Appendix L

A Little Logic **September 17, 2007, draft**

No exciting books suit feverish patients;
Unexciting books make one drowsy.
$\therefore$ *No books suit feverish patients, except such as make one drowsy.*

— Lewis Carroll

This appendix[1] reveals a bit of the logical infrastructure needed for mathematics—just enough, we hope, to get you going in reading and writing proofs. It discusses what is meant by combinations of statements formed with such words as 'or' and 'if…then', and how the quantifying phrases 'for every' and 'there exists' are applied. It points out some of the most common patterns of mathematical proof—*but your best guide to what patterns are considered legitimate are the actual proofs throughout this book.* What it includes is treated for the most part informally and descriptively.

One of the difficulties with learning logic is that logic ought to precede everything else in mathematics that uses it, yet, without any other mathematics to treat, logic is wholly abstract. Accordingly, to explain logical ideas we shall often have to talk about mathematical sets, numbers, functions, etc., along with a few examples from our everyday language about the real world. For the essentials about sets and functions, see Appendix A and Appendix B.

In a few instances—for example, the more generous meanings in logic of 'or' and 'there exists'—logical language differs a bit from everyday usage. Otherwise, logic just makes explicit and crisp those patterns of deductive reasoning used by careful speakers and writers.

L.1 The logic of solving equations

What is *really* going on, from a logical viewpoint, when you carry out familiar algebraic steps to solve an algebraic equation (or an inequality or a system of equations or of inequalities)?

Example L.1.1. Consider the quadratic equation $x^2 + x - 6 = 0$. To solve this, you would write something like this:

$$\begin{gathered} x^2 + x - 6 = 0 \\ (x-2)\,(x+3) = 0 \\ x - 2 = 0, \quad x + 3 = 0 \\ x = 2, \quad x = -3 \end{gathered}$$

and then write the solution as:

$$x = 2, -3$$

Several questions arise. First, what do the commas mean in the expressions '$x = 2, x = -3$' and '$x = 2, -3$'. We understand the commas to mean "or", so that both expressions mean '$x = 2$ or $x = -3$': there are two values of x that are solutions of the original equation.

Second, what is the connection between successive lines in the write-up? Presumably it is *not* just that an x satisfying the equation(s) in one line also satisfies the equation in the succeeding line, but also that an x satisfying the equation(s) in the succeeding line also satisfies the equation(s) in its preceding line. For example, it is not just that if a value of x satisfies $x^2 + x - 6 = 0$, then the same value of x satisfies $(x-2)\,(x+3) = 0$; but also, if a value of x satisfies $(x-2)\,(x+3) = 0$, then the same value of x satisfies $x^2 + x - 6 = 0$. In other words, you can not only "go" from one line to the next, but you can also "go" from that next line to the one preceding it: the steps are reversible.

Put more tersely, an x satisfies the equation(s) in one line *if and only if* it satisfies the equation(s) in the succeeding line: the assertions in the one line and the succeeding line are *logically equivalent* to one another. Such logical equivalence is indicated by the symbol $\iff$, which may be read as "if and only if". Thus a more careful write-up of the solution would be:

$$\begin{aligned} & x^2 + x - 6 = 0 \\ \iff\ & (x-2)\,(x+3) = 0 \\ \iff\ & x - 2 = 0 \text{ or } x + 3 = 0 \\ \iff\ & x = 2 \text{ or } x = -3 \end{aligned}$$

By the way, sometimes the two letters in 'or' are more than we want to write, and then we use the logical symbol $\vee$ to mean *or.* Thus, as we found above:

$$x^2 + x - 6 = 0 \iff x = 2 \vee x = -3$$

How would you answer the question of what the solution to the original quadratic equation is? You might write

$$x = 2, -3,$$

just as in the original write-up, and say, "The solutions are 2 and -3. Yes, you would doubtless use the word 'and', but surely you would not intend to suggest that a particular solution has both the values 2 and -3 at the same time! It is still a matter of 'or' rather than 'and'.

You can avoid the 'and'/'or' confusion in such situations by using an expression such as '$x = 2$ or $x = -3$' explicitly involving 'or'. You can also avoid the confusion by giving the *solution set* of the equation—the set of all solutions. In the example, the two numbers 2 and -3 are solutions, and no other number is a solution. Thus the solution set S is given by

$$S = \{2, -3\},$$

and this means exactly

$$S = \{\, x : x = 2 \text{ or } x = -3 \,\}.$$

Thus a number x belongs to the set S exactly when $x = 2$ or $x = -3$; more briefly:

$$x \in S \iff (x = 2 \text{ or } x = -3)$$

Unless you are careful about the logic of what you are doing, you may get results that are not only confusing, but actually wrong. Look at the next example.

Example L.1.2. Consider the algebraic equation $x + \sqrt{x^2 - 5} = 1$. To solve this, you might write

$$\begin{aligned}
x + \sqrt{x^2 - 5} &= 1 \\
\sqrt{x^2 - 5} &= -x + 1 \\
\left(\sqrt{x^2 - 5}\right)^2 &= (-x + 1)^2 \\
x^2 - 5 &= x^2 - 2x + 1 \\
2x &= 6 \\
x &= 3
\end{aligned}$$

and thereby conclude that the given equation has unique solution 3. But you would be wrong! In fact, 3 does not satisfy the original equation:

$$3 + \sqrt{3^2 - 5} = 3 + 2 = 5 \neq 1$$

So what went wrong? There were no slip-ups in the algebraic manipulations, and each step in the write-up from one equation to the next is correct. What is wrong is that one of the steps is *not* reversible: the step from $\sqrt{x^2 - 5} = -x + 1$ to $\left(\sqrt{x^2 - 5}\right)^2 = (-x + 1)^2$. (Every other step is reversible.) In general, it is correct that if $a = b$, then $a^2 = b^2$. However, it is *not* in general correct that if $a^2 = b^2$, then $a = b$. All you can conclude from $a^2 = b^2$ is that $a = b$ or $a = -b$. In the situation with our equation, take $a = \sqrt{x^2 - 5}$ and $b = -x + 1$ and note that $a^2 = x^2 - 5$ (because $(\sqrt{p})^2 = p$ for every positive number p).

In view of the preceding analysis, a careful write-up of the solution would be:

$$\begin{aligned}
& x + \sqrt{x^2 - 5} = 1 \\
\iff\ & \sqrt{x^2 - 5} = -x + 1 \\
\implies\ & \left(\sqrt{x^2 - 5}\right)^2 = (-x + 1)^2 && (\textit{not} \iff!) \\
\iff\ & x^2 - 5 = x^2 - 2x + 1 \\
\iff\ & 2x = 6 \\
\iff\ & x = 3
\end{aligned}$$

There is one step having just an *if…, then* form—*implication*—as indicated by the symbol $\implies$; since that step is not reversible, the implication $\implies$ cannot be replaced with a logical equivalence $\iff$. Hence all that the write-up tells us is: If x satisfies the original equation, then x must have value 3. But, as we checked, 3 is not a solution of the original equation; 3 is, as some people refer to it, an “extraneous” solution, which was obtained by squaring the square-root.

The given equation has *no* solutions whatsoever. Then its solution set S is the set to which no number belongs:

$$S = \{\,\}$$

This set with no elements is the **empty set**, denoted by $\emptyset$.

Strictly speaking, none of the logical equivalences or implications used above make sense, because they are not qualified in any way as to the domain of values of their variable x for which they are allegedly true. Thus, in Example L.1.1 about solving the equation $x^2 + x - 6 = 0$, probably the intent was to find the real numbers x that are solutions. In that case, the write-up of the solution at the bottom of page L2, should really look like this:

$$\begin{aligned}(\forall x \in \mathbb{R})\big(\, x^2 + x - 6 = 0 &\iff (x-2)\,(x+3) = 0\\ &\iff x - 2 = 0 \text{ or } x + 3 = 0\\ &\iff x = 2 \text{ or } x = -3\,\big)\end{aligned}$$

Here the initial string $(\forall x \in \mathbb{R})$ is read as "For all x in $\mathbb{R}$", or more verbosely as "For all real numbers x". Here $\mathbb{R}$ stands for the set of all real numbers. And then the intention is that each of the equivalences is true for every real number.

As it so happens, the solutions of the equation $x^2 - x - 6$ are integers—elements of the set $\mathbb{Z}$ of all integers—so it would be equally correct to write:

$$\begin{aligned}(\forall x \in \mathbb{Z})\big(\, x^2 + x - 6 = 0 &\iff (x-2)\,(x+3) = 0\\ &\iff x - 2 = 0 \text{ or } x + 3 = 0\\ &\iff x = 2 \text{ or } x = -3\,\big)\end{aligned}$$

Of course until you actually work through the steps of solving the equation, you would not necessarily know that the solutions were actually integers. So it would be safer to work with $\mathbb{R}$ instead of with $\mathbb{Z}$.

