3.4.2 Direct Proof

The most straightforward method of proving an implication $\mathfrak{a} \Rightarrow \mathfrak{b}$ is to assume that its hypothesis ($\mathfrak{a}$) is true and show that its conclusion ($\mathfrak{b}$) is true. This is called a ***direct proof***. Unlike the method of trivial proof, this method may be applied to any implication. The following is an example.

Proposition 3.4.1 *Let m, n, p be integers. If m divides n and n divides p, then m divides p, i.e., $(m|n \ \wedge \ n|p) \ \Rightarrow \ m|p$.*
Proof: Suppose that the hypothesis, $m|n \ \wedge \ n|p$, is true. Then, according to Definition 3.1.1, $\exists j \in \mathbb{Z}, n = jm$ and $\exists k \in \mathbb{Z}, p = kn$. Therefore, if we let $q := jk$, then $q \in \mathbb{Z}$ and $p = kn = kjm = qm$. This shows the existence of an integer q satisfying $p = qm$ and establishes the conclusion of the theorem, namely $m|p$. ■

3.4.3 Contrapositive Proof

In our discussion of Propositional Calculus, we encountered the logical equivalence of any implication $\mathfrak{a} \Rightarrow \mathfrak{b}$ and its contrapositive $\neg\mathfrak{b} \Rightarrow \neg\mathfrak{a}$. This means that these two implications have the same truth value. In particular, to establish $\mathfrak{a} \Rightarrow \mathfrak{b}$ we can show that $\neg\mathfrak{b} \Rightarrow \neg\mathfrak{a}$ is true. This is called the method of ***contrapositive proof***. Similarly to the method of direct proof, this method is generally applicable. It is more useful than the direct proof whenever the negation of the hypothesis or the conclusion has a simpler form or is related to definitions and previously proven theorems more closely. The following is a good example.

Proposition 3.4.2 *For every integer n, if n^2 is even, then so is n, i.e.,*

$$2|n^2 \ \Rightarrow \ 2|n. \tag{3.9}$$

Proof: Let $\mathfrak{a} :=$" $2|n^2$ " and $\mathfrak{b} :=$" $2|n$," so that (3.9) takes the form $\mathfrak{a} \Rightarrow \mathfrak{b}$. It is sufficient to prove the contrapositive implication: $\neg b \Rightarrow \neg a$. This is an implication in its own right, and we can apply the method of direct proof to prove it. We suppose that $\neg b$ is true, i.e., b is false. This means that n is not an even number. So it must be odd. This in turn implies that the remainder of the division of n by 2 is 1, i.e., $\exists k \in \mathbb{Z}$, $n = 2k + 1$. But then,

$$n^2 = (2k + 1)^2 = 4k(k + 1) + 1.$$

If we let $j := 2k(k + 1)$, we can write $n^2 = 2j + 1$. Because $j \in \mathbb{Z}$, this equation implies that n^2 is not even, $\mathfrak{a}$ is false, and $\neg\mathfrak{a}$ is true. ■

3.4.4 Deductive Proof

In Section 2.5 (Theorem 2.5.2) we showed that for any three statements $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$, the compound statement $(\mathfrak{a} \Rightarrow \mathfrak{c}) \wedge (\mathfrak{c} \Rightarrow \mathfrak{b})$ implies $\mathfrak{a} \Rightarrow \mathfrak{b}$. In other words, in order to establish that $\mathfrak{a} \Rightarrow \mathfrak{b}$ is true, it is sufficient to show that $(\mathfrak{a} \Rightarrow \mathfrak{c}) \wedge (\mathfrak{c} \Rightarrow \mathfrak{b})$ holds. This is the basic idea of ***deductive reasoning***. Using the notation we introduced in (2.13) we can write $(\mathfrak{a} \Rightarrow \mathfrak{c}) \wedge (\mathfrak{c} \Rightarrow \mathfrak{b})$ in the form $\mathfrak{a} \Rightarrow \mathfrak{c} \Rightarrow \mathfrak{b}$, and express the statement of Theorem 2.5.2 as: "*The compound statement*

$$(\mathfrak{a} \Rightarrow \mathfrak{c} \Rightarrow \mathfrak{b}) \Rightarrow (\mathfrak{a} \Rightarrow \mathfrak{b}) \tag{3.10}$$

is a tautology." We can easily generalize it:

