MATHEMATICS 300 — FALL 1997

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 2. September 15, 1997

Revised version, October 6, 1997

PROOFS

A **proof** of a statement is a **convincing argument** that establishes **beyond the shadow of a doubt** that the statement is true.

You should think of proving statements as a **game** that you are playing against an opponent who does not believe that the statement you are proving is true. You make statements, your opponent may find them convincing or not, and it is up to you to clear up all your opponent's doubts by arguing your case persuasively every time your opponent isn't convinced. (Maybe you should think that I, the instructor, am the "opponent." **You** have to convince **me**. If you convince me, then your proof has worked. Otherwise it has not.)

The trouble with all this is that it is not very clear what will count as a "convincing argument." Suppose your opponent says, after you have given what looks to you like a very convincing proof: "I am not convinced; I don't see why what you just said proves anything." How would you deal with something like that?

Moreover, any argument you give will have to *start* somewhere. (You cannot prove anything starting from nothing.) What can you do if your opponent refuses to accept your starting point?

EXAMPLE: suppose you want to prove that,

> *if a real number is greater than or equal to* 4*, then the square root of the number is less than or equal to half the number.*

Equivalently —and more concisely— you want to show that

> *if* x *is any real number such that* $x \geq 4$*, then* $\sqrt{x} \leq \frac{x}{2}$.

Or —even more concisely— you want to prove that

$$(\forall x)\Big(x \geq 4 \Longrightarrow \sqrt{x} \leq \frac{x}{2}\Big)\,.$$

To prove this, you can proceed as follows:
To prove $(\forall x)\Big(x \geq 4 \Longrightarrow \sqrt{x} \leq \frac{x}{2}\Big)$, we pick an arbitrary x and try to prove that $x \geq 4 \Longrightarrow \sqrt{x} \leq \frac{x}{2}$.
So, let x be arbitrary. We want to prove $x \geq 4 \Longrightarrow \sqrt{x} \leq \frac{x}{2}$. To prove this, we assume $x \geq 4$ and try to prove that $\sqrt{x} \leq \frac{x}{2}$.
Now we are assuming that $x \geq 4$. From this it follows —multiplying both sides by x— that $x^2 \geq 4x$. Then —dividing both sides by 4— we get that $\frac{x^2}{4} \geq x$. Then —taking the square root of both sides— we get $\sqrt{\frac{x^2}{4}} \geq \sqrt{x}$. Since $\sqrt{\frac{x^2}{4}} = \frac{x}{2}$, we have shown that $\frac{x}{2} \geq \sqrt{x}$, which is "the same as" $\sqrt{x} \leq \frac{x}{2}$. **END OF PROOF**

Is this a truly convincing argument?

The answer is "yes" if all the steps are convincing. But **if one step is not convincing, then the whole argument fails.** (This is why you should **not** expect to get partial credit for a wrong proof if most steps are O.K. but just a few of them are wrong. A proof is like a chain. And **a chain is no stronger than its weakest link.** If a 16-Ton weight is hanging right above your head, held by a chain, and the chain breaks because of one weak link, and the weight falls on your head and kills you, do you think the chain manufacturer should be entitled to "partial credit" because "most links were O.K.; only one broke"? If the driver of Lady Diana's car didn't drink every night, but only drank on the particular night of the accident, should he be entitled to partial credit because "after all, most of the time he didn't drink"?)

So, are ALL the steps in the above proof truly convincing?

In the proof, we have given justifications for each step. For example, at one point we went from "$x \geq 4$" to "$x^2 \geq 4x$," and we said that this was done "multiplying both sides by x." Now, why can we do that?

Suppose I tell you that "I don't believe that you can do this"? How do you persuade me? Well, let us give it a try. You can say: "because there is a general rule that says if you take an inequality and multiply both sides by a number, then you still get a valid inequality." (Or, in more symbolic notation: $(\forall a)(\forall b)(\forall c)(a \geq b \Longrightarrow ac \geq bc)$.)

This, however, will not do. This "rule" is NOT VALID. (For example, if $a = 5$, $b = 2$ and $c = -2$, then $a \geq b$, but it's not true that $ac \geq bc$, since $ac = -10$ and $bc = -4$, so $ac < bc$.) So WE CANNOT USE IT.

Now, here is a second try. You can say: "because there is a general rule that says if you take an inequality and multiply both sides by a nonnegative number, then you still get a valid inequality." (Or, in more symbolic notation: $(\forall a)(\forall b)(\forall c)\Big((a \geq b \wedge c \geq 0) \Longrightarrow ac \geq bc\Big)$.)

It turns out that this time our rule IS VALID. But notice that, in order to apply this rule, we must be sure that $c \geq 0$. In our case, the number that plays the role of c is x, and it is indeed true that $x \geq 0$, because $x \geq 4$. (Since this is a crucial fact for us to be able to apply the above "rule," it would have been better to include in our proof a little remark highlighting this. For example, instead of "multiplying both sides by x," it would have been better to say "multiplying both sides by x, which is possible because $x \geq 0$, since we are assuming that $x \geq 4$.")

But we haven't solved our problem. Remember that your proof is really a two-person game that you are playing against me, your opponent, in which you have to convince me. What if I say "How do we know that $(\forall a)(\forall b)(\forall c)\Big((a \geq b \wedge c \geq 0) \Longrightarrow ac \geq bc\Big)$? I am not really convinced that this is true."?

You could try to prove for me that $(\forall a)(\forall b)(\forall c)\Big((a \geq b \wedge c \geq 0) \Longrightarrow ac \geq bc\Big)$ is indeed true. But I am sure that in our proof you will use other "rules," and I, your opponent, could pick any of these and claim, once again, that I am not convinced of its validity.

IF I WANTED TO, I COULD GO ON LIKE THIS FOREVER. NO MATTER WHAT JUSTIFICATION YOU GIVE FOR A STEP IN YOUR PROOF, I COULD ALWAYS ASK: "WHY IS THAT VALID?"

In other words, if your opponent is truly stubborn and uncooperative, then there is *nothing* you can do. Maybe you will come up with some reason, but this reason will be based on some other facts that look obviously true to you. But your opponent can still refuse to accept these other facts, and this process can go on for ever.

To take care of this "problem of the opponent that doesn't play fair," mathematicians have come up with the concept of a **formal proof**. We give very precise rules defining what a "formal proof" is, and if you prove something correctly, and strictly following the rules, then you are *guaranteed* that your proof will be accepted as valid.

If you do *not* obey the rules, then you are on uncertain ground: you might be able to convince an instructor or grader, but you cannot be sure, because any time you take a step one of us might ask "how do you justify that step?"

