CHAPTER 2

The Propositional Calculus 2

INTRODUCTION

In the previous chapter we gradually learned what may be described as a *formal language*, a language designed for the study of certain patterns of argument in something of the way in which the language of elementary mathematics is designed for the study of certain numerical operations (addition, subtraction, etc.). This language is often called, for reasons which should be obvious, the *propositional calculus* (also sometimes the *sentential* calculus). In the present chapter, we study it at a more theoretical level, in order to gain a clearer insight into its properties and its power. Among the questions we shall raise are the following three. (i) It commonly happens in mathematics that a result, once proved, can be utilized without re-proof in obtaining new results—mathematics is *progressive* in just this sense, as any student of Euclidean geometry knows. Are there any analogous devices whereby we can use a sequent already proved to facilitate the discovery of proofs for other sequents? An affirmative answer is given in Section 2. (ii) However confident on intuitive grounds we may be that our rules of derivation are safe, is there nevertheless any way of *showing* that they are safe, showing that they will not yield sequents which are in fact invalid? A way is found in Sections 3 and 4. (iii) We have so far introduced ten rules of derivation for operating the symbols of the language: are these enough, or do we require more? Section 5 shows that our rules form in a certain sense a *complete* set, and that no more are needed. The answers to these and related questions afford a deepened understanding of the nature of the propositional calculus.

1 FORMATION RULES

The propositional calculus is, I have said, a kind of language, and as such it has a grammar or, more particularly, a *syntax*. We have taken this syntax for granted in our fairly easy-going approach so far;

but we cannot go much further without a more scrupulous account of the structure of the language itself. In particular, we have taken for granted what was understood by a *sentence in the symbolism*; it is part of our task as logicians to make this notion precise, and we devote this section to the job by introducing a rather long series of definitions.

First, I define a *bracket*. A bracket is one of the marks:

'(', ')',

and I call the first kind of mark a *left-hand* bracket and the second a *right-hand* bracket. This definition, which should be readily understood, is an *ostensive* definition, so-called because I *show* or *exhibit* what a bracket is rather than use other *words* to define one. (We could avoid ostensive definition: I might say that a bracket is an arc of a circle, with one end point placed vertically above the other end point.)

Second, I define a *logical connective*, often just called a *connective*. A logical connective is one of the marks:

'$\rightarrow$', '$-$', '&', 'v', '$\leftrightarrow$'.

This is also an ostensive definition, which formally introduces the symbols employed in the last chapter for sentence-forming operators on sentences.

Third, I define a *(propositional) variable*. A propositional variable is one of the marks:

'P', 'Q', 'R', ...

This is again an ostensive definition, but importantly different from the earlier two. There are just two kinds of mark which are called brackets, and just five which are called connectives; but the '. . .' in the definition of a variable is intended to indicate that there is an *indefinitely large* number of distinct such. Human limitations being what they are, we have room and time to list only a finite number; so we add '. . .'. Since in practice we rarely need more than four distinct variables, there is no need to specify how the list would continue. But it is well to remember that the number of variables has no *theoretical* upper limit, that if we ever need a new one we are entitled to construct it (say by adding dashes and introducing 'P'', 'R'''', etc., into our list).

Fourth, I define a *symbol* (*of the propositional calculus*) as *either a* *bracket or a logical connective or a propositional variable.* Hence any of the above marks is a symbol.

Fifth, I define a *formula (of the propositional calculus)* as *any sequence of symbols.* This definition needs a little explanation; in virtue of it,

(1) ' $P((-\&Q\leftrightarrow$ '
(2) ' $(P \vee -P)$ '

are both formulae, since both are sequences of symbols: (2) for example is the sequence consisting of a left-hand bracket, followed by an occurrence of the variable ' P ', followed by the connective ' v ', followed by the connective '—', followed by a second occurrence of the variable ' P ', followed by a right-hand bracket. But

(3) ' v P '
      & $\rightarrow$
  ($\rightarrow$ R
)

is *not* a formula, since it is not a *sequence* of symbols, but rather a jumble of them. A sequence requires order, which (1) and (2) possess but (3) lacks. Our normal convention for writing sequences of symbols is that they shall appear, not spaced too far apart, in the order from left to right. This is a contemporary European convention, which the reader will be relieved to see I am following in this book.

Of the whole class of formulae, some, like (1) above, might be loosely called meaningless or gibberish, while others, like (2), make sense and can be understood. It is only, of course, the second group that we want to use in our formal work, so that we must single them out, if we can, by a precise definition. Out of the totality of formulae, therefore, we define the sub-class of *well-formed formulae*, by a somewhat complex definition, which has seven clauses. To save space, we abbreviate ' well-formed formula ' to ' wff ' (plural ' wffs '), both here and hereafter.

(*a*) any propositional variable is a wff;
(*b*) any wff preceded by ' — ' is a wff;
(*c*) any wff followed by ' $\rightarrow$ ' followed by any wff, the whole enclosed in brackets, is a wff;

(*d*) like (*c*), with '$\&$' replacing '$\rightarrow$';
(*e*) like (*c*), with '$\vee$' replacing '$\rightarrow$';
(*f*) like (*c*), with '$\leftrightarrow$' replacing '$\rightarrow$';
(*g*) if a formula is not a wff in virtue of clauses (*a*)–(*f*), then it is not a wff.