Theorem 3.4.1 *Let $n \in \mathbb{Z}^+$ and $\mathfrak{c}_1, \mathfrak{c}_2, \cdots, \mathfrak{c}_n, \mathfrak{a}, \mathfrak{b}$ be statements. Then the following is a tautology*

$$\mathfrak{t} := (\ (\mathfrak{a} \Rightarrow \mathfrak{c}_1 \Rightarrow \mathfrak{c}_2 \Rightarrow \cdots \Rightarrow \mathfrak{c}_n \Rightarrow \mathfrak{b}) \Rightarrow (\mathfrak{a} \Rightarrow \mathfrak{b})\ ). \tag{3.11}$$

Proof: If $n = 1$, this is just the statement of Theorem 2.5.2. Therefore we consider the case $n \geq 2$. First, we express $\mathfrak{t}$ in the form

$$\mathfrak{t} = (\mathfrak{f} \Rightarrow \mathfrak{g}), \tag{3.12}$$

where $\mathfrak{f} := (\mathfrak{a} \Rightarrow \mathfrak{c}_1 \Rightarrow \mathfrak{c}_2 \Rightarrow \cdots \Rightarrow \mathfrak{c}_n \Rightarrow \mathfrak{b})$ and $\mathfrak{g} := (\mathfrak{a} \Rightarrow \mathfrak{b})$. We recall that according to (2.13),

$$\mathfrak{f} = (\ (\mathfrak{a} \Rightarrow \mathfrak{c}_1) \wedge (\mathfrak{c}_1 \Rightarrow \mathfrak{c}_2) \wedge \cdots \wedge (\mathfrak{c}_{n-1} \Rightarrow \mathfrak{c}_n) \wedge (\mathfrak{c}_n \Rightarrow \mathfrak{b})\ ). \tag{3.13}$$

Next, we examine if it is possible for $\mathfrak{t}$ to be false. The proof will be complete, if we succeed in showing that this is not the case. In order for $\mathfrak{t}$ to be false, its hypothesis $\mathfrak{f}$ must be true and its conclusion $\mathfrak{g}$ must be false. According to (3.13), $\mathfrak{f}$ is true only if all the implications $\mathfrak{a} \Rightarrow \mathfrak{c}_1$, $\mathfrak{c}_1 \Rightarrow \mathfrak{c}_2$, $\cdots$, $\mathfrak{c}_{n-1} \Rightarrow \mathfrak{c}_n$, and $\mathfrak{c}_n \Rightarrow \mathfrak{b}$ are true. Furthermore, $\mathfrak{g}$ is false provided that $\mathfrak{a}$ is true and $\mathfrak{b}$ is false. Now, because $\mathfrak{a}$ and $\mathfrak{a} \Rightarrow \mathfrak{c}_1$ are true, $\mathfrak{c}_1$ must be true. Because $\mathfrak{c}_1$ and $\mathfrak{c}_1 \Rightarrow \mathfrak{c}_2$ are true, $\mathfrak{c}_2$ must be true. Repeating this argument, we find that because $\mathfrak{c}_n$ and $\mathfrak{c}_n \Rightarrow \mathfrak{b}$ are true, $\mathfrak{b}$ must be true. But we already mentioned that $\mathfrak{b}$ is false. This shows that it is not possible for $\mathfrak{t}$ to be false; it is true regardless of the truth values of $\mathfrak{a}, \mathfrak{c}_1, \mathfrak{c}_2, \cdots, \mathfrak{c}_n$ and $\mathfrak{b}$. Therefore, it is a tautology. ■