You should think of giving formal proofs as similar to playing a game such as chess: you are given very strict, precise rules, and you are only allowed to make moves following the rules. As long as you obey the rules, your opponent does not have the right to reject your moves. (If your opponent unilaterally decides that a move of yours is not acceptable, because "you are not allowed to move a bishop if in the previous move you moved a knight," then you would say that your opponent is not playing fair, because this "rule" was not in the list of rules that had been agreed upon before the game started.)

In Mathematics we play fair. We tell you what the rules are, and if you prove something correctly following the rules, then you can be sure that it will be accepted. You may think that having to follow the rules is a restriction to your freedom. But this is not so. You should think of it as **your own protection against unfair play.** If you correctly justify every step according to the rules, then we promise you that we will not change the rules in the middle of the game, kick the board, or come up with other surprises.

REMARK. I said that you should think of giving formal proofs of theorems as a game similar to chess, in which you are given a small number of very strict rules telling you which moves are permitted, and each move has to be justifiable by explaining exactly which rule you are using and how you are using it. However, exactly as in the case of chess, if all you know is the rules, and you always apply the rules carefully and scrupulously, you may still lose all the time. If you want to **win** (that is, in the case of a proof, if you want to get to the desired conclusion) then you have to **think**. You have to plan a strategy, make a move now because it will be useful five or six steps later, etc.

The one big difference between chess and theorem-proving is that **chess is a zero-sum game**, but **theorem-proving is a cooperative game.** What this means is that in chess your opponent wants you to lose, whereas in theorem-proving you and your opponent are working together, trying to find out whether something is true, and to understand why.

That's why in chess you don't explain openly why you make a move. You do *not* say to your opponent things like: "I am making this move now so that then in the next move I can do this other thing, so that three moves later I can do that, and then I will checkmate you." *You don't want your opponent to be able to figure out your strategy.*

In theorem-proving you definitely **do** want your opponent to understand your strategy. Your opponent is going to be ruthless in criticizing you if you don't obey the rules, but as long as you obey them you will get full coopertaion. In fact, usually you don't have to go through the whole business of explaining every detail of every application of every rule. *As long as you persuade your opponent that something can be done using the rules, there is no need to go through all the steps and actually do it.* And, since your opponent wants to be persuaded, the more you do to explain why you are doing something, the better. That's why *in theorem-proving it's always nice to explain your strategy, so that your opponent can understand where you are headed.*

Because theorem-proving is a cooperative game, when writing proofs it is always nice to use the first person plural —the so-called "editorial we"— as we did in our first example of a proof ("we pick," "we are assuming," "we have shown"). This is a good way to convey the idea that the writer and the reader are *working together*, that **the writer is leading the reader gently along a path of discovery.**

FORMAL PROOFS

A *theorem* has one or several *assumptions* (or *hypotheses*, or *premisses*), and a *conclusion.* A *formal proof* of a theorem is a sequence of statements (the "steps" of the proof), ending with the conclusion, such that each step is permitted by the rules, given the previous steps.

Later, we will give a complete list of the rules that tell you when a step is permitted. For the time being, let us start with three examples of such rules.

(P.a) it is always permitted to bring in an *axiom* (or "postulate") as a new step,
(P.b) it is always permitted to bring in one of the hypotheses as a new step,
(P.c) it is always permitted to bring in as a new step something that follows from previous steps by applying a valid *rule of inference.*

For all this to make sense, I have to tell you what are the axioms and what are the rules of inference. We will start with the rules of inference. There will be exactly **eight** of them.

WHAT IS A VALID INFERENCE?

An *inference* is a way of passing from certain statements (the *premisses*) to another statement (the *conclusion*). A *valid inference* is one for which it is guaranteed that, if the premisses are true, then the conclusion is also true.

For example:

$$\begin{array}{r} \text{All men are mortal} \\ \text{Socrates is a man} \\ \hline \text{Socrates is mortal} \end{array} \qquad (1)$$

is an example of a valid inference known as a *syllogism.*

Roughly speaking, we would like to say that an inference is *logically valid* if the conclusion follows from the premisses *by virtue of the "form" of the statements involved.*

For example, the syllogism of (1) is logically valid, because it does not matter what "Socrates" or "man" or "mortal" mean. It would be equally valid to say

$$\begin{array}{r} \text{All men are immortal} \\ \text{Socrates is a man} \\ \hline \text{Socrates is immortal} \end{array} \qquad (2)$$

or

$$\begin{array}{r} \text{All men are mortal} \\ \text{Donald Duck is a man} \\ \hline \text{Donald Duck is mortal} \end{array} \qquad (3)$$

or

All borogoves are mimsy
The Mad Hatter is a borogove

The Mad Hatter is mimsy (4)

It does not matter whether the premisses are true (in some of the above examples they are true, in others they are not) or whether the conclusion is true. It doesn't even matter whether you know what a "borogove" is or what "mimsy" means. The point is:

The four examples of syllogism given above all are of the same **logical form**, *namely,*

All X are Y
Z is an X

Z is a Y (5)

To be able to talk about an inference being "logically valid" we have to be have a way to say what the **form** (or maybe "a" form, rather than "the" form) of an inference is. For example, we could say that all four inferences (1), (2), (3), (4) are of the form (5), and any reasoning of this form is valid. Another example of a valid inference form would be:

X is Z
Y is Z

X and Y are Z (6)

Examples of inferences of the form (6) are:

John is happy
Mary is happy

John and Mary are happy (7)

and

My mother is smart
My father is smart

My mother and my father are smart (8)

So it would seem that we have two examples of "valid forms", namely, (5) and (6). Consider, however, the following examples:

All men are equal
Socrates is a man

Socrates is equal (9)

and

Bob Dole is married
Hillary Clinton is married

Bob Dole and Hillary Clinton are married (10)

Superficially, (9) is "of the form (5)," and (10) is "of the form (6)." Something is clearly wrong here, because in (10) the conclusion is clearly false, even though the premisses are true, and in (9) the conclusion is meaningless.

What is wrong here is that "statement forms" such as "All X are Y" or "X and Y are Z" are not good enough to capture logical distinctions that matter. For example, the statements "Bob Dole and Hillary Clinton are married" and "Bob Dole and Hillary Clinton are smart" both appear to be of the same "form," namely, "X and Y are Z," but they really are not. "Smart" is a **one-variable predicate**. (If x is a person, you can say that "x is smart.") But "married" is *both* a *one-variable predicate* (in "Bob Dole is married") and a 2-variable predicate (in "Bob Dole and Hillary Clinton are married"). In normal English discourse, when we say that "x and y are married" we do not mean that each one, separately, is married. We mean that "x and y are married to each other." (If you don't believe that, ask yourself the following: when someone asks a couple "are you two married", isn't it clear that this means "to each other"?)

So, if we really want to talk about **forms** of statements and inferences, then we need a more sophisticated *formal language*.