But for some other equations, not even $\mathbb{R}$ might be a large enough set of numbers: you might need, say, the set $\mathbb{C}$ of all complex numbers. For example:

$$\begin{aligned}(\forall x \in \mathbb{C})\big(\, x^2 + 9 = 0 &\iff (x-3i)\,(x+3i) = 0\\ &\iff x - 3i = 0 \text{ or } x - (-3i) = 0\\ &\iff x = 3i \text{ or } x = -3i\,\big)\end{aligned}$$

Here i is the complex number having the property that $i^2 = -1$. Thus the solution set here is $\{3i, -3i\}$.

Exercise L.1.3. Suppose, nonetheless, you tried to work out a solution of $x^2 + 9 = 0$ using the set $\mathbb{R}$ of real numbers:

$$(\forall x \in \mathbb{R})\big(\, x^2 + 9 = 0 \iff x \ldots\big)$$

What might you write as the end, where the dots are? (This is a question you might need to ponder for a while!) And what is the solution set—as a subset of $\mathbb{R}$?

The equation $x^2 + x - 6 = 0$ has at least one solution (in fact, it has precisely two solutions) that are real numbers. To indicate it has at least one, we write:

$$(\exists x \in \mathbb{R})(x^2 + x - 6 = 0)$$

The string $(\exists x \in \mathbb{R})$ is read as "There exists "x in $\mathbb{R}$" or, more verbosely, "There exists a real number x".

The logical connectives *or*, *implies* ($\Longrightarrow$), and *if and only if* ($\Longleftrightarrow$) already used above, as well as the connectives *not* ($\neg$) and *and* (&), can help solve inequalities, too.

Example L.1.4. The problem we pose is to solve $|2x - 1| \geq 3$. But it is simpler to solve the inequality $|2x - 1| < 3$:

$$\begin{aligned} |2x-1| < 3 &\iff -3 < 2x - 1 < 3 \\ &\iff -2 < 2x < 4 \\ &\iff -1 < x < 2. \end{aligned}$$

In other words,

$$|2x - 1| < 3 \iff -1 < x \,\&\, x < 2.$$

Then

$$\begin{aligned} |2x-1| \geq 3 &\iff \neg(|2x-1| < 3) \\ &\iff \neg(-1 < x \,\&\, x < 2) \\ &\iff \big(\neg(-1 < x)\big) \text{ or } \big(\neg(x < 2)\big) \\ &\iff x \leq -1 \text{ or } x \geq 2 \end{aligned}$$

The next-to-last equivalence above used one of De Morgan's Laws of logic (Tautologies L.4.10), namely, $\neg(P \,\&\, Q) \iff \big((\neg P) \text{ or } (\neg Q)\big)$.

In terms of sets, the solution set T of $|2x - 1| < 3$ is

$$\begin{aligned} T &= (-1, 2) = \{\, x : -1 < x \,\&\, x < 2 \,\} \\ &= \{\, x : -1 < x \,\} \cap \{\, x : x < 2 \,\} = (-1, \infty) \cap (-\infty, 2) \end{aligned}$$

whereas the solution set S of the original inequality $|2x - 1| \geq 3$, we found, is

$$\begin{aligned} S &= \{\, x : x \leq -1 \text{ or } x \geq 2 \,\} = \{\, x : x \leq -1 \,\} \cup \{\, x : x \geq 2 \,\} \\ &= (-\infty, -1] \cup [2, \infty). \end{aligned}$$

The logical equivalence $|2x - 1| \geq 3 \iff \neg(|2x - 1| < 3)$ may be expressed in terms of the solution sets S and T of $|2x - 1| \geq 3$ and $|2x - 1| < 3$, respectively, as

$$S = \mathbb{R} \setminus T.$$

In other words, the subset S of the set $\mathbb{R}$ of all real numbers is the *complement* in $\mathbb{R}$ of its subset T. Thus

$$S = \mathbb{R} \setminus \big(\, (-1, \infty) \cap (-\infty, 2) \,\big)\,.$$

(Notice the different meanings of parentheses there: the inside ones are used to denote open rays, whereas the outer ones are punctuation.) One of De Morgan's Laws about sets (Proposition A.1.4) implies that

$$\begin{aligned} S = \mathbb{R} \setminus \big((-1, \infty) \cap (-\infty, 2) \big) &= \big(\mathbb{R} \setminus (-1, \infty) \big) \cup \big(\mathbb{R} \setminus (-\infty, 2) \big) \\ &= (-\infty, -1] \cup [2, \infty). \end{aligned}$$

Of course, that is the same solution set obtained before.

Exercises L.1.5. Give careful write-ups, including appropriate use of 'or', &, $\Longrightarrow$, and $\Longleftrightarrow$, for solving the equation(s) or inequality. Do this both without using, and with using, the $\forall$ qualification. Then tell what the solution set is, using the set-builder notation $\{\dots\}$.

(1) $x^3 - 2x^2 - 5x + 6 = 0$

(2) $(x-1)(x+2) < 0$

(3) $(x-1)^2 < 4$

(4) $x + 4 = \sqrt{2x^2 + 14x}$

(5) $\begin{cases} x(x^2 + y^2 - 1) = 0, \\ y(x^2 + y^2 - 1) = 0 \end{cases}$

Exercise L.1.6. The equation $x + \sqrt{x^2 - 5} = 1$ in Example L.1.2 has no solutions whatsoever, and we indicated this by writing that its solution set is the empty set $\varnothing$. How, without referring to the solution set, might you indicate that the equation has no solutions? (*Hint:* Recall that the notation $\exists$ may be used to indicate existence of an equation's solution.)

Exercise L.1.7. Let $f(x) = 5x^4 - x^5$. Determine:

(a) the set $\{x : f'(x) = 0\}$ of all critical points of f;

(b) the set $\{x : f'(x) > 0\}$ on which f is increasing and the set $\{x : f'(x) < 0\}$ on which f is decreasing;

(c) the set $\{x : f''(x) > 0\}$ on which f is concave upward and the set $\{x : f''(x) < 0\}$ on which f is concave downward.

Exercise L.1.8. For which values of x is $\sqrt{x/(1-x)}$ defined as a real number? In other words, in Calculus I terms, what is the domain of $\sqrt{x/(1-x)}$?

L.2 Formulas and Statements

Section L.1 introduced informally the logical symbols $\vee$, &, $\iff$, and $\implies$, which connect statements about mathematical objects. In order to understand just how these logical symbols behave, you need first to understand how to form such statements and objects. And to understand that involves looking at a rather "formal" description of the language of logic and mathematics.

To begin, we need *symbols.* Our symbols will include:

- **letters**, such as x, C, $\mathbb{N}$, and $\mathcal{A}$ (to make things more readable and to prevent us from running out of letters when many are involved, we allow letters to be ornamented in various ways, such as x', b'', A_0, y_{99}, $\mathbb{N}^*$, $\vec{v}$);

- the logical **connectives** $\neg$ (negation), $\vee$ (disjunction), $\wedge$ (conjunction), $\implies$ (implication), and $\iff$ (equivalence);

- the logical **quantifiers** $\forall$ (universal quantifier), $\exists$ (existential quantifier), and $\imath$ (descriptor);

- the set-theoretic signs $=$ (equality) and $\in$ (elementhood)—the latter not to be confused with the Greek epsilon, ε; and

- parentheses, as punctuation marks.

In actual mathematical writing, we often use ordinary words and whole phrases instead of the connectives, quantifiers, and other symbols. Such words and phrases, used as shown in Table L.1 on page L9, suggest the meanings we intend for the corresponding symbols. Here are some mnemonics for the logical connectives and quantifiers:

- The symbol $\neg$ is reminiscent of a negative sign; it means *not.*

- The symbol & is the usual ampersand; it means *and.*

- The symbol $\implies$ in $P \implies Q$ goes from P to Q; it means *if* P*, then* Q.

- The symbol $\iff$ in $P \iff Q$ goes from P to Q as well as from Q back to P; it means P *if and only if* Q.

- The symbol $\forall$ resembles an upside-down letter A; it means *for* ***a****ll.*

- The symbol $\exists$ resembles a backwards letter E; it means *there* ***e****xists.*

(The descriptor $\imath$ is an upside-down Greek letter iota, ι.) When we use such words as part of English sentences with embedded mathematical

Table L.1: Meanings of logical symbols.