This theorem provides the logical basis for the method of ***proof by deduction***. It states that *in order to establish the validity of an implication* $\mathfrak{a} \Rightarrow \mathfrak{b}$*, we may introduce a number* $(n \in \mathbb{Z}^+)$ *of intermediate statements* $\mathfrak{c}_1, \mathfrak{c}_2, \cdots, \mathfrak{c}_n$ *and prove the implications* $\mathfrak{a} \Rightarrow \mathfrak{c}_1$*,* $\mathfrak{c}_1 \Rightarrow \mathfrak{c}_2$*,* $\cdots$*,* $\mathfrak{c}_{n-1} \Rightarrow \mathfrak{c}_n$*, and* $\mathfrak{c}_n \Rightarrow \mathfrak{b}$. The main motivation for this method is that it reduces the problem of proving a given implication $\mathfrak{a} \Rightarrow \mathfrak{b}$ into that of a number of intermediate implications that may admit simpler proofs. Many of the proofs we have so far given make use of this method. Indeed, we employ it whenever we engage in a logical argument.

In the following we first give a proof of the statement $\mathfrak{d}$:="*sum of two even integers is even.*" and then identify the intermediate deductive steps of this proof.

Proof of $\mathfrak{d}$: For every pair m and n of even integer, $2|m$ and $2|n$, i.e., there are integers j and k such that $m = 2j$ and $n = 2k$. Then $m + n = 2(j + k)$. Because j and k are integers, so is $i := j + k$. Therefore, there is an integer i such that $m + n = 2i$. This shows that $2|(m + n)$, i.e., $m + n$ is even. ■

Analysis of the deductive structure of the preceding proof: Let $\mathfrak{p}(x)$ be the predicate

$$\mathfrak{p}(x) :=\ 2|x\ :=\ \text{“}\ \exists k \in \mathbb{Z}, x = 2k,\ \text{”} \tag{3.14}$$

with an integer variable x. Then,

$$\mathfrak{d} = (\forall m, n \in \mathbb{Z},\ ((\mathfrak{p}(m) \wedge \mathfrak{p}(n)) \Rightarrow (\mathfrak{p}(m + n))). \tag{3.15}$$

Let $\forall m, n \in \mathbb{Z}$, $\mathfrak{f} := \mathfrak{p}(m)$, $\mathfrak{g} := \mathfrak{p}(n)$, $\mathfrak{a} := \mathfrak{f} \wedge \mathfrak{g}$, and $\mathfrak{b} := \mathfrak{p}(m + n)$. Then $\mathfrak{d}$ is equivalent to "$\forall m, n \in \mathbb{Z}$, $\mathfrak{a} \Rightarrow \mathfrak{b}$." The above proof involves the following chain of implications.

$$\mathfrak{a} \Rightarrow (\exists j, k \in \mathbb{Z},\ (m = 2j) \wedge (n = 2k)) \Rightarrow ((m + n = 2(k + j)) \wedge (k + j \in \mathbb{Z})) \Rightarrow \mathfrak{b}.$$

3.5 Proof by Contradiction

Suppose that we wish to prove the statement $\mathfrak{a}$ of a theorem. We can achieve this by showing that its negation $\neg\mathfrak{a}$ is false. One way of doing this is to find a statement $\mathfrak{b}$ such that (i) $\neg\mathfrak{a} \Rightarrow \mathfrak{b}$ is true, and (ii) $\mathfrak{b}$ is false. Recalling the fact that the only way in which an implication with a false conclusion is true is that its hypothesis is false, we see that conditions (i) and (ii) imply that $\neg\mathfrak{a}$ is false. Hence $\mathfrak{a}$ must be true. This argument forms the logical basis of the method of ***proof by contradiction***. A successful application of this method involves three steps, namely

1. finding an appropriate argument $\mathfrak{b}$,
2. proving $\neg\mathfrak{a} \Rightarrow \mathfrak{b}$, and
3. proving that $\mathfrak{b}$ is false.