One formal language that does the required job rather well is the *predicate calculus*. Using this language, we can see that (1), (2), (3) and (4) are of the form

$$\begin{array}{r} (\forall x)(p(x) \Longrightarrow q(x)) \\ p(a) \\ \hline q(a) \end{array} \qquad (11)$$

(In (1), "$p(x)$" stands for "x is a man," "$q(x)$" for "x is mortal," and "a" for "Socrates." In (2), "$p(x)$" stands for "x is a man," "$q(x)$" for "x is immortal," and "a" for "Socrates." In (3), "$p(x)$" stands for "x is a man," "$q(x)$" for "x is mortal," and "a" for "Donald Duck." In (4), "$p(x)$" stands for "x is a borogove," "$q(x)$" for "x is mimsy," and "a" for "the Mad Hatter.")

On the other hand, *(9) is not if the form (11)*. In fact, to represent (9) correctly we need a binary predicate $E(x, y)$ (meaning "x and y are equal to each other"), and then (9) cannot even be represented in the language. (Using a 1-variable predicate $M(x)$ for "x is a man", and the symbol a for "Socrates", we can represent the premisses as $(\forall x)(\forall y)((M(x) \wedge M(y)) \Longrightarrow E(x, y))$ and $M(a)$. But *there is no way to represent the conclusion*, which is fine because the conclusion is meaningless.)

Similarly, (7) and (8) are of the form

$$\begin{array}{r} p(x) \\ p(y) \\ \hline p(x) \wedge p(y) \end{array} \qquad (12)$$

which is valid, but (10) is of the form

$$\begin{array}{r} p(x) \\ p(y) \\ \hline q(x, y) \end{array} \qquad (12)$$

where q is a *different predicate* from p. (In fact, q is binary and p is unary. Naturally, p and q are related, because $p(x)$ —i.e. "x is married"— is a way of saying $(\exists y)q(x, y)$, i.e. "x is married to somebody," or "there exists a person that x is married to," or "there exists a y such that x is married to y.")

So from on we will use the formalism of the **predicate calculus** to formulate our rules.

PREDICATE CALCULI

A predicate calculus is a formal language whose expressions (or "words") are finite sequences made of some *basic symbols*. (Remember that the plural of "calculus" is "calculi." That's why this section is called "predicate calculi," because there are lots of different such calculi, depending on which symbols you use.)

For the predicate calculi to be considered in this course, there will be *basic symbols*, which are combined to form *terms* and *formulas*.

The basic symbols will be:

1. constants;
2. variables;
3. function symbols;
4. predicate symbols;
5. the logical connectives $\forall$, $\exists$, $\wedge$, $\vee$, $\Rightarrow$, $\Longleftrightarrow$, $\sim$;
6. the left and right parentheses, "(" and ")," and the comma ",".

VARIABLES are letters such as x, y, z, m, n, k, ε, X, Y, etc. In fact, any letter (or even other symbols, such as $\diamond$, or $\aleph$, or even a sequence of letters such as "grrrr" can be used as a variable, provided it is *declared* to be a variable. Often, there is no need to declare a symbol to be a variable, because the context makes it clear that it is a variable. For example, if I write $(\forall x)(x^2 \geq 0)$, then x *has* to be a variable, because only variables can appear in quantifiers such as $(\forall x)(x^2 \geq 0)$.

CONSTANTS are letters such as a, b, c, α, A, B, etc. Actually, any letter (or even other symbols, such as $\diamond$, or $\aleph$, or ε, or x, or y, or π, or e, or 0, or 1, or 2, or 3, or $\emptyset$, or even a sequence of letters such as "grrrr" or "34612) can be used as a constant, provided it is *declared* to be a constant. Often, there is no need to declare a symbol to be a constant, because the context makes it clear that it is a constant. For example, if I write "let a be an arbitrary real number," or "let $a = 3$," or "suppose A and B are sets," then I am declaring that a, b, A, B are going to be treated as constants.

Notice that, if a symbol is a constant, then there are certain things you cannot do with it. For example, after you have declared "a" to be a constant by saying, for example, "let a be an arbitrary real number," *you cannot use quantifiers such as* $(\forall a)$, because a is now fixed, not variable.

Similarly, if a symbol is a variable, then there things you cannot do with it. For example, after you have said in a proof $(\forall x)(\forall y)(x + y = y + x)$, you cannot write in your proof something like $x + y = y + x$, because *this is not a proposition*. (This means that, if x and y are variables, then "$x + y = y + x$" does not have a definite truth value. It doesn't make sense to say that $x + y = y + x$" is true or false unless x and y are given specific values. And, if you give x and y specific, definite values, then they become constants.)

FUNCTION SYMBOLS are letters such as f, g, F, G, or other symbols such as $+$, $\cdot$, $\cap$, $\cup$, $\sim$. Each function symbol admits a *fixed* number of arguments. (If admits *one* argument, then it is a *unary*, or *one-variable* symbol. If admits *two* arguments, then it is a *binary*, or *two-variable* symbol. If admits *three* arguments, then it is a *ternary*, or *three-variable* symbol. And so on.) If you write a function symbol, followed by a "(," then as many arguments as the function symbol admits, separated by commas, and then ")," you get a *term*. The strings that can be used as arguments are variables, or constants, or more general terms.

EXAMPLE. Suppose you want to have a predicate calculus to talk about kinship and comparing ages of people. You could introduce one-variable function symbols f and g to stand for "father of" and "mother of" and, say, a binary predicate y to stand for "the younger of two people." Then, for example, the term $f(Bill)$ would stand for "Bill's father," the term $m(Bill)$ would stand for "Bill's mother," and the term $y(Bill, John)$ would stand for "the younger of Bill and John" (that is, $y(Bill, John) = Bill$ if Bill is younger than John, and $y(Bill, John) = John$ if John is younger than Bill). As explained before, function letters can themselves admit terms as argument, so for example you could write $f(f(Bill))$, which would stand for "Bill's paternal grandfather," $f(m(Bill))$, which would stand for "Bill's maternal grandfather," or even more complicated expressions such as

$$f(m(y(Bill, y(John, Patricia)))),$$

which stands for "the maternal grandfather of the youngest of Bill, John and Patricia." (QUESTION: could we have written $f(m(y(Bill, John, Patricia)))$. Yes? No? Why?)

ANOTHER EXAMPLE. In mathematics, we use a predicate calculus that has symbols for the basic arithmetic operations "$+$" and "$\cdot$" ("plus" and "times"), which are *binary* (that is, you add and multiply *two* numbers). In this case, it is customary to write things such as "$a + b$," "$a \cdot b$," rather than "$+(a, b)$," "$\cdot(a, b)$." There are, of course, many other function symbols in common use. For example, $|\ldots|$ ("absolute value of") is a *one-variable* function symbol, so we use terms such as $|3|$. As in our previous example, one can use terms as arguments, so for example we caan form terms such as $|(|3| + 5).|7 + 8| + 4|$.