Symbolism	*Meanings*
$\neg(P)$	not P it is not the case that P
$(P)\,\&\,(Q)$	P and Q both P and Q P but Q P yet Q P whereas Q
$(P) \vee (Q)$	P or Q P and/or Q either P or Q or both P and Q
$(P) \implies (Q)$	P implies Q if P, then Q P only if Q Q if P Q provided that P P is sufficient for Q Q is necessary for P Q because P Q since P P whence Q
$(P) \iff (Q)$	P if and only if Q P iff Q P is (logically) equivalent to Q P is necessary and sufficient for Q P precisely when Q
$(\forall x)(P)$	for all x, P for every x, P for each x, P for arbitrary x, P for any x, P
$(\exists x)(P)$	there exists x such that P there is an x such that P for some x, P
$(\imath x)(P)$	the x such that P the unique x such that P
$x = y$	x equals y
$x \in Y$	x is an element of Y x is a member of Y x belongs to Y x is in Y

symbolism, we shall also use commas and other punctuation besides parentheses.

Writing one or more of such symbols in succession gives us a *string.* For example, 'x', '=', and '$x \in A$' are strings.[2]

A letter x is said to be **bound** in a string S in case any one of the strings $(\forall x)$, $(\exists x)$, $(\imath x)$ occurs as part of S.[3] Otherwise, the letter is said to be **free** in the string. In particular, the letter is free in the string if it does not occur there at all. Here are two examples, which use the notations $\mathbb{N}$ for the set $\{0, 1, 2, \dots\}$ of all natural numbers and $\mathbb{Z}$ for the set $\{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ of all integers. First, n is bound in

$$(\forall n)(n \in \mathbb{N} \implies 2n > n)$$

(which means that the double of each natural number is greater than the number itself). Second, n is bound in

$$(\imath n)(n \in \mathbb{Z} \;\&\; 2n = n)$$

(which represents the one and only natural number whose double is itself, namely, 0). However, n is free in each of the three strings:

$$2n > n, \qquad n \in \mathbb{N} \implies 2n > n, \qquad k \in \mathbb{N} \implies 2k > k$$

When a particular occurrence of a letter x is bound in a string S because that occurrence is within part of S that has one of the three form $(\forall x)(P)$, $(\exists x)(P)$, $(\imath x)(P)$, then that occurrence of x is said to be **within the scope** of that quantifier $\forall$, $\exists$, or $\imath$.

Most strings we could write would be utter nonsense—the sort of thing a roomful of monkeys typing at random would produce before they ever happened to get around to Shakespeare. The strings that are to be regarded as meaningful are *terms* and *formulas.* Informally, a term denotes an object that the logical language talks about, such as: the natural number 0, the set of those x for which $x \neq x$, the set of natural numbers, the variable x. A formula, by contrast, denotes an

[2]We just mentioned—talked about—three specific strings, and therefore used single quotes around them in order to name them. In a formal presentation of logic, we would have to distinguish carefully between things and the names of things. In our informal treatment, we shall be rather sloppy about the distinction, and we will revert to the more careful naming only when it would be utterly confusing not to do so. For example, once we begin to use the word 'and' in place of the connective &, to mean '$P \,\&\, Q$' we shall need to write "'P and Q'" rather than "P and Q", lest we confuse the latter with the phrase "'P' and 'Q'", as in the assertion: "The statements 'P' and 'Q' are true."

[3]We just did it—confused the name of a thing with the thing itself. When we wrote "in a string S", we did *not* necessarily mean to refer to the one-letter string 'S', but rather, an arbitrary string that we are temporarily naming 'S'.

assertion—not necessarily true!—about such objects, such as:

$$3 \in \mathbb{N},$$
$$1/2 + 1/3 = 1/5,$$
$$(\exists x)\,\big(x \in \mathbb{R} \;\&\; (\forall y)(y \in \mathbb{R} \implies x > y)\big).$$

Thus a formula in the sense meant here need not at all be a formula in the customary sense, such as $V = \pi r^2 h$, telling how to compute one quantity from others.

More formally, **terms** and **formulas** are those strings that can be built up by a finite number of applications of the following rules:

- each letter is a term;
- if X and Y are terms, then both $X = Y$ and $X \in Y$ are formulas;
- if P is a formula, then $\neg(P)$ is a formula;
- if P and Q are formulas, then each of $(P) \vee (Q)$, $(P) \wedge (Q)$, $(P) \implies (Q)$, and $(P) \iff (Q)$ are formulas;
- if P is a formula and x is a letter that is *free* in P, then both $(\forall x)(P)$ and $(\exists x)(P)$ are formulas; and
- if P is a formula and x is a letter that is *free* in P, then $(\imath x)(P)$ is a term.

For example,

$$(\forall x)\big(\neg(x = x)\big) \tag{*}$$

and

$$(\imath A)\,\big((\forall x)\,\big((x \in A) \iff (\neg(x = x))\big)\big) \tag{**}$$

are formulas. (The first of these makes the *false* statement that each object is unequal to itself. The second represents the object characterized by the property that no object belongs to it—the *empty set*).

Notice that a string such as $(\forall x)\big((\exists x)(x = x)\big)$ is *not* a formula according to the preceding rules, because the letter x is already bound in $(\forall x)(x = x)$. On the other hand, $(\forall x)\big((\exists y)(x \in y)\big)$ is a formula.

Obviously formulas and terms written in strict compliance with those rules can be awkward to read because of their length and all the nested parentheses. In practice, we shorten such strings to make them more readable (and writable!). One way to do so is to omit any pair of parentheses immediately surrounding any *quantified* formula—one of the form $(\forall x)(P)$, $(\exists x)(P)$, or $(\imath x)(P)$—in a larger formula. Thus, we write

$$(\forall x)(\exists Y)(x \in Y)$$

to mean
$$(\forall x)\big((\exists Y)(x \in Y)\big)$$
and write
$$(\forall x)(x = x) \vee (\exists y)\big(\neg(y = y)\big)$$
to mean
$$\big((\forall x)(x = x)\big) \vee \big((\exists y)(\neg(y = y))\big)\,.$$

Terms and formulas become still shorter and more readable when additional parentheses are omitted in accordance with a rule of *order of precedence*. The order of precedence in logic is similar to the one in algebra where multiplication takes precedence over addition, so that $x \cdot y + z$ means $(x \cdot y) + z$ rather than $x \cdot (y + z)$. In logic, if we consider the connectives and set-theoretic signs in the order

$$\longleftarrow \textit{ weaker} \qquad = \quad \in \quad \neg \quad \& \quad \vee \quad \Longrightarrow \quad \Longleftrightarrow \qquad \textit{stronger } \longrightarrow$$

from "weakest" to "strongest", then the rule is: **when parentheses are missing, the stronger sign reaches further.** For example, $x \in A \vee x \in B$ means $(x \in A) \vee (x \in B)$, and $x = y \implies x \in A$ means $(x = y) \implies (x \in A)$. The formula (*) on page L11 may now be written in the shorter form
$$(\forall x)(\neg\, x = x)$$
and the term (**) on page L11 may now be written much more readably as:
$$(\iota A)(\forall x)(x \in A \iff \neg\, x = x)$$

The rule of precedence hardly allows us to remove all parentheses. For example, the string
$$P \implies Q \implies \neg\, Q \implies \neg P$$
is ambiguous. When parenthesized as
$$(P \Longrightarrow Q) \implies (\neg\, Q \Longrightarrow \neg P)$$
it will turn out to be a true formula no matter what the formulas P and Q are; when parenthesized as
$$\big(P \Longrightarrow (Q \Longrightarrow \neg\, Q)\big) \implies \neg P,$$
it is a formula that is true for some formulas P and Q but false for others (namely, when P is true and Q is false).

Such examples suggest two of the commonly used **definitions**—abbreviations, in effect—shown in Table L.2. These definitions provide another way to shorten formulas and terms.

Table L.2: Some common logical abbreviations.

Abbreviation	*Stands for*	*Meaning*
$x \neq y$	$\neg(x = y)$	x is not equal to y
$x \notin A$	$\neg(x \in A)$	x is not an element of A
$(\forall x \in X)(P)$	$(\forall x)(x \in X \Longrightarrow P)$	for all x in X, P
$(\exists x \in X)(P)$	$(\exists x)((x \in X)\ \&\ (P))$	there exists x in X such that P

With the first of the abbreviations in Table L.2, along with omissions of superfluous parentheses, the formula (*) and the term (**) from page L11 may be written in the still shorter forms

$$(\forall x)(x \neq x)$$

and

$$(\iota A)(\forall x)\,(x \in A \iff x \neq x).$$

What do you now think the preceding formula and term mean? (Use Tables L.1 and L.2.)

Some quantified formulas, such as $(\forall x)(x = x)$, are intended to make "universal" statements about all possible objects. Many quantified formulas, however, are intended to make statements about only those objects that are elements of some particular set. Here are two, expressed in typically informal mathematical language:

Every integer n that is a multiple of 4 is even.
Some real number has square 2.

These statements are, in other words:

For every integer n, if n is a multiple of 4, then n is even.
There is a real number x such that $x^2 = 2$.