The best way to see that these clauses do successfully define a wff is to consider examples. We show that

(4) '$(((P \rightarrow Q) \vee -Q) \leftrightarrow (--P \,\&\, Q))$'

is a wff, as we wish it to be, in view of the definition. First, in virtue of clause (*a*),

$$\text{'}P\text{'}, \text{'}Q\text{'}$$

are wffs, since by (*a*) all variables are wffs. By (*b*), the result of prefixing '$-$' to a wff gives a wff: hence

$$\text{'}-P\text{'}, \text{'}-Q\text{'}$$

are wffs. But if '$-P$' is a wff, as we have shown it to be, then by clause (*b*) again

$$\text{'}--P\text{'}$$

is a wff. (We could go on applying (*b*) to show that '$---P$', '$-----P$', etc., were all wffs.) Now since '$--P$' and 'Q' have been shown to be wffs, by clause (*d*) the result of placing '$\&$' between them and enclosing the whole in brackets yields a further wff: hence

(5) '$(--P \,\&\, Q)$'

is a wff. Again, by (*c*), since 'P' and 'Q' are wffs, so is

$$\text{'}(P \rightarrow Q)\text{'}.$$

Using (*e*), given that '$(P \rightarrow Q)$' and '$-Q$' are wffs, we have that

(6) '$((P \rightarrow Q) \vee -Q)$'

is a wff. Finally, using (*f*), given that (6) and (5) are wffs, we see that (4) itself is a wff: for (4) results from writing (6), followed by '$\leftrightarrow$', followed by (5), the whole enclosed in brackets. Our definition has enabled us to show, step by step beginning from the smallest parts (the variables), that a complex formula such as (6) is well-formed. A careful study of the example should make clear how the technique can be generally applied.

On the other hand, it is obvious (though not too easy to prove) that no such applications of clauses (*a*) to (*f*) could ever show that (1) above—the example of 'gibberish'—is a wff. Hence, by clause (*g*), the ruling-out or *extremal* clause of the definition, (1) is *not* a wff. The force of clauses (*a*)–(*g*), taken together, is to divide the totality of formulae into two camps: those that can be obtained by applications of clauses (*a*)–(*f*), which are wffs by the definition, and those that cannot be so obtained, which by (*g*) of the definition are not wffs.

An important aspect of this definition is the insistence, in clauses (*c*)–(*f*), on introducing surrounding *brackets*. This is necessary because of ambiguities that would result from their omission. For example, we do not wish to admit as well-formed the formula '$P \,\&\, Q \rightarrow R$', because as it stands this might mean either '$(P \,\&\, (Q \rightarrow R))$' (expressing a conjunction with a conditional second conjunct) or '$((P \,\&\, Q) \rightarrow R)$' (expressing a conditional with a conjunction for antecedent). Our emphasis on bracket-insertion removes risks of this kind. (On the other hand, we need no such insertion of brackets in clause (*b*), and the student may profitably speculate as to why not.)

In some ways, however, the bracketing conventions imposed by the definition of a wff, though theoretically correct, are in practice a nuisance. In fact, as a result of them the vast majority of formulae exhibited in Chapter 1 are unfortunately not well-formed. They lacked the requisite outer pair of brackets. We accepted there, for example, '$-P \rightarrow Q$', whilst by clause (*c*) we require '$(-P \rightarrow Q)$'. But our instinct was sound, if our precision was faulty: human beings cannot stand very much proliferation of brackets. A natural *practical* convention to adopt is to permit the dropping of outermost brackets, since evidently no ambiguity can result. And there is another useful practical way in which we can cut down brackets safely, as follows.

Let us *rank* the connectives in a certain order: let us agree that '$-$' 'ties more closely' than '&' or 'v', that '&' and 'v' 'tie more closely' than '$\rightarrow$', and that '$\rightarrow$' 'ties more closely' than '$\leftrightarrow$'. Thus we can safely write in practice '$P \,\&\, Q \rightarrow R$' for

'$((P \& Q) \rightarrow R)$', dropping the outer brackets by our previous convention, and dropping the inner ones by our present one: '$\&$', tying more closely than '$\rightarrow$', steals the 'Q' in '$P \& Q \rightarrow R$' for a second conjunct, rather than leaving it as the antecedent of '$Q \rightarrow R$'. If we require the latter interpretation, we need to write '$P \& (Q \rightarrow R)$'. Using these conventions, we can write (4) unambiguously in the less bracket-infested form

(7) '$(P \rightarrow Q) \vee -Q \leftrightarrow --P \& Q$',

where only one pair of brackets is required. (In this connection, the student should notice the difference between $--(P \& Q)$, the double negation of the conjunction of P and Q, and $--P \& Q$, the conjunction of the double negation of P and Q.)

These conventions will be adopted from now on. But it must be stressed that they are practical guides to the eye, not theoretical devices. In theory, a wff remains as defined above, complete with its outer brackets and inner pairs of the same.

So far, we have described the basic syntax of the propositional calculus: the definition given of a wff can be read as an exact account of what is to be understood by the hitherto vague notion of a sentence in the symbolism; and clauses (*a*)–(*f*) of that definition can be read as giving what are often described as the *formation rules* of the propositional calculus—the rules, that is, determining what is a properly formed expression of the language.

But there are other syntactical notions which will be important later and which it is useful to define now. The first of these is that of the *scope* of a connective. Roughly speaking, the scope of a connective in a certain formula is the formulae *linked* by the connective, together with the connective itself and the (theoretically) encircling brackets. For example, the scope of '$\&$' in (4) is the wff '$(--P \& Q)$' and the scope of '$\leftrightarrow$' in (4) is the wff (4) itself: in general, the scope of any connective is a wff. More strictly, we need to define the scope of an *occurrence* of a connective in a certain wff: in (4) there are three occurrences of '$-$'; the scope of the first occurrence (reading from left to right) is '$-Q$', the scope of the second is '$--P$', and the scope of the third is '$-P$'. The scope is what a particular occurrence of a connective controls. A precise definition of scope is as follows: the *scope* of an occurrence of a connective in a wff is *the shortest wff in which that occurrence appears*.