PREDICATE SYMBOLS are letters such as p, q, P, Q, or other symbols such as $=$, $>$, $<$, $\leq$, $\geq$, ϵ, $\subseteq$. Each function symbol admits a *fixed* number of arguments. (If admits *one* argument, then it is a *unary*, or *one-variable* predicate. If admits *two* arguments, then it is a *binary*, or *two-variable* predicate. If admits *three* arguments, then it is a *ternary*, or *three-variable* predicate. And so on.) If you write a predicate symbol, followed by a "(," then as many arguments as the predicate symbol admits, separated by commas, and then ")," you get an *atomic formula*. The strings that can be used as arguments are *terms*.

EXAMPLE. Let us go on with the predicate calculus that enables us to talk about kinship and compare ages of people. We could introduce two-variable predicates s, d, c, so that $s(a, b)$ would stand for "a is b's son", $d(a, b)$ would stand for "a is b's daughter", $c(a, b)$ would stand for "a is b's child." (Then $c(a, b) \Longleftrightarrow (s(a, b) \vee d(a, b))$. Make sure you understand why!) We could also have the binary predicate "$=$" with its usual meaning (that is, "$a = b$" means that a and b are the same person). With these symbols, we could say lots of more complicated things. For example, suppose I want to say "a is b's uncle." I could say this by writing

$$(\exists x)(\exists y)(\exists z)\Big(s(a, x) \wedge s(a, y) \wedge (\sim x = y) \wedge (\sim a = z) \wedge c(z, x) \wedge c(z, y) \wedge c(b, z)\Big).$$

ANOTHER EXAMPLE. In mathematics, the predicate calculi we use have symbols for the basic predicates "$=$," "$>$," "$<$," "$\geq$," "$\leq$," which are *binary*. In this case, it is customary to write things such as "$a > b$," "$a = b$," rather than "$> (a, b)$," "$= (a, b)$." There are, of course, many other predicates in common use. For example, for integers we could introduce a binary predicate symbol "$|$" that stands for "divides." (That is, $m|n$ stands for $(\exists k)(k.m = n)$.) These symbols admit terms as arguments, so for example we can write things such as $(3 + 5).7 = |50 + 6|$. Here $(3 + 5).7$ and $|50 + 6|$ are terms, and $(3 + 5).7 = |50 + 6|$ is an atomic formula.)

Atomic formulas can be combined with the logical connectives to yield *formulas*. For example,

$$(\exists x)(\exists y)(\exists z)\Big(s(a, x) \wedge s(a, y) \wedge (\sim x = y) \wedge (\sim a = z) \wedge c(z, x) \wedge c(z, y) \wedge c(b, z)\Big)$$

is *not* an atomic formula, but is obtained from the atomic formulas $s(a, x)$, $s(a, y)$, $x = y$, $a = z$, $c(z, x)$, $c(z, y)$, $c(b, z)$ by combining them via the connectives $\wedge$, $\sim$ and $\exists$.

TERMS VS. FORMULAS

Terms are supposed to be names of "things." **Formulas** are expressions that —when we plug in values for the open variables— become sentences or statements.

For example, the following are terms:

$$\begin{array}{cccc} 3 & 3+5 & x & 5xyz \\ x+3 & 3+5 & x^2+3y+7 & \{x : x^2 < 3y\} \end{array},$$

and the following are formulas:

$$\begin{array}{cccc} 3<5 & 3+5=8 & x+3=7y & 5xyz < x+z \\ (\forall x)(x+3>x) & (\forall x)(x+y>x) & (\exists x)(x+y>xz) & (\forall x)(x>y \Longrightarrow y=z) \end{array}.$$

If you want to see a completely precise definition of "term" and "formula" then you have to consult a mathematical logic textbook. In this course, we will take these concepts for granted.

How can you tell whether something is a term or a formula?

TERMS. A **term** stands for a **definite thing** (it may be a number, or a set, or a line, or a function, or some other entity such a person or an animal), or for a "variable thing" that becomes definite once you plug in values for the variables. (For example, "$3+5$" denotes a definite number, whereas "$3+x$" denotes a "variable number" that becomes definite once you plug in values for x: when you plug in $x = 5$, $3 + x$ has the value 8; when you plug in $x = -3$, $3 + x$ has the value 0; when you plug in $x = -20$, $3 + x$ has the value -17; and so on.) For a more complicated example of a term, consider the expression "$f(x)$". This is a term that contains two letter variables, namely, f and x, standing, respectively, for a function and a number. So, when you plug in a specific function for f, and a specific number for x, you get a number. (For example, if f is the "squaring" function, i.e. the function such that $f(y) = y^2$ for all y, and $x = 3$, then $f(x)$ has the value 9. If f is the "exponential" function, i.e. the function such that $f(y) = e^y$ for all y, and $x = 6$, then $f(x)$ has the value e^6. If f is the function such that $f(y) = y^2 + 3y + 7$ for all y, and $x = 6$, then $f(x)$ has the value 61.)

FORMULAS. A **formula** makes an **assertion**, which may be true or false. So a formula has a **definite truth value** ("true" or "false," often abbreviated T or F) or a "variable truth value" that becomes definite once you plug in values for the variables. (For example, "$3 + 5 = 8$" has a definite truth value, namely, T, and "$3 + 5 = 6$" has a definite truth value, namely, F. On the other hand, "$3 + x = y$" has a variable truth value, which becomes definite once you plug in values for the variables x and y: when you plug in $x = 5$ and $y = 8$, $3 + x = y$ is T; when you plug in $x = 2$ and $y = 8$, $3 + x = y$ is F; when you plug in $x = 2$ and $y = 5$, $3 + x = y$ is T; and so on.)

VARIABLES AND CONSTANTS

As explained before, the basic constituents of terms are *variables* and *constants*.

Constants are symbols that stand —permanently or temporarily— for one *fixed*, *definite* thing. *Variables* are letters such as x, y that are meant to stand for things that only become definite when you assign a specific *value* to the variable.

In principle, any symbol could be used for a constant, and also for a variable. What matters is that in each case it should be clear which use is intended, e.g. by *declaring* a symbol to be a constant or a variable. Usually, letters such as x, y, z, are used as variables for real numbers, letters such as k, m, n, p are used as variables for natural numbers, and letters such as X, Y, Z are used as variables for sets. So, for example, we would write formulas such as

$$(\forall x)(\exists y)(y > x)\,,$$

$$(\forall m)(\forall n)(\forall k)((k|m \wedge k|n) \Rightarrow k|m+n)\,,$$

$$(\forall X)(\forall Y)(\forall Z)((X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z)\,.$$

But there is nothing sacred about this particular use. We could, for example, write

$$(\forall a)(\exists b)(b > a)\,,$$

$$(\forall x)(\forall y)(\forall z)((z|x \wedge z|y) \Rightarrow z|x+y)\,,$$

$$(\forall \alpha)(\forall \beta)(\forall \gamma)((\alpha \subseteq \beta \wedge \beta \subseteq \gamma) \Rightarrow \alpha \subseteq \gamma)\,,$$

provided that we specify that "a, b are real variables, x, y, z are natural-number variables, α, β, γ are set variables."