The intended meanings of these statements are:

For every $n \in \mathbb{Z}$, if n is a multiple of 4, then n is even.
There exists $x \in \mathbb{R}$ such that $x^2 = 2$.

And the latter two statements, in turn, are understood to mean:

For every n, if $n \in \mathbb{Z}$, then: if n is a multiple of 4, then n is even.
There exists x such that $x \in \mathbb{R}$ and $x^2 = 2$.

Using the final two abbreviations in Table L.2, we may express these statements more formally, using quantifiers, as:

$$(\forall n \in \mathbb{Z})(n \text{ is a multiple of } 4 \implies n \text{ is even}).$$
$$(\exists x \in \mathbb{R})(x^2 = 2).$$

Suppose you were asked to prove the first of these two statements. To do so, you would, of course, have to know the precise meaning of 'n is a multiple of 4' and 'n is even'. By definition, n is even when $n = 2\,k$ for some integer k, that is:

$$(\exists k \in \mathbb{Z})(n = 2\,k)$$

Exercise L.2.1. (a) Write a definition for 'n is a multiple of 4', first including words and then using symbols alone.

(b) Using your definition from (a) and the meaning of *even*, now prove: $(\forall n \in \mathbb{Z})(n \text{ is a multiple of } 4 \implies n \text{ is even})$.

(c) What, if anything, is wrong with the following proof of the statement in (b)?

> *"Proof."* Let $n \in \mathbb{Z}$. Assume n is a multiple of 4. Let k be an integer for which $n = 4\,k$; such exists by the meaning of 'multiple of 4'. Then also $n = 2\,k$. This means that n is even.

(d) Is it true that $(\forall n \in \mathbb{Z})(n \text{ is even} \implies n \text{ is a multiple of } 4)$? If so, prove it; if not, tell why not.

Exercise L.2.2. Symbolize the formula saying that for no integer $n > 2$ does the equation $a^n + b^n = c^n$ have a solution in integers a, b, and c other than $a = b = c = 0$. (You may use the term $\mathbb{Z}$—the set of all integers.) Then try to write the symbolized formula without using the abbreviations and omissions of parentheses discussed above.

Exercise L.2.3. Symbolize the following sentences:

(a) The squares of real numbers are nonnegative.

(b) A differentiable function is continuous. (Use $\mathcal{F}$ to denote the set of all real-valued functions of a real variable.)

According to the rules for forming terms and formulas, terms are of two types—those of the form $(\imath x)(P)$ and those that are single letters. A term of the form $(\imath x)(P)$ represents a specific object; such a term is like a proper noun ('Neil Armstrong') or a definite description ('the first human to walk on the Moon') in ordinary English. A term that is a single letter—also called a **variable**—ambiguously represents an unspecified object; a variable is like a common noun ('a person', 'a thing') or a pronoun ('she', 'it').

When a formula or term is, or includes, a string of the form $(\forall x)(P)$, $(\exists x)(P)$, or $(\iota x)(P)$, then the letter x is sometimes called a *dummy variable.* This terminology is used to indicate that, without the meaning being altered, the variable could be replaced by any other letter not already occurring in that formula or term. Thus, the two formulas

$$\text{For every } x \in \mathbb{N},\, x^2 \geq 0$$
$$\text{For every } n \in \mathbb{N},\, n^2 \geq 0$$

although different, say in effect the same thing (namely, that the square of each natural number is nonnegative). We stipulate that in such a case, one is true exactly when the other is true. Likewise, the terms

$$(\iota y)(\forall x)\,(x \in y \iff x \neq x)$$
$$(\iota S)(\forall y)\,(y \in S \iff y \neq y)$$

are different but represent the same object, namely, the empty set $\varnothing$. We stipulate that in such a case, the two objects are equal.

The situation with dummy variables in logic is akin to the one in calculus, where the letter x in $\int_0^1 e^{-x^2}\,dx$ is a dummy variable that could be replaced by any other letter (except *e* and *d*): $\int_0^1 e^{-x^2}\,dx = \int_0^1 e^{-t^2}\,dt$. But it is different from the situation with limits, where there is a distinction between limit of a function of a real variable x, on the one hand, and the limit of a sequence defined in terms of a discrete, integer-valued variable n, on the other hand. The convention in calculus is that letters such as x and y and t refer to real variables, whereas letters such as m and m and k refer to integers. Thus the statement $\lim_{x\to\infty} 2x/(1+x) = 2$ refers to the limiting behavior of the function $f(x) = 2x/(1+x)$, defined for all real $x \neq -1$, whereas the statement $\lim_{n\to\infty} 2n/(1+n) = 2$ refers to the limiting behavior of the sequence $2/2, 4/3, 6/4, 8/5, 10/6, \ldots$. (Of course the formula for the limit of the function of the real variable x implies the formula for the limit of the sequence involving n.)

In various realms of mathematical discourse, it is not unusual to adopt conventions about the domains of different sets of letters just like those used in calculus. In this book, however, we shall generally avoid such conventions and, instead, explicitly state the domain of the variables we use. For example, we would *not* write $(\forall n)(n^2 \geq 0)$ to suggest, "by agreement", that the n is restricted to integers. Instead, we write $(\forall n \in \mathbb{Z})(n^2 \geq 0)$.

To deal with formulas involving dummy variables, some notation helps. If x is a letter that occurs in a string P and that S is a string, then

$$P[x \to S]$$

will mean the string obtained by replacing each occurrence of x in P by S. For example, if P is the formula $(\forall x \in \mathbb{N})(x^2 \geq 0)$ and S is the letter y, then $P[x \to y]$ is the formula $(\forall y \in \mathbb{N})(y^2 \geq 0)$.

A formula in our sense is like a declarative sentence in ordinary language. Thus, '$0 < 1$' and 'The empty set is a subset of X' are (informal renderings of) formulas, whereas the command 'Solve $x^2 = 1$' and the question 'Is $\pi^e > e^\pi$?' are not.

Formulas, like terms, are of two types:

- A *closed* formula is one that contains no free letters. A closed formula may make a definite assertion about the specific objects named in it; for example, 'The empty set $\emptyset$ is an element of the one-element set $\{\emptyset\}$'. Or, a closed formula may make a definite assertion about all objects; for example, 'For every X, the empty set is a subset of X'.

- An *open* formula is one that contains at least one free letter. For example, 'The empty set is a subset of X'. An open formula makes an actual statement only when the free letters in it are replaced by terms that are not letters. For example, replacing X by $\emptyset$ in 'The empty set is a subset of X' yields the formula 'The empty set is a subset of $\emptyset$', which is no longer open and so is a statement.

A closed formula is sometimes called a **statement**, or **sentence**. It makes sense to ask whether a statement is true. However, we shall soon become sloppy about this usage and refer even to open formulas such as $x = x$ as "statements".

To emphasize that a formula P is open because the variable x occurring in it is free, we sometimes write $P(x)$ and then call the formula a **predicate in** x. For example, $(\exists y)(x \in y)$ is a predicate in x; but it is *not* a predicate in y (because y is bound in the whole formula). Similarly, we can have a predicate $P(x, y)$ in two variables, such as $x \in y \vee y \in x$.

It does not seem to make sense to ask whether an open formula is true, because of the ambiguity of its free variables. For example, if $P(x)$ is the predicate $x \in \mathbb{R} \wedge x > 0$, then $P(x)$ is true when the variable x is replaced by the term $\sqrt{2}$ but false when x is replaced by -1.

L.3 Proof and truth

Logic is like a sewer—what you get out of it depends on what you put into it: it cannot provide any "absolute" truth, only the truth of statements relative to the truth of assumptions from which they are deduced. So we have to start with certain basic assumptions, and these are called **axioms.** The three simplest axioms customarily used in mathematics are:

Axioms L.3.1 (Axioms for Equality).

1. (reflexivity) $(\forall x)\,(x = x)$

2. (symmetry) $(\forall x)(\forall y)\,(x = y \implies y = x)$

3. (transitivity) $(\forall x)(\forall y)(\forall z)\,(x = y \;\&\; y = z \implies x = z)$

The letters x, y, and z in these axioms are dummy variables, so we must agree to accept as axioms all statements that result when we legitimately replace these letters consistently by letters different from x, y, and z. For example, we take

$$(\forall x)(\forall A)\,(x = A \implies A = x)$$

to be an axiom, too.

A statement C is said to be **true** when it has a *proof.* By a **proof** of C is meant a (finite) list of statements, one after (or under) the other, whose last statement is C and in which each statement is:

- an axiom,
- another (already proved) true statement, or
- a statement Q where P and $P \implies Q$ are true statements that appear before Q in the proof.

The statements in a proof are called the *steps* of the proof.