Consider, for example, the (sole occurrence of) ' v ' in (4): this appears, within (4), in such formulae as:

(i) ') v — '
(ii) ' $\rightarrow Q$) v $-Q$) '
(iii) ' (($P \rightarrow Q$) v $-Q$) '
(iv) ' ((($P \rightarrow Q$) v $-Q$) $\leftrightarrow$ (— — '.

The shortest formula in which it appears which is also a *well-formed* formula by clauses (*a*)–(*f*) above is (iii), and this is in fact the scope of that occurrence of ' v '. Even if the definition of scope seems a bit queer, the intuitive content of the notion should be obvious.

In terms of scope, we may define a second important syntactical notion, that of one (occurrence of a) connective being *subordinate*, in a certain wff, to another. One (occurrence of a) connective is *subordinate* to another if *the scope of the first is contained in the scope of the second.* For example, in (4) the ' $\rightarrow$ ' is subordinate to the ' v ', and the ' v ' and the ' & ' are both subordinate to the ' $\leftrightarrow$ '. The first ' — ' is subordinate to ' v ', but not to ' $\rightarrow$ '; the second '—' is subordinate to ' & ' but not to ' v '; the third '—' is subordinate to the second ' — ', and so to ' & ' and ' $\leftrightarrow$ ', but not to ' $\rightarrow$ ' or ' v '. In any wff, there is exactly one connective to which all other connective-occurrences are subordinate, which is in fact the connective of widest scope. This is called the *main connective*, and its scope is the whole wff. For example, in (4) the main connective is ' $\leftrightarrow$ ', and in (2) and (6) it is ' v '.

When we prove, by application of clauses (*b*)–(*f*), that a certain formula is well-formed, we need to proceed from subordinate to subordinating connectives. Thus, in proving (4) to be well-formed, we establish that ' $-P$ ' is well-formed before we prove that ' $--P$ ' is; and that ' $--P$ ' is before we prove that ' ($--P$ & Q) ' is; and so on—at each step introducing a connective which subordinates or has in its scope the previously introduced connectives. From this point of view, the notions of scope and subordination as well as clauses (*a*)–(*f*) are ways of indicating the *natural structure* of a wff.

With the notion of a wff clear in our minds, we can readily define a *sequent-expression* (an expression which expresses a sequent, in the sense of the last chapter). As before, let us call ' $\vdash$ ' the *assertion-sign*, and let $A_1, A_2, \ldots, A_n$, B be any set of wffs. Then

$$A_1, A_2, \ldots, A_n \vdash B$$

is a sequent-expression. In other words, write down any (finite) number of wffs, with commas between them; add to the right the assertion-sign, and follow this by any wff; the result is a sequent-expression. In the last chapter, at least 36 sequent-expressions are proved to express valid sequents, corresponding to the proofs numbered 1-36.

This last definition introduces a device which is extremely helpful in logic: the device of *metalogical variables*, such as 'A_1', 'A_n', 'B'. (They appeared earlier, in Chapter 1, Section 4, in the statement of *Df.* $\leftrightarrow$.) *Propositional* variables, such as 'P', 'Q', have as instances propositions; numerical variables in algebra, such as 'x', 'y', have as instances *numbers*. But metalogical variables are of service when we wish, as we do at present, to talk about *symbols themselves*, for they have as instances *symbols* or sequences of them. When I say that $A_1, A_2, \ldots, A_n$ are to be a set of wffs, this is entirely analogous to saying, in algebra, that $x_1, x_2, \ldots, x_n$ are to be a set of numbers. We may illustrate further the usefulness of metalogical variables by restating clauses (*a*)–(*f*) in a new form (these versions have exactly the sense of the earlier ones).

(*a'*) any propositional variable is a wff;
(*b'*) if A is a wff, then $-$A is a wff;
(*c'*) if A and B are wffs, then (A $\rightarrow$ B) is a wff;
(*d'*) if A and B are wffs, then (A & B) is a wff;
(*e'*) if A and B are wffs, then (A v B) is a wff;
(*f'*) if A and B are wffs, then (A $\leftrightarrow$ B) is a wff.

EXERCISE

Select formulae (say from Chapter 1), and write them out as wffs. In each case, prove them to be wffs, using the definition of a wff; state the scope of each (occurrence of a) connective; state which is the main connective, and the relations of subordination which are present between the connective-occurrences.

2 THEOREMS AND DERIVED RULES

With the syntax of the propositional calculus now described, we may turn to the first question raised in the introduction to this chapter: what devices can we develop for utilizing already proved sequents to shorten the proofs for other sequents? One of the main devices will be the introduction of *theorems* into proofs, so that we begin by explaining what these are.

As was pointed out in Chapter 1, two out of the ten rules of derivation so far introduced—CP and RAA—have the property that as a result of their application in a proof the number of assumptions marked on the left falls by one. Suppose, now, that before the application of one of these rules there is only *one* assumption on the left: then as a result of this application there will be *no* assumption on the left. This possibility was countenanced in the statement of the rules; for example, in Section 5 of the last chapter, RAA was said to permit us, given a proof of B & —B from A, to derive —A on the remaining assumptions (*if any*). Here is a simple example of a proof having this feature.

37	1	(1) P & $-P$	A
		(2) $-(P$ & $-P)$	1,1 RAA

At line (1), we assume the contradiction P & $-P$ (nothing in the rule of assumptions prevents us from assuming what we will). Hence line (1) affirms that, given this contradiction, we have a contradiction. We can thus apply RAA to derive the negation of (1) *on no assumptions at all.* Consequently, at line (2) there are *no* citations on the left-hand side.

We may state the sequent proved at line (2) of 37 very simply.