One way to make it clear that something is a variable and to specify its range is to put the range in the quantifier. For example, if we write

$$(\forall a \in \mathbf{R})(\exists b \in \mathbf{R})(b > a)\,,$$

$$(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})((z|x \wedge z|y) \Rightarrow z|x+y)\,,$$

then it is clear that a, b are real variables, and x, y, z are natural-number variables.

For our third sentence, involving sets, the situation is a little bit more complicated. The obvious thing to do would be to write something like

$$(\forall X \in \mathcal{S})(\forall Y \in \mathcal{S})(\forall Z \in \mathcal{S})((X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z)\,,$$

where $\mathcal{S}$ is "the set of all sets." This, however, is *forbidden*, because the "set of all sets" has to be avoided, due to the Russell Paradox (see below).

So we can get around this by writing, instead,

$$(\forall X)(\forall Y)(\forall Z)((X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z)\,, \quad \text{where } X, Y, Z \text{ are set variables,}$$

or

$$\text{If } X, Y, Z \text{ are sets, then } (X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z\,.$$

Naturally, we could even use more informal expressions such as

$$\text{If } X, Y, Z \text{ are sets, then if } X \subseteq Y \text{ and } Y \subseteq Z \text{ it follows that } \Rightarrow X \subseteq Z\,,$$

or

$$\text{If } X, Y, Z \text{ are sets, and } X \subseteq Y \text{ and } Y \subseteq Z, \text{ then } \Rightarrow X \subseteq Z\,.$$

More complicated terms can be constructed from the basic constants and variables by means of (i) function symbols, and (ii) the "curly bracket" set notation. For example, the expression $x+3$ is a term, obtained by combining the variable x and the constant 3 by means of the binary (i.e. 2-argument) function symbol $+$. The expression $\{x \in \mathbf{R} : x^2 > 2\}$ is a term, that stands for a certain set of numbers. **A more detailed description of how function symbols work, and how to build more complicated terms and work with them, will be given later. For the time being, let us forget about function symbols until further notice, and concentrate on predicates, constants, variables, and the logical connectives.**

THE STRUCTURE OF A PROOF

As was explained before, a **proof** is a sequence of **steps**, each of which must be justified. The justification of a step consists of showing that it is permitted by the rules, given the previous steps.

For example, one of our rules (called "Modus Ponens") will say that if you have two formulas of the form P and $P \Rightarrow Q$, then you can go to Q. So, for example, suppose that you are writing a proof, and you already got

(25) $\quad 3 > 0,$ $\qquad$ (.....)

and, later,

(47) $\quad 3 > 0 \Rightarrow (\exists x)(x^2 = 3).$ $\qquad$ (.....)

Then you are permitted to add a new step to you proof (say Step 95), by saying:

(95) $\quad (\exists x)(x^2 = 3).$ $\qquad$ (Modus Ponens, from (25) and (47)).

Of course, if every step had to be justified by invoking previous steps, then we would never be able to get started. So *some* kinds of steps must be permitted that do not require any previous step. Indeed, we have already mentioned two such kinds of steps, that we labeled (P.a) and (P.b) before. (Recall that (P.a) says that it is always permitted to bring in an axiom as a new step, and (P.b) tells us that it is O.K. to bring in one of the hypotheses.)

In addition, one of our rules will tell us that you can always bring in a tautology. For example, suppose that at some point of a proof you have

(238) $\quad 3 > 0 \vee 3 < 0\,.$ $\qquad$ (.....)

and then later you managed to get

(455) $\quad \sim 3 < 0.$ $\qquad$ (.....)

Armed with these two facts, it should now be possible to go to "$3 > 0$." (Intuitively, this is clear: if you know that either $3 > 0$ or $3 < 0$, and also that it's not the case that $3 < 0$, then the only remaining possibility is that $3 > 0$.) Our rules enable us to do this, as follows (assuming, say, that you have just written Step 698):

(699) $\quad (3 > 0 \vee 3 < 0) \Rightarrow ((\sim 3 < 0) \Rightarrow 3 > 0).$ $\qquad$ (Tautology $(P \vee Q) \Rightarrow ((\sim Q) \Rightarrow P)$)
(700) $\quad (\sim 3 < 0) \Rightarrow 3 > 0.$ $\qquad$ (Modus Ponens from (238) and (699))
(701) $\quad 3 > 0.$ $\qquad$ (Modus Ponens from (455) and (700))

At this point, you may ask "Why did we pick this particular tautology in Step 699?" This question has two answers, depending on what you mean when you ask **why**.

(A) If by "**why?**" you mean "what allows you to do it?" then the answer is quite simple: **because it is a tautology**, and one of our rules allows us to bring in any tautology we want at any time. (Maybe you will ask: how do I know that $(P \vee Q) \Rightarrow ((\sim Q) \Rightarrow P)$ is a tautology? First of all, if you don't believe it, you can check it with truth tables. Second, you should be able to "see" directly that it is a tautology because all it says is that "if one of two things is true and the second thing isn't true, then the first thing must be true," which is clearly true. Third, you can check that $(P \vee Q) \Rightarrow ((\sim Q) \Rightarrow P)$ is a tautology without using truth tables, by just asking yourself "when would $(P \vee Q) \Rightarrow ((\sim Q) \Rightarrow P)$ be false?" For this to happen, $P \vee Q$ must be true but $(\sim Q) \Rightarrow P$ must be false. But $(\sim Q) \Rightarrow P$ can only be false if $\sim Q$ is true but P is false. But if $\sim Q$ is true then Q is false. So if $\sim Q$ is true but P is false then both P and Q must be false. But then $P \vee Q$ is false, and we have already said that it must be true. So it is impossible for $(P \vee Q) \Rightarrow ((\sim Q) \Rightarrow P)$ to be false.)

(B) If by "**why?**" you mean "what for?" (that is, "what is the purpose of picking this particular tautology?"), then the asnwer is **because I had done some strategic planning and I figured that this tautology was precise what I needed.** You can see that my planning was O.K. because it worked, and in Step 701 I got exactly what I wanted.

PROOFS WITHIN PROOFS

There is one more thing you need to know, which is quite easy to understand but somehow confuses many people:

> *Whenever you want, you can start a "subproof," or "proof within a proof," in which you can make* **any assumptions you want**. However, when you do that then all the things you prove are proved **under those assumptions**.