When you are asked to "prove" a statement you are, of course, being asked to furnish a proof of it. Synonyms for *prove* are *show, verify, demonstrate, establish,* and *deduce.*

The central ingredient of any proof is the pattern P, $P \implies Q$, Q, which may be written with the aid of the symbol $\therefore$ (*therefore*) in the form:

$$\begin{array}{rl} & P \\ & P \implies Q \\ \therefore & Q \end{array}$$

(Many steps could intervene between P and $P \implies Q$.) This pattern is known as **Modus Ponens**. Often one of the words “therefore”, “hence”, or “thus” is used before the conclusion of a Modus Ponens.

Here is an example. We shall prove that $4 = 2 + 2$ (not that you doubted it!). We use the definitions (abbreviations) 2, 3, and 4 for the terms $1 + 1$, $2 + 1$, and $3 + 1$, respectively. We take to be true the associative law

$$(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall k \in \mathbb{N})\,\big((m + n) + k = m + (n + k)\big) \qquad (*)$$

for addition of natural numbers. [Why this associative law is true is another matter entirely—see Exercise 1.2.11 (1) (b).] For brevity, abbreviate the associative law (*) by A. Then our proof that $4 = 2 + 2$ is as follows:

$$\begin{aligned}
&4 = 3 + 1, \text{ that is, } 4 = (2 + 1) + 1\\
&A \implies (2 + 1) + 1 = 2 + (1 + 1)\\
\therefore\ &(2 + 1) + 1 = 2 + (1 + 1)\\
&(\forall x)(\forall y)(\forall z)(x = y \;\&\; y = z \implies x = z)\\
&4 = (2 + 1) + 1 \;\&\; (2 + 1) + 1 = 2 + (1 + 1) \implies 4 = 2 + (1 + 1)\\
\therefore\ &4 = 2 + (1 + 1), \text{ that is, } 4 = 2 + 2
\end{aligned}$$

The idea behind the second step in the preceding proof is to substitute 2 for m, 1 for n, and 1 for k, respectively, in the associative law (*); this is an application of Universal Specialization (Axiom L.5.2), stated later. The fifth step is just transitivity of equality—one of Axioms L.3.1. Then the next-to-last step follows from that by substituting 4 for x, $(2 + 1) + 1$ for y, and $2 + (1 + 1)$ for z, respectively; this is another application of Universal Specialization.

In practice, we never—well, hardly ever—write a proof quite that formally. And, in practice, we often include in the proof justifications for many of its steps. An informal version of the same proof would be:

Proof. By the definitions, $4 = 3 + 1$, that is, $4 = (2 + 1) + 1$. From the associative law for addition, $4 = 2 + (1 + 1)$. This means $4 = 2 + 2$. □

The symbol □ marks the end of a proof; it is the modern-day equivalent of the traditional *QED*—an abbreviation for the Latin *quod erat demonstrandum,* meaning ‘which was to be proved’.

In a technical sense, every true (because proved) statement may be called a **theorem**. Then the just-proved statement $4 = 2 + 2$ is a theorem—but hardly an earth-shaking one. Generally we designate as theorems only the most significant true statements. (You will find only a handful of theorems in this book.) A true statement of lesser significance may be called a **proposition**, whereas an easily proved consequence—for example, a special case—of a proposition or theorem is usually called a **corollary**. A true statement whose main interest is only in its use as a step in proving a more significant result is called a **lemma**.

In view of the definition of what a *proof* is, we shall accept as a proof of an implication $P \Longrightarrow Q$ the sequence of steps as shown in the following **proof rule***:*

Proof Rule L.3.2 (Direct Proof—AH). *A list of steps of the following form produces a proof of an implication $P \Longrightarrow Q$:*

Assume P.

[Steps of a proof in which P is treated as if it were an axiom.]

$\therefore Q$

In such a proof, P is known as the *assumed hypothesis.* So the rule is sometimes referred to as the Method of the Assumed Hypothesis—hence the abbreviation AH. A fancier name for the method of direct proof is the **Herbrand-Tarski Deduction Criterion.**

For example, here is a proof of the implication that, if a positive integer n is divisible by 4, then n is even (that is, n is divisible by 2):

Proof. Let n be a positive integer. Assume n is divisible by 4. This means there is some integer k for which $n = 4k$. Then $n = 2(2k)$, and $2k$ is an integer. Thus n is even. $\square$

We shall reexamine this proof later, because several issues involving quantifiers are involved.

Exercise L.3.3. Write out, or find in a calculus book, a proof of some implication about differentiability of functions whose proof exploits the Herbrand-Tarski Deduction Criterion.

L.4 Combining Statements

In our development of logic, the next thing to do is establish a series of axioms governing the meaning of statements formed by combining others through use of the connectives *not, or, and, implies,* and *if and only if.* These axioms will also provide new proof rules as shortcuts for constructing proofs. Since most meaningful examples of proofs involve quantifiers, we defer stating these proof rules until Section L.6.

The simplest thing to do with a statement aside from asserting it is to deny it. For a statement P, its **negation** is the statement $\neg P$, which is also expressed as '*not P*'. In mathematical writing, $\neg P$ may be expressed more verbosely, for example, as in, "It is not the case that $2 < -1$."

The negation of P is deemed to be false when P is true, and true when P is false. We can express this situation by a **truth table**, as follows:

P	$\neg P$
T	F
F	T

Down the left column of the truth table we have written the two possible *truth values* T and F for P. These are, of course, abbreviations for *true* and *false,* respectively. In the right column of the table are the truth values of $\neg P$ corresponding to each of those two truth values in turn.[4]

Implicitly in the truth table for $\neg$ we just gave meaning to the word *false.* Here it is explicitly: A statement P is **false** when its negation $\neg P$ is true—that is, when $\neg P$ can be proved. For example, $4 \neq 2+2$ is false because (as was proved on page L18), the statement $4 = 2 + 2$ is true.

Do not think that a negated statement (not P) has to be false just because it has the word 'not' in it: $\neg(0 = 1)$, that is, $0 \neq 1$, is true (because $0 = 1$ is false). This situation resembles that with negation in algebra: an expression of the form $-x$ need not denote a negative number [because, for example, $-(-1) > 0$].

For statements P and Q, their **conjunction** $P \,\&\, Q$, which is also expressed by 'P *and* Q', is the statement that is true when both P and Q are true, but false otherwise. In other words, the truth table for & (*and*) is:

P	Q	$P \,\&\, Q$
T	T	T
T	F	F
F	T	F
F	F	F

In the two columns at the left we have systematically written all four of the possible pairs of truth values (TT, TF, FT, and FF); in the column at the right are the truth values of $P \& Q$ corresponding to each of these four combinations of truth values in turn.

As with all the connectives, so & (*and*) is rendered in various ways in

[4] Strictly speaking, the column headings of a truth table (such as P and $\neg P$ above) are not actual statements but rather "statement-forms". The table indicates what truth value to ascribe in each case to the statement obtained from the heading of the last column by replacing each of the constituent letters in the statement-form by an actual statement. Nonetheless, we shall often speak as if the statement forms in a truth table were actual statements.

informal mathematical writing, as indicated in Table L.1. For example:

$$2n \text{ is even } \textit{but } 2n + 3 \text{ is odd}$$
$$\varnothing \text{ is empty } \textit{whereas } \{\varnothing\} \text{ is nonempty}$$
$$x^2 \geq 0 \textit{ yet } x < 0$$

For statements P and Q, their **disjunction** $P \vee Q$, which is also expressed by 'P *or* Q', is the statement that is true when at least one of P, Q is true—in other words, when P is true, Q is true, or P and Q are both true—and false otherwise. Thus ***or* is used in the *inclusive* sense** to allow that both individual statements connected by it be true and yet their disjunction also be true. In other words, the *only* case in which $P \vee Q$ is false is that in which both P and Q are false. The truth table for $\vee$ (*or*) is:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

The inclusive sense of *or* is just what is intended, for example, in the mathematical statement that $x \leq y \vee y \leq x$ is true for all real numbers x and y: when $x = y$, then both $x \leq y$ and $y \leq x$ are separately true. In ordinary language, this use of *or* in the inclusive sense can be annoying: pity the poor restaurant waiter who, upon asking the mathematician diner, "Would you like soup or salad?" receives the answer, "Yes."

Students are sometimes puzzled or even annoyed when they are told that the statement "$4 \leq 2 + 2$" is true; they complain, "How can 4 be less than or equal to $2 + 2$ when, in fact, 4 is exactly equal to $2 + 2$?" Now according to the definition of $\leq$, the statement "$4 \leq 2 + 2$" means "$4 < 2 + 2$ or $4 = 2 + 2$". Whereas the statement "$4 < 2 + 2$" is false, the statement "$4 = 2 + 2$" is true. Then the truth table for $\vee$ gives us no choice: the disjunction "$4 < 2 + 2$ or $4 = 2 + 2$" must be true.