37 $\vdash -(P$ & $-P)$

Here the assertion-sign appears with no wffs written to the left of it, corresponding to the absence of citation on the left at line (2). The conclusions of sequents which we can prove in this form we call *theorems*; thus a theorem is *the conclusion of a provable sequent in which the number of assumptions is zero.* Instead of reading the assertion-sign as ' therefore ', which is the most natural reading in the case of sequents which have assumptions, in the case of sequents provable with no assumptions we may naturally read it as ' it is a theorem that . . .'. Thus 37 states that it is a theorem that it is not the case that P and not $-P$: for example, it is a theorem that it is not the case that it is raining and it is not raining.

Most theorems of interest are obtained in fact by application of CP. For example:

38 $\vdash P \rightarrow P$ (compare sequent 29)

1	(1) P	A
	(2) $P \rightarrow P$	1,1 CP

39 $\vdash P \rightarrow --P$

1	(1) P	A
1	(2) $--P$	1 DN
	(3) $P \rightarrow --P$	1,2 CP

40 $\vdash --P \rightarrow P$

1	(1) $--P$	A
1	(2) P	1 DN
	(3) $--P \rightarrow P$	1,2 CP

41 $\vdash P \& Q \rightarrow P$ (compare sequent 14)

1	(1) $P \& Q$	A
1	(2) P	1 &E
	(3) $P \& Q \rightarrow P$	1, 2 CP

38 and 41, when compared with 29 and 14, suggest that a theorem can be obtained from *any* sequent proved in the last chapter simply by appending to its proof one or more steps of CP. For example:

42 $\vdash (P \rightarrow Q) \rightarrow (-Q \rightarrow -P)$

1	(1) $P \rightarrow Q$	A
2	(2) $-Q$	A
1,2	(3) $-P$	1,2 MTT
1	(4) $-Q \rightarrow -P$	2,3 CP
	(5) $(P \rightarrow Q) \rightarrow (-Q \rightarrow -P)$	1,4 CP

Here, lines (1)–(4) are identical with the proof of sequent 9, $P \rightarrow Q \vdash -Q \rightarrow -P$, and the step of CP at line (5) completes the proof of 42. Similarly, three steps of CP added to the proof of sequent 4 yields:

43 $\vdash (P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$

The importance of theorems resides in the fact that, since they are provable as conclusions from *no* assumptions, they are propositions which are *true simply on logical grounds*. Such truths, often called *logical truths* or *logical laws*, occupy an important place not only in logic but in philosophy also. Many of them have received special names. For example, 37 is called the *law of non-contradiction*; 38 is called the *law of identity*; 39 and 40 are sometimes called the *laws of double negation*. As an example of 38, we may consider the proposition that if it is raining then it is raining; this is true on purely logical grounds, quite independently of the actual state of the weather.

Theorems, such as $P \rightarrow P$, should be contrasted with the corresponding valid sequents with assumptions, such as $P \vdash P$. Whilst the latter are argument-frames, patterns of valid argument, the former are (logically) *true propositions*. 'It is raining; therefore it is raining' expresses an argument, of which we can ask: is it *valid* or not? 'If it is raining, then it is raining' expresses a proposition, of which we can ask: is it *true* or not? To confuse arguments with propositions is analogous to confusing validity with truth—a confusion I tried to eliminate in the first section of this book.

There is one further theorem of importance, which cannot be proved by a final step of CP since it is not conditional in form, called the *law of excluded middle*:

44 $\vdash P \vee -P$

1	(1) $-(P \vee -P)$	A
2	(2) P	A
2	(3) $P \vee -P$	2 vI
1,2	(4) $(P \vee -P) \& -(P \vee -P)$	3,1 &I
1	(5) $-P$	2,4 RAA
1	(6) $P \vee -P$	5 vI
1	(7) $(P \vee -P) \& -(P \vee -P)$	6,1 &I
	(8) $--(P \vee -P)$	1,7 RAA
	(9) $P \vee -P$	8 DN

We assume at line (1) the negation of the desired theorem, and aim for a contradiction. By assuming P (line (2)), we obtain a contradiction (line (4)) resting on both (1) and (2), so that (1) leads (line (5)) to $-P$. This leads to the same contradiction (line (7)), which now, however, rests solely on (1). Hence, using DN, we obtain the desired result. It is worth noting that at line (6) we find $P \vee -P$ resting *on its own negation* as assumption—given that it is not the case, it is the case; this should throw some light on the 'surprising' result 23 of the last chapter.

The law of excluded middle effectively affirms that, for any proposition, either it or its negation is the case, which is fairly evidently a logical truth. It is closely related to the law that every proposition is either true or false, and from this law it receives its name—a third or middle value between truth and falsity is excluded for all propositions. As a matter of logic, either it is raining or it is not raining: there is no third possibility. To be quite fair, it should be said that it can be and has been doubted whether this law has universal application: for example, is it true that either you have stopped beating your wife or you have not?

The proof just given is a proof of the theorem $P \vee -P$. Suppose, however, that we wished to prove $Q \vee -Q$; a moment's thought should convince us that, if we systematically changed each occurrence of 'P' in the given proof to 'Q', the result would be an equally sound proof of this further theorem. Suppose, again, that we wished to prove $(Q \rightarrow R) \vee -(Q \rightarrow R)$; slightly more thought should convince us that a similar change of 'P' to '$(Q \rightarrow R)$' throughout the proof will do the job. Consideration of such cases suggests that, in proving a theorem, we are implicitly proving a wide variety of other theorems closely related to the proved theorem by substitutions of the kind just instanced: so that it would be wasteful to prove these other theorems separately—it would involve virtual reduplication of the discovered proof. This in turn suggests a short cut to new results.