For example, suppose we are reading a mystery novel, and I am trying to prove to you that it was Bob that murdered Bill. Suppose we got to a point where I have established that the murderer must have been Bob or John. Now I want to convince you that it's not John, so it must have been Bob.

Here is one thing I could say: "Suppose John murdered Bill. We know that Bill's body was found in his house, so the killing must have taken place in the house itself, or nearby, because even if the body had been moved it still couldn't have been moved very far. So John must have been in or near Bill's house at the time of the murder. But Bill was killed on September 8 between 9 and 10 p.m. EST. So John must have been in or near Bill's house on September 8 between 9 and 10 p.m. EST. On the other hand, we know that John gave a public lecture in San Diego on September 8, starting at 6 p.m. Pacific time, i.e. at 9 p.m. EST. So he must have traveled from New York to San Diego in one hour or less, which is impossible. So John did not murder Bill."

Notice that what we did here is construct, within our main proof that Bob is the murderer, a "subproof," or "proof within a proof," whose goal is to prove that John is not the murderer. We did this by *introducing a new hypothesis*, namely, by assuming that John is the murderer. In other words, *we created and set out to explore an imaginary world*, in which John did indeed kill Bill, in order to find out what are the consequences and ramifications of the new hypothesis. In this imaginary world, we proved a number of things, such as, for example, that "John traveled from New York to San Diego in one hour or less." But we proved these things *under the hypothesis that John killed Bill.* In order words, we did not really prove that "John traveled from New York to San Diego in one hour or less," but only that this must have been so *if John killed Bill.*

The ultimate consequence of our "proof within a proof" is that this world we have imagined, in which John killed Bill, is impossible, because in this world something impossible happened. So we get out of this "proof within a proof" the conclusion that *John did not kill Bill.* And *this conclusion no longer depends on the new hypothesis that "John killed Bill."* The final conclusion, that *John did not kill Bill*, is valid *without any extra hypotheses*, so it is part of our main proof.

In our mathematical formalism, we will be allowed to start a "proof within a proof" any time we want, by assuming anything we want. However, anything we prove will only be part of this "proof within a proof." There will be rules telling us how to get out of the "proof within a proof" and go back to the main proof. The most important one is the following:

RULE 3. *If assuming P you get to Q, then you can go, without assuming P, to $P \Rightarrow Q$.*

For example, suppose you are writing a proof and you already got,

(3591) $P \Rightarrow Q$ (.....)
(4507) $Q \Rightarrow R$. (.....)

Suppose you just finished writing Step 6812, and now you want to prove $P \Rightarrow R$. Here is one thing you could do:

(6813)	Assume P.	(Preparation to apply Rule 3)
(6814)	Q.	(Modus Ponens from (3591) and (6813))
(6815)	R.	(Modus Ponens from (4507) and (6814))
(6816)	$P \Rightarrow R$.	(Rule 3, from (6813) and (6815))

Steps 6813, 6814, 6815 constitute a "proof within a proof," in which you introduce the new assumption P, and under this assumption you prove first Q and then R. Then in Step 6816 you go back to the main proof, using Rule 3.

Notice that we have used extra indentation to indicate that we are writing a proof within a proof. The way we have organized our proof makes it clear that *at no point are we proving Q or R.* We are proving Q and R *under the assumption* P, from which we can conclude that $P \Rightarrow R$, as we do in Step 6816. For all we know, *Q and R could perfectly well be false*, and nothing in what we wrote says otherwise. All our "proof within a proof" says is that *if you assume that P is true, then Q and R must be true.* The "proof within a proof" tells us nothing about what happens if P is false. And our final conclusion, that $P \Rightarrow R$, is of course valid if P is false.

There is another way to start a "proof within a proof," by *introducing an arbitrary constant.* For example, suppose you want to prove that "if you take a natural number and add it to its square, then the result is an even number." (Symbolically: $(\forall n \in \mathbb{N})(2|n^2 + n)$.) Then you could say: "let us pick an **arbitrary** natural number and let us call it k. I will show that $k^2 + k$ is even. There are two possibilities, namely, that k is even and that k is odd. If k is even then k^2 is also even, so $k^2 + k$ is even, because the sum of two even numbers is even. If k is odd then k^2 is also odd, and then $k^2 + k$ is even, because the sum of two odd numbers is even. So we have seen that in all possible cases $k^2 + k$ must be even. So we have proved $(\forall n \in \mathbb{N})(2|n^2 + n)$."

Notice that here we introduced a new letter k, which serves as the name of a number that is *fixed* throughout our analysis, until we get to the final step, in which we say that, since what we did was O.K. no matter what k was, then we have shown that $(\forall n \in \mathbb{N})(2|n^2 + n)$. In our "proof within a proof," the letter k is treated as a constant.

We could organize this as follows:

(***)	Let $k \in \mathbb{N}$ be arbitrary.	(Preparation to apply Rule 5)
	. . . . .	
	. . . . .	
	. . . . .	
(!!!)	(k is even)$\vee$(k is odd).	(. . . . .)
($$$)	$(\forall n \in \mathbb{N})\Big((n \text{ is even}) \vee (n \text{ is odd})\Big)$.	(Rule 5, from (***) and (!!!))

When we start a subproof by introducing a letter by saying "let such and such be arbitrary," then this has automatically the effect of declaring that letter to be a constant for this subproof. But, **this declaration is "local," that is, valid within the subproof only. Once the subproof is finished, then the effect of this declaration is undone.**

BASIC INFERENCE RULES FOR PROOFS

Let us first review our conditions telling us when a step in a proof is valid.

(P.a) it is always permitted to bring in an *axiom* (or "postulate") as a new step,

(P.b) it is always permitted to bring in one of the hypotheses as a new step,

(P.c) it is always permitted to bring in as a new step something that follows from previous steps by applying a valid *rule of inference*.

(P.d) it is always permitted to start a proof within a proof by introducing any sentence you want as an assumption, or by bringing in a **new** letter as an arbitrary constant. However, whatever is proved after this is done, is only valid in the "proof within a proof", and one can only get out of it by applying Rule 3 or Rule 5.

And here are the eight basic rules of inference.

RULE 1. You are allowed to bring in any statement which is an instance of a tautology.

RULE 2. If you have p and $p \Longrightarrow q$ then you can go to q. (This is called *Modus Ponens*).

RULE 3. If you have proved q under the assumption p (that is, if you have assumed p and proved q), then you can go to $p \Longrightarrow q$.

RULE 4. Suppose $p(x)$ is a formula where there is no quantifier involving x, a is a letter, and $p(a)$ is what you get from $p(x)$ by substituting a for x in **all** the occurrences of x in $p(x)$. Then, if you have $(\forall x)p(x)$ and a has been declared to be a constant, then you can go to $p(a)$.

