sim c \vee d$, and $d \rightarrow \sim (e \vee \sim e)$, then a

Section 2.4 Proof of statements in the form of “ $p \to q$ ”

There are two ways to proof the statements in the form of $p \to q$.

1) Assume p, then prove q.
2) Use Law of Contraposition, that is $(p \to q) \leftrightarrow (\sim q \to \sim p)$ or $(p \to q) \equiv (\sim q \to \sim p)$, then we prove $(\sim q \to \sim p)$ instead of $(p \to q)$. To prove $(\sim q \to \sim p)$, we assume $\sim q$, then prove $\sim p$

Example 1: Prove that if $x \vee \sim y$, and $z \to \sim (x \vee t)$, then $y \to \sim z$.

Example 2: Prove that if $\left[a \vee (b \to c)\right] \wedge (b \vee e)$, then $\sim a \to (\sim c \to e)$.

Example 3: Prove that if $(x \vee \sim y) \wedge \left[z \vee \left(x \to (y \wedge \sim w)\right)\right]$ and $\sim x \to y$, then $\sim z \to \sim w$.

Example 4: Prove that $\left[\sim a \to (b \wedge \sim b)\right] \to a$

Section 2.5 Proof of statements in the form of “ $p \vee q$ ”

Since $(p \vee q) \leftrightarrow (\sim p \rightarrow q)$, by Law of Implication, we can then prove $\sim p \rightarrow q$ instead of $p \vee q$. To prove $\sim p \rightarrow q$, we can assume $\sim p$ and show that q is true. Moreover, since $(p \vee q) \equiv (q \vee p)$ and $(q \vee p) \leftrightarrow (\sim q \rightarrow p)$, hence there are two ways to prove $p \vee q$.

1) Assume $\sim p$ and show that q is true.
2) Assume $\sim q$ and show that p is true

Example 1: Prove that if $(\sim x \wedge y) \rightarrow \sim z$, $\sim (x \vee y) \rightarrow w$, and $\sim x$, then $\sim z \vee w$.

Example 2: Prove that if $a \vee (b \wedge \sim c)$, $\sim a$, $b \rightarrow (d \rightarrow e)$, and $\sim c \rightarrow (x \rightarrow y)$, then $[a \vee x \vee d] \rightarrow (y \vee e)$.

Example 3: Prove that if $(x \wedge y \wedge \sim z) \rightarrow \sim y$, then $\sim x \vee (y \rightarrow z)$.

Section 2.6 Proof of statements in the form of " $p \leftrightarrow q$ "

Since $(p \leftrightarrow q) \leftrightarrow [(p \to q) \wedge (q \to p)]$, by Law of Equivalence, we can then prove $(p \to q) \wedge (q \to p)$ instead of $p \leftrightarrow q$. To prove $(p \to q) \wedge (q \to p)$, we have to prove that $p \to q$ is true and also $q \to p$ is true by the method of proving the statements in the form of $p \to q$.

Example 1: Prove that if $a \to (b \wedge c)$, $(d \wedge c) \to (e \wedge \sim a)$, $a \vee (d \to \sim e)$, and $d \wedge (b \to e)$, then $\sim e \leftrightarrow \sim a$.

Example 2: Prove that $[p \to (q \to r)] \leftrightarrow [\sim (p \to r) \to (q \to \sim p)]$.

Section 2.7 Proof of statements in the form of "$(p \vee q) \to r$"

Note that

$$
\begin{aligned}
[(p \vee q) \to r] &\equiv [\sim (p \vee q) \vee r] && \text{Law of Implication} \\
&\equiv [(\sim p \wedge \sim q) \vee r] && \text{De Morgan's Laws} \\
&\equiv [(\sim p \vee r) \wedge (\sim q \vee r)] && \text{Distributive Laws} \\
&\equiv [(p \to r) \wedge (q \to r)] && \text{Law of Implication}
\end{aligned}
$$

Hence, we can prove $(p \to r) \wedge (q \to r)$ instead of $(p \vee q) \to r$. In order to show that $(p \to r) \wedge (q \to r)$ is true, we must show that $p \to r$ is true and also $q \to r$ is true.

Example 1: Let m and n be integers. Prove that *if* m and n are even *or* m and n are odd, *then* the sum of m and n is even.

We have now seen many examples of integers that can be expressed as $2x$ for some integer x. There are precisely the even integers, of course. However, some integers can also be written as $3x$ or $4x$ or as $-5x$ for some integer x. In general, for integers a and b with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$. In this case, we write $a | b$.

If $a | b$, then we also say b is a **multiple** of a and that a is a **divisor** of b. Thus every even integer is a multiple of 2. If a does not divide b, then we write $a | b$.

Example 2: Let m be any integer. Prove that if 4 divides m or 6 divides m, then $m^2 - 1$ is odd.