Exercises L.4.1. For statements P and Q, how would you symbolize each of the following?

(1) "Exactly one of P and Q." (As in, for example: "If $x \in \mathbb{R}$ and $x \neq 0$, then exactly one of $x < 0$ and $x > 0$ holds.")

(2) "Neither P nor Q." (As in, for example, "The number 0 is neither positive nor negative.")

A statement may also be built up using logical connectives from more than two constituent statements. For example, $(P \& Q) \vee R$ involves three statements P, Q, and R. Then the truth table for this statement requires $2 \cdot 2 \cdot 2 = 2^3 = 8$ combinations of truth values. To help us obtain the result column of truth values for the entire statement,we ordinarily insert intermediate columns showing the truth values of its components:

P	Q	R	$P \mathbin{\&} Q$	$(P \mathbin{\&} Q) \vee R$
T	T	T	T	T
T	T	F	T	T
T	F	T	F	T
T	F	F	F	F
F	T	T	F	T
F	T	F	F	F
F	F	T	F	T
F	F	F	F	F

Apply the truth table for $\vee$ in the special case that Q is the negation $\neg P$ of P. The first and fourth rows of the body of the table are irrelevant here: in view of the truth table for $\neg$, the truth value of Q cannot be chosen independently of the truth value of P. Thus we get the truth table

P	$\neg P$	$P \vee \neg P$
T	F	T
F	T	T

According to the table, no matter what the truth value of P itself, the statement $P \vee \neg P$ has the truth value T. A statement such as this is called a **tautology** to mean that each of the entries in the last column of its truth table is a T.

Tautology L.4.2 (Law of the Excluded Middle). *Let P be a statement. Then:*

$$P \vee \neg P$$

We stipulate that ***every tautology is an axiom.***

For example, according to the Law of the Excluded Middle $P \vee \neg P$ is an axiom no matter what the statement P might be.[5]

When asked on an exam to prove a certain proposition, a student once answered: “By the Law of the Excluded Middle, either the proposition is true or it is false. If it is true, then there is no need for me to prove it; if it is false, I can hardly be asked to prove it!” The student’s response betrays a fundamental—and all too common—misunderstanding of the

[5] Strictly speaking, the phrase ‘$P \vee \neg P$’ is only an *axiom-form* because the ‘P’ there is only a statement form. Our stipulation about axioms resulting from tautologies really means the following: *Every statement that results from replacing each constituent letter in a tautology by an actual statement is an axiom.* For example, the instance $(\pi^e < e^\pi) \vee (\pi^e \geq e^\pi)$ of $P \vee \neg P$ is such an axiom; so is $(2^e \in \mathbb{Q}) \vee (2^e \notin \mathbb{Q})$, where $\mathbb{Q}$ is the set of all rational numbers.

Law of the Excluded Middle. All this tautology does is assert the truth of the compound statement $P \vee \neg P$ no matter what the truth value of P itself; it says nothing about the truth or falsity of P itself. For example, it is true that 2^e is rational or 2^e is irrational, but so far nobody has been able to determine which of the two possibilities holds! Moreover, it is entirely possible, albeit disconcerting, that somebody will discover a mathematical statement that cannot be proved and yet whose negation also cannot be proved—in other words, that some mathematical statement is neither true nor false!

The logical connective most central to the very notion of proof is $\Longrightarrow$. For statements P and Q, the **implication** $P \Longrightarrow Q$ may be expressed as '*P implies Q*', as '*if P then Q*', or in one of the other ways listed in Table L.1. The implication $P \Longrightarrow Q$ is taken to be true in every case *except* when P is true and Q is false. In other words, the truth table for $\Longrightarrow$ is:

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

In an implication $P \Longrightarrow Q$, the statement P is called the **hypothesis** (or **premise**), and the statement Q is called the **conclusion.**

Most people have no difficulty accepting what the truth table for $\Longrightarrow$ indicates in the two cases where P is true. But the two cases where P is false often cause some consternation. They should not, because these two cases do reflect the way 'if ...then' is used in everyday language. For example, "If you are good, then I will give you some candy." We understand this as a promise to be honored no matter what. If you are not good and I give you no candy, I certainly do not break the promise. If you are not good and yet I still give you candy, I also do not break the promise (even though my promise may not have the intended effect the next time I make it).[6]

Notice the "asymmetry" between P and Q in $P \Longrightarrow Q$: For particular statements P and Q, *the implication $P \Longrightarrow Q$ may be true whereas its **converse** $Q \Longrightarrow P$ may be false.* For example, take P to be the statement $1 = 0$ and Q to be the statement $0 = 0$. Then the implication $1 = 0 \Longrightarrow 0 = 0$ is true because its hypothesis $1 = 0$ is false. However, the converse implication $0 = 0 \Longrightarrow 1 = 0$ is false because its hypothesis $0 = 0$ is true whereas its conclusion $1 = 0$ is false.

[6]Calling an implication true when its hypothesis and conclusion are both false is problematic, however, when the hypothesis and conclusion are about real-world events. For example: "If Great Britain had won the War for Independence, then the United States would be a British colony today." What do we really mean when we utter such a "counterfactual conditional"?

Exercise L.4.3. What is the relationship between the truth of an implication $P \implies Q$ and that of its **contrapositive** $\neg Q \implies \neg P$?

Numerous tautologies and resulting axioms can now be derived. One such tautology is:

$$P \,\&\, Q \implies P$$

Its truth table is:

P	Q	$P \,\&\, Q$	P	$P \,\&\, Q \implies P$
T	T	T	T	T
T	F	F	T	T
F	T	F	F	T
F	F	F	F	T

Notice that the fourth column, headed P, repeats the first. The fourth column is not really needed, but it was inserted to the right of the column headed $P \,\&\, Q$ to facilitate using the truth table for $\implies$ in order to fill in the final column.

Here are a couple more tautologies involving implication:

$$P \implies P \vee Q$$
$$(P \implies Q) \implies (R \vee P \implies R \vee Q)$$

For statements P and Q, the logical **equivalence** $P \iff Q$ may be expressed as 'P *is equivalent to* Q', as 'P *if and only if* Q', or in one of the other ways listed in Table L.1. The equivalence $P \implies Q$ is taken to be true exactly when P and Q have the same truth value, that is, when they are both true or else both false. In other words, the truth table for $\iff$ is:

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

An equivalence $P \iff Q$ is true precisely when the implication $P \implies Q$ and its converse $Q \implies P$ are both true. In other words, the following is a tautology:

Tautology L.4.4. *let P and Q be statements. Then:*

$$(P \iff Q) \iff \big((P \implies Q) \,\&\, (Q \implies P)\big)$$

To verify this tautology, compare the truth table for $P \iff Q$ with that for $(P \implies Q) \,\&\, (Q \implies P)$.

A common way to prove a statement of the form $P \iff Q$ is to prove separately the implications $P \implies Q$ and $Q \implies P$. Can you justify that way?

Many of the most useful tautologies are logical equivalences. Here are some.

Tautologies L.4.5. *Let P, Q, and R be statements. Then:*

1. *(double negation)* $P \iff \neg\neg P$
2. *(idempotent law)* $P \vee P \iff P$
3. *(idempotent law)* $P \,\&\, P \iff P$
4. *(commutative law)* $P \vee Q \iff Q \vee P$
5. *(commutative law)* $P \,\&\, Q \iff Q \,\&\, P$
6. *(associative law)* $(P \vee Q) \vee R \iff P \vee (Q \vee R)$
7. *(associative law)* $(P \,\&\, Q) \,\&\, R \iff P \,\&\, (Q \,\&\, R)$
8. *(distributive law)* $P \vee (Q \,\&\, R) \iff (P \vee Q) \,\&\, (P \vee R)$
9. *(distributive law)* $P \,\&\, (Q \vee R) \iff (P \,\&\, Q) \vee (P \,\&\, R)$

Exercise L.4.6. Use truth tables to establish parts 1, 2, 4, 6, and 8 of the preceding list of tautologies.

The following three tautologies express fundamental properties of logical equivalence. They are easy enough to establish by constructing truth tables. They may also be deduced from Tautology L.4.4 and some of the other, previously listed tautologies.

Tautologies L.4.7. *Let P, Q, and R be statements. Then:*

1. $P \iff P$
2. $(P \iff Q) \implies (Q \iff P)$
3. $\big((P \iff Q) \,\&\, (Q \iff R)\big) \implies (P \iff R)$

That an implication $P \implies Q$ is false only in the case that P is true but Q is false, and the implication is true in every other case, is also expressed by the following tautology.

Tautology L.4.8. *Let P and Q be statements. Then:*

$$(P \implies Q) \iff (\neg P \vee Q)$$

Exercise L.4.9. Use connectives to symbolize 'P unless Q' for statements P and Q.