RULE 5. Suppose $p(x)$ is a formula where there is no quantifier involving x, a is a letter, and $p(a)$ is what you get from $p(x)$ by substituting a for x in **all** the occurrences of x in $p(x)$. Suppose the letter a has not appeared before. Then you can start a proof within a proof by saying "Let a be arbitrary." If in this proof within a proof you get to $p(a)$, then you can go to $(\forall x)p(x)$ in your main proof.

RULE 6. Suppose $p(x)$ is a formula where there is no quantifier involving x, a is a letter, and $p(a)$ is what you get from $p(x)$ by substituting a for x in **all** the occurrences of x in $p(x)$. Suppose the letter a has **not** appeared before. Then you can start a proof within a proof by introducing a new object, calling it a, and stipulating that $p(a)$. This effectively declares a to be a constant, locally, within the "proof within a proof." If you ever get to something that does *not* contain a, then you can use it outside your proof within a proof, in the main proof.

RULE 7. Suppose $p(x)$ is a formula where there is no quantifier involving x, a is a letter, and $p(a)$ is what you get from $p(x)$ by substituting a for x in **all** the occurrences of x in $p(x)$. Then from $p(a)$ you can go to $(\exists x)p(x)$.

RULE 8. You can substitute equals for equals. That is, if you know that $a = b$, then you can go from a statement involving a to the statement in which b is substituted for a in all or some of its ocurrences, and from a statement involving b to the statement in which a is substituted for b in all or some of its ocurrences. (EXAMPLES: (1) If you have $a = b$ and $a.c = a.c$, you can go to $a.c = b.c$. (2) After you have given the definition

$$[0,1] = \{x : 0 \leq x \leq 1\}$$

you can go from $a \in [0,1]$ to $a \in \{x : 0 \leq x \leq 1\}$, and then you can use Set Axiom 2 below to get to $0 \leq a \leq 1$.)

(Naturally, instead of "a" you could use "b," or "z," or "α," or "β," or "$\aleph$," or "$\diamond$," or any symbol you want. What is important is that what you do should apply to a *completely arbitrary*

object in our universe of discourse. Otherwise, you will not be proving that $p(x)$ is true for *all* x. For example —if our universe of discourse is $\mathbf{R}$— it would not be O.K. to prove that $(\forall x)(\exists y)(y^2 = x)$ by saying "Let 9 be arbitrary. Then $(\exists y)(y^2 = 9)$ is true, so we have proved that $(\forall x)(\exists y)(y^2 = x)$." What is wrong here? What is wrong is that 9 is not an *arbitrary* real number. 9 is 9, and just because something is true for the number 9 it doesn't mean that it is true for **all** real numbers.)

(Here **it's important that this new object should be given a name that has not been used before.** For example, suppose $p(x)$ stands for "x killed Polonius," and our universe of discourse is the set of all people. Suppose you are told that $(\exists x)p(x)$, i.e. that somebody killed Polonius. Then you can introduce a name for this individual. You can call him/her a or, if you prefer, "the killer," in which case you would be able to say that $p(a)$, or that p(the killer). But you cannot say "let's call this person Hamlet," or "let's call him Laertes," because Hamlet and Laertes are names of characters that have already appeared in the play. If you call the killer "Hamlet" or "Laertes" then you would be *prejudging*, and declaring that p(Hamlet), i.e. that Hamlet killed Polonius, or that p(Laertes), i.e. that Laertes killed Polonius. One of these happens to be true, and the other one is false, but in either case you cannot just conclude that it is true by merely choosing a name for the killer.)

DERIVED RULES (SHORTCUTS)

In a formal proof you are supposed to use the eight basic rules and nothing else. However, if you really had to do this all the time, then your proofs would become too long. This is why one often "skips steps," or "carries out several steps together." In fact, what you do is observe that in many cases there are certain sequences of steps that appear over and over again. So you know in advance that whenever you have such-and-such formulas you can always go to some other formula. We collect this information into a list of **derived rules**.

EXAMPLE: Suppose you want to go from $(\forall x)(p(x) \Longrightarrow q(x))$ and $p(a)$ to $q(a)$. (For example, you want to deduce the conclusion that "Socrates is mortal" from the premisses "All men are mortal" and "Socrates is a man." In formal language, if $p(x)$ stands for "x is a man," $q(x)$ stands for "x is mortal," and a stands for "Socrates," then the premisses are precisely $(\forall x)(p(x) \Longrightarrow q(x))$ and $p(a)$, and what you want to get is $q(a)$.) Then you could do it as follows:

(1) $(\forall x)(p(x) \Longrightarrow q(x))$ (hypothesis);
(2) $p(a)$ (hypothesis);
(3) $p(a) \Longrightarrow q(a)$ (Rule 4, specialization of (1) to $x = a$);
(4) $q(a)$ (Rule 2, from (2) and (3)).

However, this situation is going to occur over and over again, and you do not want to repeat the above four steps every time, so you can state a

DERIVED RULE 1. If you have $(\forall x)(p(x) \Longrightarrow q(x))$ and $p(a)$ then you can go to $q(a)$.

JUSTIFICATION: Steps (1), (2), (3), (4) above.

Now that you have Derived Rule 1, every time you need to go from (1) and (2) as above you can skip (3), and go directly to (4), invoking the derived rule.

Here are a few more derived rules. There are lots of them. Hundreds of them. But you do not need to memorize them, because they are all rather trivial and reflect plain common sense, and you can derive them whenever you want to. For example, Derived Rule 10 is the basis of "proofs by contradiction," but what it says is rather obvious:

(E) If you put yourself in a scenario where q is not true, and end up showing that something impossible must happen, then this scenario cannot be possible, so q must be true.

Students sometimes find proofs by contradiction hard to justify. Read the previous explanation (E) a couple of times. You should have no trouble understanding that the justification of proofs by contradiction is quite trivial.

Another example: Derived Rule 15 says another completely obvious and trivial thing: suppose that q necessarily must be true when p is false, and also when p is true. Then q must be true (because p is either true or false, and in either case q is true.)

DERIVED RULE 2. If you have $p \wedge q$ then you can go to p.

JUSTIFICATION: $p \wedge q \Longrightarrow p$ is a tautology, so you can bring it in any time you want. If in addition you have $p \wedge q$, then from this and $p \wedge q \Longrightarrow p$ you get p by Modus Ponens (Rule 2).

DERIVED RULE 3. If you have $p \wedge q$ then you can go to q.

JUSTIFICATION: $(p \wedge q) \Longrightarrow q$ is a tautology, so you can bring it in any time you want. If in addition you have $p \wedge q$, then from this and $(p \wedge q) \Longrightarrow q$ you get q by Modus Ponens (Rule 2).

DERIVED RULE 4. If you have p and q then you can go to $p \wedge q$.