The matter can be made more precise by defining a *substitution-instance* of a given wff, as follows. A substitution-instance of a given wff is *a wff which results from the given wff by replacing one or more of the variables occurring in the wff throughout by some other wffs*, it being understood that each variable so replaced is replaced by the *same* wff. For example, '$(Q \rightarrow R) \vee -(Q \rightarrow R)$' is, by this definition, a substitution-instance of '$P \vee -P$', because it results from the latter wff by replacing the variable 'P' occurring in

'$P \vee -P$' throughout by the same wff '$(Q \rightarrow R)$'. Similarly, '$Q \vee -Q$' is a substitution-instance of '$P \vee -P$', and, in this case, conversely too.

Here is a more complex case. Consider the wffs:

(1) $P \rightarrow Q \vee -(-P \,\&\, Q)$;

(2) $R \vee S \rightarrow P \vee -(-(R \vee S) \,\&\, P)$.

Then (2) is a substitution-instance of (1), because (2) results from (1) by replacing the variable 'P' at its two occurrences in (1) by '$(R \vee S)$' and the variable 'Q' at its two occurrences in (1) by 'P'.

It is worth stressing two features of substitution which are easily and often forgotten. First, the substitution must be made *uniformly*—i.e. throughout—for each substituted variable: the *same* wff must be substituted for *every* occurrence of a given variable for a substitution-instance to result. Second, it is only on *propositional variables* that this substitution can be performed, and *not*, for example, on negated variables. Thus

(3) $-S \rightarrow Q \vee -(S \,\&\, Q)$

is not a substitution-instance of (1), by our definition, though

(4) $-S \rightarrow Q \vee -(--S \,\&\, Q)$

is a substitution-instance of (1): if we replace 'P' in (1) by '$-S$' throughout, we obtain (4) but not (3). Hence a substitution-instance of a wff will always be at least as long as the given wff, and none of the connectives in the given wff disappear in the substitution-instance. In an obvious though vague sense, a substitution-instance has the same broad structure as the original.

Now we can say that a proof of a theorem constitutes implicit proof of all the (indefinitely many) possible substitution-instances of that theorem. The proof of $P \rightarrow P$ (38 above) is implicitly a proof of any theorem of the form $\mathrm{A} \rightarrow \mathrm{A}$, for *any* wff A, and so implicitly a proof of $(-P \rightarrow Q) \rightarrow (-P \rightarrow Q)$, $R \vee S \rightarrow R \vee S$, and so on. More precisely, suppose that the wff A expresses a theorem for which we have a proof, and suppose that B is some variable occurring in A. Then, if we systematically replace B throughout the proof of A by some other wff C, we obtain a new proof of that substitution-instance of A which results from replacing B throughout A by C. And this can be extended readily to substitution for more than one variable in A. That the new proof really is a proof—that all the applications of the rules of derivation remain correct applications after the substitution has been performed—can be seen by inspecting the rules themselves; for the rules concern only the broad structure of the wffs involved, and this structure is unaffected by substitution. We may summarize our result in the following form:

(S1) A proof can be found for any substitution-instance of a proved theorem.

This result for theorems can be extended to sequents in general. We may define a *substitution-instance of a sequent-expression* as *any sequent-expression which results from the given sequent-expression by replacing one or more of the variables occurring in some wff in the sequent-expression throughout the sequent-expression by some other wffs*, it being understood that each variable so replaced is replaced by the *same* wff. (This definition virtually becomes the earlier definition in the limiting case that the sequent-expression contains just one wff.) For example, sequent 2 is a substitution-instance of sequent 1, and

(5) $P \rightarrow (Q \;\&\; R \rightarrow --S), P, ---S \vdash -(Q \;\&\; R)$

is a substitution-instance of

(6) $P \rightarrow (Q \rightarrow R), P, -R \vdash -Q$,

obtained by substituting throughout '$(Q \;\&\; R)$' for 'Q' and '$--S$' for 'R'. We proved that (6) expresses a valid sequent as proof 6. We can now see that the proof of 6 constitutes implicit proof of the sequent-expression (5) also. By entirely similar reasoning, we obtain a generalization of the principle (S1):

(S2) A proof can be found for any substitution-instance of a proved sequent.

The proof is indeed obtained by performing the relevant substitutions systematically throughout the given proof, whereupon all applications of rules of derivation remain correct applications in the new proof.

The principles (S1) and (S2) reveal an important property of our proved results, that of *generality*. We introduced symbols 'P', 'Q', 'R', etc., at the outset as stand-ins for *particular* sentences of ordinary speech, which had the merit that they helped to reveal the logical form of complex sentences—a form that was shared by other sentences. We can now see that they in fact deserve the label 'variable', since a theorem or sequent proved for P is implicitly proved for *any* proposition of the propositional calculus, just as a result in algebra containing 'x' is implicitly a result about any number. In this way, our results, though stated for particular propositions, implicitly concern any proposition expressible in our notation, and are quite general in content.

We may take advantage of theorems and their substitution-instances to shorten proofs by the *rule of theorem introduction* (TI). This rule permits us to introduce, at any stage of a proof, a theorem already proved or a substitution-instance of such a theorem. At the right, we cite TI (or TI(S), if a substitution-instance is involved) together with the number of the theorem proved. On the left, of course, no numbers appear, since theorems depend on no assumptions. For example:

45 $P \vdash (P \& Q) \vee (P \& -Q)$

1	(1) P	A
	(2) $Q \vee -Q$	TI(S) 44
3	(3) Q	A
1,3	(4) $P \& Q$	1,3 &I
1,3	(5) $(P \& Q) \vee (P \& -Q)$	4 vI
6	(6) $-Q$	A
1,6	(7) $P \& -Q$	1,6 &I
1,6	(8) $(P \& Q) \vee (P \& -Q)$	7 vI
1	(9) $(P \& Q) \vee (P \& -Q)$	2,3,5,6,8 vE

After assuming P, we introduce (line (2)) the law of excluded middle, 44, under a substitution-instance, and then proceed by vE, assuming each disjunct of the law in turn (lines (3) and (6)), and obtaining the desired conclusion from each (lines (5) and (8)). When we apply vE at line (9), the conclusion rests only on P, since the disjunction at (2), being a theorem, rests on no assumptions.