Often in constructing proofs you will want to form the negation of a compound *or*- or *and*-statement. For this the following pair of tautologies are relevant:

Tautologies L.4.10 (De Morgan's Laws). *Let P and Q be statements. Then:*

1. $\neg(P \vee Q) \iff (\neg P) \,\&\, (\neg Q)$
2. $\neg(P \,\&\, Q) \iff (\neg P) \vee (\neg Q)$

Here is an instance of the first of De Morgan's Laws: To deny that an integer n is a multiple of 2 or a multiple of 3 is to affirm that it is *not* the case that n is a multiple of 2 and a multiple of 3; in other words, that n is neither a multiple of 2 nor a multiple of 3. You should be able to write a similar instance of the second of De Morgan's Laws.

Exercise L.4.11. Use De Morgan's Laws to deduce Tautologies L.4.5 parts 3, 5, 7, and 9 from parts 2, 4, 6, and 8, respectively. (For example, use the idempotent law $P \vee P \iff P$ together with De Morgan's Laws to deduce the idempotent law $P \,\&\, P \iff P$.)

It is easy to check that the following are tautologies:

$$\begin{aligned}
\big((\neg P) \,\&\, (P \iff P')\big) &\implies (\neg P') \\
\big((P \vee Q) \,\&\, (P \iff P') \,\&\, (Q \iff Q')\big) &\implies (P' \vee Q') \\
\big((P \,\&\, Q) \,\&\, (P \iff P') \,\&\, (Q \iff Q')\big) &\implies (P' \,\&\, Q') \\
\big((P \implies Q) \,\&\, (P \iff P') \,\&\, (Q \iff Q')\big) &\implies (P' \implies Q')
\end{aligned}$$

Together these tautologies justify the following rule: *Let S be a statement built up in some way from simpler statements $P_1, P_2, \ldots, P_n$ by using the logical connectives. If one or more of the constituent statements P_i are replaced by equivalent statements P_i', then the resulting statement S' has the same truth value as the original statement S.*

We have not attempted to list here all the tautologies commonly used in constructing proofs. Consequently, when you see a proof whose pattern is unfamiliar, you should suspect that it is justified by an axiom resulting directly from some as-yet-unstated tautology—and you should attempt to write that tautology and verify it (by using other tautologies or directly, by constructing the truth table).

L.5 Quantifiers

The logical quantifiers $\forall$ (*for all*, *for every*), $\exists$ (*there exists*, *for some*), and $\imath$ (*the*) were already introduced. Here we examine them further and, in particular, state some axioms and tautologies involving them.

The quantifiers have no real effect unless the formula to which they are applied involve a free variable. That is why, to emphasize the fact that a letter x is a free variable in the formula P, we also denote the formula by $P(x)$ and then call it a *predicate in* x. [Recall that, in particular, x is free in P when x does not occur in P, but still we might write $P(x)$.]

The letter x used in a universally or existentially quantified statement about a predicate $P(x)$ is a dummy variable that can be replaced by another letter, as stated precisely in the following axiom.

Axiom L.5.1. *Let x be a free variable in the formula P and let y be a letter that does not occur in P. Then:*

1. $(\forall x)P(x) \iff (\forall y)P[x \to y]$
2. $(\exists x)P(x) \iff (\exists y)P[x \to y]$

As already suggested in Table L.1, the statement $(\forall x)P(x)$ involving the **universal quantifier** $\forall$ may be read or expressed variously as:

for every x, $P(x)$
for all x, $P(x)$
for each x, $P(x)$
for arbitrary x, $P(x)$

Sometimes, $(\forall x)P(x)$ is even expressed as "for any x, $P(x)$." However, it is best to avoid using 'any' this way, since in some contexts 'any' can mean 'some'! (Compare: "Can you draw any conclusion from that?")

Often a statement of the form $(\forall x)P(x)$ is expressed with additional words, such as:

for every x, it is the case that $P(x)$
for each x, the property $P(x)$ holds

The word 'any' is sometimes used to suggest a universally quantified statement. For example: "Any even integer has a square that is even." "Any integer that is even has an even square." "The square of any even integer is even." Sometimes the 'every', 'all', 'each', or 'any' is deleted as in: "An even integer has an even square" and "The square of an even integer is even."

The universal quantifier was used, for example, in formulating the Axioms for Equality (Axioms L.3.1), which were:

$$(\forall x)\,(x = x)$$
$$(\forall x)(\forall y)\,(x = y \implies y = x)$$
$$(\forall x)(\forall y)(\forall z)\,(x = y \,\&\, y = z \implies x = z)$$

The intended meaning of the universal quantifier $\forall$ in $(\forall x)P(x)$ is that $(\forall x)P(x)$ be true precisely when $P(x)$ is true no matter what particular term is substituted for x in $P(x)$. We formulate this meaning in an axiom. The formulation uses the notation $P[x \to X]$ which, you should recall, means that every occurrence of the letter x in P is replaced by the string X.

Axiom L.5.2 (Universal Specialization). *Let x be a free variable in the formula P and let X be a term. Then:*

$$(\forall x)P(x) \implies P[x \to X]$$

Informally speaking, Universal Specialization expresses that when some property holds about every object in the mathematical world, it must also hold for any particular object. For example, according to US,

$$(\forall x)\,(x = x) \implies \varnothing = \varnothing$$

is an axiom. Since $(\forall x)\,(x = x)$ is an axiom, then

$$\varnothing = \varnothing$$

is therefore true.

More generally, in view of AH (the Herbrand-Tarski Deduction Criterion, Proof Rule L.3.2), the preceding axiom provides a corresponding proof rule.

Proof Rule L.5.3 (Universal Specialization—US). *Let x be a free variable in the formula P and let X be a term. If $(\forall x)P(x)$ is true, then $P[x \to X]$ is true.*

The order of consecutive universal quantifiers in a statement is immaterial:

Axiom L.5.4. *Let x and y be free in the formula $P(x,y)$. Then:*

$$(\forall x)\,(\forall y)\,P(x,y) \iff (\forall y)\,(\forall x)\,P(x,y)$$

Exercise L.5.5. (a) Does the order of consecutive existential quantifiers in a statement matter? That is, is $(\exists x)(\exists y)P(x,y)$ logically equivalent to $(\exists y)(\exists x)P(x,y)$? Why or why not?

(b) Is $(\exists x)(\exists y)P(x,y)$ logically equivalent to $(\exists y)(\exists x)P(y,x)$? Why or why not? [Notice that here the order of the letters in $P(x,y)$ is also reversed.]

Axioms L.5.6. *Let x be free in the formulas $P(x)$ and $Q(x)$. Then:*

1. $(\forall x)\,(P(x)\,\&\,Q(x)) \iff (\forall x)\,P(x))\,\&\,(\forall x)\,Q(x)$

2. $(\forall x)\,(P(x) \Longrightarrow Q(x)) \iff ((\forall x)\,P(x) \Longrightarrow (\forall x)\,Q(x))$

As always, so in the preceding pair of axioms, the letter x need not actually occur in either P or Q. If x does not occur, say, in P but does occur as a free variable in Q, we could rewrite the first of the pair as:

$$(\forall x)\,(P \,\&\, Q(x)) \iff (\forall x)\,P \,\&\, (\forall x)\,Q(x)$$

Similarly for the second axiom.

Often you will see the axioms for equality written in the simpler forms

$$\begin{gathered} x = x \\ x = y \implies y = x \\ x = y \,\&\, y = z \implies x = z \end{gathered}$$

where the universal quantifiers are omitted but implicit. To justify such omissions, we rely upon the following proof rule.

Proof Rule L.5.7 (Universal Generalization—UG). *Suppose the letter x is free in the formula $P(x)$. If $P(x)$ is true, then $(\forall x)\,P(x)$ is true.*

In view of this proof rule, we sometimes refer to an formula *as if* it, too, were a statement.

Notice that we did *not* first give as an axiom "$P(x) \implies (\forall x)P(x)$" and then suggest that the proof rule UG is a consequence. Indeed, there are two essential *restrictions upon the use of* UG:

- The letter x is not free in any preceding step in the proof that results by using Existential Specialization (ES); and
- If in a preceding step of the proof AH (Proof Rule L.3.2) was used to deduce a statement C by assuming a hypothesis H, then AH has already been invoked to prove $H \implies C$, and H is no longer being assumed.

In particular, Universal Generalization may *not* be used in a proof of the following form.

Assume $P(x)$.
$(\forall x)P(x)$ (by UG).
$\therefore P(x) \implies (\forall x)P(x)$ (by the Deduction Criterion).