46 $P \rightarrow Q \vdash P \& Q \leftrightarrow P$

1	(1) $P \rightarrow Q$	A
	(2) $P \& Q \rightarrow P$	TI 41

3	(3) P	A
1,3	(4) Q	1,3 MPP
1,3	(5) $P \& Q$	3,4 &I
1	(6) $P \rightarrow P \& Q$	3,5 CP
1	(7) $(P \& Q \rightarrow P) \& (P \rightarrow P \& Q)$	2,6 &I
	(8) $P \& Q \leftrightarrow P$	7 *Df.* $\leftrightarrow$

To obtain the biconditional $P \& Q \leftrightarrow P$, we aim separately at the two conditionals $P \& Q \rightarrow P$ and $P \rightarrow P \& Q$; but the first is a proved theorem, 41, which we therefore introduce directly by TI. Conjoining 27 and 46, we have the interderivability result

47 $P \& Q \leftrightarrow P \dashv\vdash P \rightarrow Q$.

The rule TI is *not* a new fundamental rule of derivation: it does not enable us to prove sequents which we cannot otherwise prove by applications of our basic ten rules; it merely enables us to prove *more briefly* further results by using results already proved. In the case of 45, for example, we could prefix the proof given by 8 lines, corresponding to the first 8 lines of the proof of 44 but with 'Q' in place of 'P', and then continue as before, renumbering (1) to (9) as (9) to (17). In place of TI(S) 44, we would read on the right 8 DN (compare line (9) of 44), and thus obtain a complete, if lengthy, proof of 45 from our basic rules. Whenever a theorem is introduced by TI, we can prefix the proof given by a proof of the theorem from basic rules, and thus transform the proof into a lengthier proof from first principles: only a certain renumbering of lines is involved. Rules of this character, which expedite our proof-techniques but can be shown not to increase our derivational power, are called *derived rules*, in contrast to our basic ten rules, which may be called *primitive rules*.

Having seen this use of theorems to shorten proofs, we naturally ask whether an analogous rule will enable us to use sequents already proved. For example, suppose that we have proved, on certain assumptions, $P \rightarrow Q$. Then, by sequent 9 ($P \rightarrow Q \vdash -Q \rightarrow -P$), we should be able to conclude, without special proof, $-Q \rightarrow -P$ on the same assumptions. Or suppose that we have proved, on various assumptions, $P \rightarrow Q$, $Q \rightarrow R$, and P. Then, by sequent 3 ($P \rightarrow Q$, $Q \rightarrow R$, $P \vdash R$), we should be able to conclude, without special proof, R on the pool of these assumptions. And this should apply not only to the sequents actually proved but to any substitution-instances of them too, in virtue of (S2).

The *rule of sequent introduction* (SI), again a derived not a primitive rule, enables us to do just this. It is a little complex both to state and to justify in full generality, but its main function should be clear from examples. Suppose that we have as conclusions in a proof $A_1, A_2, \ldots, A_n$, on various assumptions, and suppose that $A_1, A_2, \ldots, A_n \vdash B$ is a (substitution-instance of a) sequent for which we already have a proof; then SI permits us to draw B as a conclusion on the pool of the assumptions on which $A_1, A_2, \ldots, A_n$ rest. SI may be justified as follows. By hypothesis (and (S2) if necessary), we have a proof using only primitive rules of

(i) $A_1, A_2, \ldots, A_n \vdash B$.

Hence, by n successive steps of CP added to the proof, we can prove as a theorem

(ii) $A_1 \rightarrow (A_2 \rightarrow (\ldots (A_n \rightarrow B) \ldots))$

(the conditional theorem corresponding to the sequent in the way in which the conclusion of 43 above corresponds to 4). Hence by TI we can introduce (ii) into the proof given with conclusions A_1, $A_2, \ldots, A_n$, as a new line resting on no assumptions. Now, by n successive steps of MPP, using in turn $A_1, A_2, \ldots, A_n$ as antecedents of given conditionals, we can draw as conclusion B. Evidently B will depend, as assumptions, on any propositions on which any of $A_1, A_2, \ldots, A_n$ depends. This justifies SI, in the sense that it shows how any proof using SI can be systematically transformed into a proof of the same sequent using only primitive rules—the step of TI involved can, as we already know, be eliminated in favour of these rules.

48 $-P \vee Q \vdash P \rightarrow Q$

1	(1) $-P \vee Q$	A
1	(2) $-(--P \;\&\; -Q)$	1 SI(S) 36(a)
1	(3) $--P \rightarrow Q$	2 SI(S) 35(b)
4	(4) P	A
4	(5) $--P$	4 DN

1,4	(6) Q	3,5 MPP
1	(7) $P \rightarrow Q$	4,6 CP

A substitution-instance of 36(a) is $-P \vee Q \vdash -(--P \,\&\, -Q)$, and a substitution-instance of 35(b) is $-(--P \,\&\, -Q) \vdash --P \rightarrow Q$: these two sequents are used to obtain (2) from (1) and (3) from (2) by SI. The rest of the proof is then immediate. Together with Exercise 1.5.1(i), 48 yields

49 $P \rightarrow Q \dashv\vdash -P \vee Q$.

50 $P \vdash Q \rightarrow P$

1	(1) P	A
1	(2) $-Q \vee P$	1 vI
1	(3) $Q \rightarrow P$	2 SI(S) 48

51 $-P \vdash P \rightarrow Q$

1	(1) $-P$	A
1	(2) $-P \vee Q$	1 vI
1	(3) $P \rightarrow Q$	2 SI 48

52 $-P, P \vee Q \vdash Q$

1	(1) $-P$	A
2	(2) $P \vee Q$	A
3	(3) P	A
1	(4) $P \rightarrow Q$	1 SI 51
1,3	(5) Q	3,4 MPP
6	(6) Q	A
1,2	(7) Q	2,3,5,6,6 vE

53 $-Q, P \vee Q \vdash P$

(Proof similar to 52.)

54 $\vdash (P \rightarrow Q) \vee (Q \rightarrow P)$

	(1) $P \vee -P$	TI 44
2	(2) P	A
2	(3) $Q \rightarrow P$	2 SI 50

2	(4) $(P \rightarrow Q) \vee (Q \rightarrow P)$	3 vI
5	(5) $-P$	A
5	(6) $P \rightarrow Q$	5 SI 51
5	(7) $(P \rightarrow Q) \vee (Q \rightarrow P)$	6 vI
	(8) $(P \rightarrow Q) \vee (Q \rightarrow P)$	1,2,4,5,7 vE

An interesting feature of this last series of results is its progressive nature: once 48 was proved, it was used to obtain 50 and 51, which in turn were employed in the proofs of 52 and 54. It should be clear by now that TI and SI are powerful devices for generating new theorems and sequents out of old. Our work now has the progressive character of a mathematical theory such as Euclidean geometry.

Of the latest results, 50 and 51 are sometimes called *the paradoxes of material implication.* To see their paradoxical flavour, bear in mind that Q in 50 and 51 may be *any* proposition, even one quite unrelated in content to P. Thus 50 enables us to conclude from the fact that Napoleon was French that if the moon is blue then Napoleon was French; and 51 enables us to conclude from the fact that Napoleon was not Chinese that if Napoleon was Chinese then the moon is blue. The name ' material implication ' was given by Bertrand Russell to the relation between P and Q expressed in our symbolism by '$P \rightarrow Q$'; we have been reading this ' if P then Q ', but it is clear from 50 and 51 that ' $\rightarrow$ ' has logical properties which we should not ordinarily associate with ' if . . . then . . .'. This discrepancy is chiefly brought about by the fact that, before we would ordinarily accept ' if P then Q ' as true, we should require that P and Q be connected in thought or content, whilst, as 50 and 51 show, no such requirement is imposed on the acceptance of '$P \rightarrow Q$'. However, whilst admitting that this discrepancy exists, we may continue safely to adopt '$P \rightarrow Q$' as a rendering of 'if P then Q' *serviceable for reasoning purposes*, since, as will emerge in Section 4, our rules at least have the property that they will never lead us from true assumptions to a false conclusion. And any reader who is inclined not to accept the validity of 50 and 51 is asked either to suspend judgement until this fact has been established or to indicate exactly which step in their proof he regards as faulty and which rule of derivation he thinks is unsafe and why. (A natural reply is that the step of vI at line (2) of each proof is unsound; but compare the justification of vI in Chapter 1, Section 3. Anyway, 50 and 51 can be proved using only the rules A, &I, &E, RAA, DN, and CP, in each case in nine lines; it is an instructive exercise to discover these ' independent ' proofs, since they reveal how difficult it is to ' escape ' the paradoxes.) Along with 23, therefore, we may classify 50 and 51 as some of the more surprising consequences of our primitive rules. 54 is a less well-known paradox: it claims as a logical truth that, for any propositions P and Q, it is either the case that if P then Q or the case that if Q then P. Either if it is raining it is snowing or if it is snowing it is raining.

The principle of reasoning associated with 52 and 53 has the medieval name *modus tollendo ponens*. This is the fourth medieval *modus* I have mentioned, and the last there is, so this is a good place to bring them together.

(i) *Modus ponendo ponens* is the principle that, if a conditional holds and also its antecedent, then its consequent holds;

(ii) *Modus tollendo tollens* is the principle that, if a conditional holds and also the negation of its consequent, then the negation of its antecedent holds;

(iii) *Modus ponendo tollens* is the principle that, if the negation of a conjunction holds and also one of its conjuncts, then the negation of its other conjunct holds;

(iv) *Modus tollendo ponens* is the principle that, if a disjunction holds and also the negation of one of its disjuncts, then the other disjunct holds.

(i) and (ii) have been embodied in our primitive rules MPP and MTT. Clearly, in virtue of SI and 52 and 53, a rule analogous to *modus tollendo ponens*, which we may call MTP, can be framed; this, as a *derived* rule, will merely be a special case of SI. It runs: given a disjunction and the negation of one disjunct, then we are permitted to derive the other disjunct as conclusion. When required, this rule will in fact be cited as MTP. Similarly, in virtue of SI and 34 and the readily proved $Q, -(P \& Q) \vdash -P$, we may formulate, as a special derived rule, MPT: given the negation of a conjunction and one of its conjuncts, then we are permitted to derive the negation of the other conjunct as conclusion.

In connection with the *modi*, it is finally worth noting that MTT need not have been taken as a primitive rule, but can be obtained as a derived rule from the others. Thus:

55 $P \rightarrow Q, -Q \vdash -P$

1	(1)	$P \rightarrow Q$	A
2	(2)	$-Q$	A
3	(3)	P	A
1,3	(4)	Q	1,3 MPP
1,2,3	(5)	$Q \& -Q$	2,4 &I
1,2	(6)	$-P$	3,5 RAA

We prove 55 without using MTT. In view of SI, 55 can be used to give exactly the effect of MTT as a derived rule. This would be of interest if we were trying to reduce our primitive rules to as small a number as possible—an important consideration in certain areas of logic.