And thus Universal Generalization may *not* be invoked so as to prove the formula:

$$P(x) \implies (\forall x)P(x) \qquad \textit{Wrong!}$$

That formula is wrong because the letter x is unbound in $P(x)$ but bound in $(\forall x)P(x)$. In fact, suppose it were legitimate to deduce that implication. Since x is a dummy variable in $(\forall x)P(x)$, then x in this universally quantified statement could be replaced by a different letter y so as to deduce:

$$P(x) \implies (\forall y)P(y) \qquad \textit{Wrong!}$$

Why that restriction? Just suppose that, to the contrary, it were legitimate to deduce the preceding implication. As an example, take $P(x)$ to be the predicate $x \in \mathbb{N} \Longrightarrow x > 0$. Then $(x \in \mathbb{N} \Longrightarrow x > 0) \implies (\forall x)(x \in \mathbb{N} \Longrightarrow x > 0)$ would be true. Replace x by y in the quantified part of this formula to obtain $(x \in \mathbb{N} \Longrightarrow x > 0) \implies (\forall y)(y \in \mathbb{N} \Longrightarrow y > 0)$, which would then also be true. Now the hypothesis $1 \in N \Longrightarrow 1 > 0$ is true. Hence the conclusion $(\forall y)(y \in \mathbb{N} \Longrightarrow y > 0)$ would also be true. But clearly it is false!

Here is an example of how proof rule UG is employed. Suppose you want to prove that

$$(\forall x)(\forall y)(\forall z)(x = y \,\&\, z = y \implies x = z).$$

Note that, in this statement, the & has a higher precedence than $\Longrightarrow$, so that the statement means:

$$(\forall x)(\forall y)(\forall z)\,\big((x = y \,\&\, z = y) \implies x = z\big)$$

Then you could write a proof of the statement without any quantifiers whatsoever by using the axioms for equality and invoking US implicitly as follows:

Proof.

$$\begin{aligned} z = y &\implies y = z \\ x = y \,\&\, z = y &\implies x = y \,\&\, y = z \\ x = y \,\&\, y = z &\implies x = z \\ x = y \,\&\, z = y &\implies x = z. \quad \square \end{aligned}$$

In practice, we do not usually write the proof in such excruciating detail. Rather, we shorten it and express it more informally, as follows:

Proof. Assume $x = y$ and $z = y$. By symmetry of equality, $y = z$. By transitivity of equality, then $x = z$. $\square$

In the proof on page L19 that if a positive integer n is divisible by 4, then n is even, several steps appear only implicitly. Here is a more complete version of the proof in which those steps have been made explicit:

> Let n be a positive integer. Assume n is divisible by 4. This means there is some integer k for which $n = 4k$. Let k be such an integer. Then $n = 2(2k)$. Let $t = 2k$. Then t is an integer such that $n = 2t$. This means that there is some integer t such that $n = 2t$. Thus n is even.

Recall that the step "Assume n is divisible by 4" indicates a use of the Herbrand-Tarski Deduction Criterion (Proof Rule L.3.2). Aside from that proof rule, three issues about quantifiers are also involved in the preceding proof:

1. What is being proved is really a universally quantified statement:

   > For every positive integer n, if n is divisible by 4, then n is even.

   To prove this universally quantified statement, we removed the "For every" part "For every positive integer n" involving the universal quantifier and instead wrote, "Let n be a positive integer"—meaning, "Let n be an *arbitrary* (but specific) positive integer".

   Then, using several steps, we proved, "If n is divisible by 4, then n is divisible by 2." That this procedure actually proves the universally quantified statement is justified by Universal Generalization (Proof Rule L.5.7).

2. Recall that the assumption that n is divisible by 4 meant that there exists some integer k such that $n = 4k$. So the more complete version of the proof said next, "Let k be such an integer," in other words:

   > Let k be a particular integer such that $n = 4k$.

   That is justified by the principle of **Existential Specialization**—ES, for short.

3. After letting $t = 2k$, where k was that particular integer obtained from ES, we deduced that

   > $n = 2t$

   for that particular t (which depended upon the particular k). And from that in turn we deduced:

   > There is some integer t such that $n = 2t$

   Putting the existential quantifier back there is justified by the principle of **Existential Generalization**—EG, for short.

Here are the precise formulations of ES and EG.

Proof Rule L.5.8 (Existential Specialization—ES). *Let x be a letter that is free in P and does not occur in C. Suppose that both*

$$(\exists x)(P(x)$$

and

$$P(x) \implies C$$

are true. Then C is true.

Proof Rule L.5.9 (Existential Generalization—EG). *Suppose x is free in P and S is a term. If $P[x \to S]$ is true, then $(\exists x)P(x)$ is true.*

Existential Generalization says, in effect, that one way to prove existence of an object x with a certain property $P(x)$ is to construct or "exhibit" a particular object S having that property. For example, to prove there exists some nonempty set—that is, $(\exists A)(A \neq \emptyset)$—you could construct the set $\{\emptyset\}$ and note that $\{\emptyset\}$ is not empty—that is, $\{\emptyset\} \neq \emptyset$—because $\emptyset \in \{\emptyset\}$. Or, to prove there exists some negative integer whose square is 4, you could exhibit the integer -2 and note that $(-2)^2 = 2$.

Recall that $(\exists x \in X)P(x)$ is an abbreviation for $(\exists x)\big(x \in X \& P(x)\big)$. Then Existential Generalization has as a particular case the situation where the formula $P(x)$ takes the form $x \in X \,\&\, Q(x)$ for a predicate $Q(x)$.

Proof Rule L.5.10 (Existential Generalization—relative form—EG). *Suppose x is free in P and s and X are terms. If $s \in X$ and $P[x \to s]$ are both true, then $(\exists x)P(x)$ is true.*

Recall that $(\forall x \in X)(P)$ is an abbreviation for $(\forall x)(x \in X \implies P)$. For now we shall also take as axiomatic the following variant of Universal Specialization:

Axiom L.5.11 (Universal Specialization—relative form). *Let x be a free variable in the formula P and let a and X be terms. Then:*

$$(\forall x \in X)\big(P(x)\big) \,\&\, a \in X \implies P[x \to a]$$

The preceding axiom means that when some property holds for every element of a set X and when a is one of the elements of X, then the property must hold, in particular, for a. Surely you have no qualms about accepting that! (Actually, it can be deduced from US.)

As an example of this relative form of US, look again at the proof that $4 = 2 + 2$ (see page L18). Again, abbreviate by A the associative law

$$(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall k \in \mathbb{N})\,\big((m+n)+k = m+(n+k)\big).$$

Then our proof that $4 = 2 + 2$ is as follows:

$$\begin{aligned}
&4 = 3 + 1, \text{ that is, } 4 = (2 + 1) + 1 \\
&A \\
&A \implies (2 + 1) + 1 = 2 + (1 + 1) \\
\therefore\ &(2 + 1) + 1 = 2 + (1 + 1) \\
&(\forall x)(\forall y)(\forall z)(x = y \;\&\; y = z \implies x = z) \\
&4 = (2 + 1) + 1 \;\&\; (2 + 1) + 1 = 2 + (1 + 1) \implies 4 = 2 + (1 + 1) \\
\therefore\ &4 = 2 + (1 + 1), \text{ that is, } 4 = 2 + 2
\end{aligned}$$

The third step and sixth steps are applications of the relative form of US.

The relative form of Universal Specialization, Axiom L.5.11, justifies the following proof method:

Proof Rule L.5.12. *Let X is a set and let $P(x)$ be a predicate in x. Then following is a proof of $(\forall x \in X)P(x)$:*

> *Let $x \in X$.*
> Proof of $P(x)$ where $x \in X$ is assumed to be an axiom.

Intuitively, to deny that a certain property holds for all x is to assert that it fails to hold for some x. We express this formally in an axiom, which relates universal and existential quantification by means of negation.

Axiom L.5.13. *Let $P(x)$ be a predicate in x. Then:*

$$\neg(\forall x)P(x) \iff (\exists x)\big(\neg P(x)\big)$$

By applying negation to both sides of the equivalence in Axiom L.5.13, and replacing $P(x)$ in it by $\neg P(x)$, we obtain at once the first part of the following theorem; the second part follows from the first by replacing negating both sides of the first part.

Theorem L.5.14. *Let $P(x)$ be a predicate in x. Then:*

1. $\neg(\exists x)P(x) \iff (\forall x)\big(\neg P(x)\big)$
2. $(\exists x)P(x) \iff \neg(\forall x)\big(\neg P(x)\big)$

The second part of the preceding theorem implies something significant about mathematical proof as it is commonly understood: *To prove existence of some x for which $P(x)$ holds, it suffices to prove it false that the negation of $P(x)$ holds for every x.*

Thus one can prove existence of an object with a certain property *without* actually constructing or exhibiting a particular object with that property![7]

L.6 More proof rules

[7]A small minority of mathematicians, the “constructivists,” object to establishing existence of an object having a given property without actually constructing a particular object having that property. In other words, they reject Axiom L.5.13.