Apart from the special cases of MTP and MPT, the most rewarding sequents for use with SI are the various forms of *de Morgan's laws*, as they are called, namely 36 and Exercise 1.5.1(*f*)–(*h*), which enable us to transform negated conjunctions and disjunctions into non-negated disjunctions and conjunctions respectively. Also worth remembering are 49 (enabling us to change conditionals into disjunctions), 35 (enabling us to change conditionals into negated conjunctions), Exercise 1.5.1(*e*) (enabling us to change conjunctions into negated conditionals), and Exercise 1.5.1(*c*) and (*d*) (the so-called *distributive laws*). Often it helps to introduce 44 and proceed by vE, as in the proof of 54. And the trick of using the paradoxes 50 and 51, as in the same proof, should be borne in mind.

EXERCISES

1 Using only the 10 primitive rules, prove the following sequents:

(*a*) $\vdash (Q \rightarrow R) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$

(*b*) $\vdash P \rightarrow (Q \rightarrow P \& Q)$

(*c*) $\vdash (P \rightarrow R) \rightarrow ((Q \rightarrow R) \rightarrow (P \vee Q \rightarrow R))$

(*d*) $\vdash (P \rightarrow Q \& -Q) \rightarrow -P$

(*e*) $\vdash (-P \rightarrow P) \rightarrow P$

2 The following are valid sequents, because they are substitution-instances of sequents already proved in this book. For each, cite by number the proved sequent of which it is a substitution-instance, and what substitutions have been used:

(*a*) $(P \rightarrow Q) \rightarrow P,\ P \rightarrow Q \vdash P$

(*b*) $--P \rightarrow ---P,\ ----P \vdash -P$

(*c*) $-P \,\&\, (Q \,\&\, R) \rightarrow Q \vee P \vdash -P \rightarrow (Q \,\&\, R \rightarrow Q \vee P)$

(*d*) $(-Q \rightarrow Q) \rightarrow -(-Q \rightarrow Q) \vdash -(-Q \rightarrow Q)$

(*e*) $-(S \vee P) \vdash S \vee P \rightarrow (P \,\&\, Q \leftrightarrow R \vee -S)$

3 Prove by primitive rules alone:

(*a*) $\vdash P \rightarrow P \vee Q$

Using this result, prove by primitive rules and TI:

(*b*) $Q \rightarrow P \vdash P \vee Q \leftrightarrow P$

In view of Exercise 1.4.1(*e*) this gives:

(*c*) $P \vee Q \leftrightarrow P \dashv\vdash Q \rightarrow P$

4 Prove, using primitive rules and SI in connection with 50:

(*a*) $P \,\&\, Q \dashv\vdash P \,\&\, (P \leftrightarrow Q)$

5 Using primitive or derived rules, together with any sequents or theorems already proved, prove:

(*a*) $\vdash P \vee (P \rightarrow Q)$

(*b*) $\vdash (P \rightarrow Q) \vee (Q \rightarrow R)$

(*c*) $\vdash ((P \rightarrow Q) \rightarrow P) \rightarrow P$

(*d*) $-Q \vdash P \rightarrow (Q \rightarrow R)$

(*e*) $P,\ -P \vdash Q$

(*f*) $P \vee Q \dashv\vdash -P \rightarrow Q$ (cf. Ex. 1.5.1(*j*))

(*g*) $-(P \rightarrow Q) \dashv\vdash P \,\&\, -Q$

(*h*) $(P \rightarrow Q) \rightarrow Q \dashv\vdash P \vee Q$

(*i*) $(P \rightarrow Q) \vee (P \rightarrow R) \dashv\vdash P \rightarrow Q \vee R$

(*j*) $P \rightarrow Q \dashv\vdash (P \leftrightarrow Q) \vee Q$

(*k*) $Q \vdash P \,\&\, Q \leftrightarrow P$

(*l*) $-Q \vdash P \vee Q \leftrightarrow P$

6 Let A and B be any propositions expressible in the propositional calculus notation.

(i) Show that A $\vdash$ B is provable by our rules if and only if it is provable that $\vdash$ A $\rightarrow$ B;

(ii) Show that A ⊣⊢ B is provable if and only if it is provable that ⊢ A ⟷ B.

7 In effect, our rule DN is two rules combined: (i) from A to derive – – A, and (ii) from – – A to derive A. Show that (i) can be obtained as a derived rule from the other primitive rules (compare the corresponding demonstration for the rule MTT, sequent 55).

3 TRUTH-TABLES

The last section has answered the first question raised at the beginning of this chapter. To help answer the other two questions (Are our rules of derivation safe? Are they complete?), we approach in this section the propositional calculus in a quite new way, by the technique of *truth-tables*. This technique will also incidentally afford us a method of showing the *invalidity* of sequents, whereas the rules of derivation merely show their validity. Truth-tables are easy to master, so our treatment here will be brisk.

The truth-table method is a method for *evaluating* wffs: we assign values (called *truth-values*) to the variables of a wff, and proceed by means of given tables to calculate the value of the whole wff. We may usefully compare the corresponding mathematical procedure for evaluating algebraic expressions, say

(1) $(x + y)z - (y + z)(y + x)$.

Let us assign the value 10 to x, 3 to y, and 5 to z. By substitution, we obtain

(2) $(10 + 3)5 - (3 + 5)(3 + 10)$.

Computation by given tables yields successively

(3) $13 \times 5 - 8 \times 13$;

(4) $65 \quad - \quad 104$;

(5) $- 39$.

The result at (5) is the value of the whole expression (1) for the assignment of values to the variables $x = 10$, $y = 3$, $z = 5$.

In the case of wffs of the propositional calculus, there are only two possible values which variables are permitted to take, the *true* and the *false*, which we mark by ‘ T ’ and ‘ F ’ respectively. Our assumption that there are only these two possibilities is in effect the assumption that every proposition is either true or false, and