JUSTIFICATION: $p \Longrightarrow (q \Longrightarrow (p \wedge q))$ is a tautology, so you can bring it in any time you want. If in addition you have p and q, then from p and $p \Longrightarrow (q \Longrightarrow (p \wedge q))$ you get $q \Longrightarrow (p \wedge q)$ by Modus Ponens (Rule 2), and then from q and $q \Longrightarrow (p \wedge q)$ you get $p \wedge q$.

DERIVED RULE 5. If you have p then you can go to $p \vee q$.

JUSTIFICATION: $p \Longrightarrow (p \vee q)$ is a tautology, so you can bring it in any time you want. If in addition you have p, then from p and $p \Longrightarrow (p \vee q)$ you get $p \vee q$ by Modus Ponens (Rule 2).

DERIVED RULE 6. If you have q then you can go to $p \vee q$.

JUSTIFICATION: $q \Longrightarrow (p \vee q)$ is a tautology, so you can bring it in any time you want. If in addition you have q, then from q and $q \Longrightarrow (p \vee q)$ you get $p \vee q$ by Modus Ponens (Rule 2).

DERIVED RULE 7. If you have $p \Longrightarrow q$ and $q \Longrightarrow p$ then you can go to $p \Longleftrightarrow q$.

JUSTIFICATION: $(p \Longrightarrow q) \Longrightarrow ((q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q))$ is a tautology, so you can bring it in any time you want. If in addition you have $p \Longrightarrow q$, then from $p \Longrightarrow q$ and $(p \Longrightarrow q) \Longrightarrow ((q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q))$ you get $(q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q)$ by Modus Ponens (Rule 2). If you also have $q \Longrightarrow p$, then from $q \Longrightarrow p$ and $(q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q)$ you get $p \Longleftrightarrow q$ by Modus Ponens (Rule 2).

DERIVED RULE 8. If you have $p \Longleftrightarrow q$ then you can go to $p \Longrightarrow q$.

JUSTIFICATION: $(p \Longleftrightarrow q) \Longrightarrow (p \Longrightarrow q)$ is a tautology, so you can bring it in any time you want. If in addition you have $p \Longleftrightarrow q$, then from $p \Longleftrightarrow q$ and $(p \Longleftrightarrow q) \Longrightarrow (p \Longrightarrow q)$ you get $p \Longrightarrow q$ by Modus Ponens (Rule 2).

DERIVED RULE 9. If you have $p \Longleftrightarrow q$ then you can go to $q \Longrightarrow p$.

JUSTIFICATION: $(p \Longleftrightarrow q) \Longrightarrow (q \Longrightarrow p)$ is a tautology, so you can bring it in any time you want. If in addition you have $p \Longleftrightarrow q$, then from $p \Longleftrightarrow q$ and $(p \Longleftrightarrow q) \Longrightarrow (q \Longrightarrow p)$ you get $q \Longrightarrow p$ by Modus Ponens (Rule 2).

DERIVED RULE 10. If assuming $\sim q$ you get a contradiction, then you can go to q.

JUSTIFICATION: Suppose that assuming $\sim q$ you get c, which is a contradiction. Then you can go to $\sim q \Longrightarrow c$ by Rule 3. Now, if c is a contradiction, then $(\sim q \Longrightarrow c) \Longrightarrow q$ is a tautology (why?), so you can bring it in. Since you have $\sim q \Longrightarrow c$, then from $\sim q \Longrightarrow c$ and $(\sim q \Longrightarrow c) \Longrightarrow q$ you get q by Modus Ponens (Rule 2).

DERIVED RULE 11. From $\sim p$ and $p \vee q$ you can go to q.

JUSTIFICATION: $(\sim p) \Longrightarrow ((p \vee q) \Longrightarrow q)$ is a tautology, so you can bring it in any time you want. If in addition you have $\sim p$, then you get $(p \vee q) \Longrightarrow q$ by Modus Ponens (Rule 2). If you also have $p \vee q$, then you get q by Modus Ponens (Rule 2).

DERIVED RULE 12. From $\sim q$ and $p \vee q$ you can go to p.

JUSTIFICATION: $(\sim q) \Longrightarrow ((p \vee q) \Longrightarrow p)$ is a tautology, so you can bring it in any time you want. If in addition you have $\sim q$, then you get $(p \vee q) \Longrightarrow p$ by Modus Ponens (Rule 2). If you also have $p \vee q$, then you get p by Modus Ponens (Rule 2).

DERIVED RULE 13. If assuming p and $\sim q$ you get $\sim p$, then you can go to $p \Longrightarrow q$.

JUSTIFICATION: Assume p. Then assuming $\sim q$ you can get $\sim p$, and you can also get p, so you can get $p \wedge \sim p$ by Derived Rule 4. But $p \wedge \sim p$ is a contradiction. So you can get q by Derived Rule 12, still assuming p. In other words, assuming p we get q. By Rule 3, we get $p \Longrightarrow q$.

DERIVED RULE 14. If assuming $\sim p$ you get q, then you can go to $p \vee q$.

JUSTIFICATION: $((\sim p) \Longrightarrow q) \Longrightarrow (p \vee q)$ is a tautology, so you can bring it in any time you want. If you can prove q assuming $\sim p$, then you get $(\sim p) \Longrightarrow q$ by Rule 3. But then from $(\sim p) \Longrightarrow q$ and $((\sim p) \Longrightarrow q) \Longrightarrow (p \vee q)$ you get $p \vee q$ by Modus Ponens (Rule 2).

DERIVED RULE 15. If assuming $\sim p$ you get q, and assuming p you also get q, then you can go to q assuming nothing.

JUSTIFICATION: $((\sim p) \Longrightarrow q) \Longrightarrow ((p \Longrightarrow q) \Longrightarrow q)$ is a tautology, so you can bring it in any time you want. If you can prove q assuming $\sim p$, then you get $(\sim p) \Longrightarrow q$ by Rule 3. But then from $(\sim p) \Longrightarrow q$ and $((\sim p) \Longrightarrow q) \Longrightarrow ((p \Longrightarrow q) \Longrightarrow q)$ you get $(p \Longrightarrow q) \Longrightarrow q$ by Modus Ponens (Rule 2). If you can also prove q assuming p, then you get $p \Longrightarrow q$ by Rule 3. But then from $p \Longrightarrow q$ and $(p \Longrightarrow q) \Longrightarrow q$ you get q by Modus Ponens (Rule 2).

DERIVED RULE 16. If assuming p you get q, and assuming q you get p, then you can go to $p \Longleftrightarrow q$.

JUSTIFICATION: $(p \Longrightarrow q) \Longrightarrow ((q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q))$ is a tautology, so you can bring it in any time you want. If you can prove q assuming p, then you get $p \Longrightarrow q$ by Rule 3. But then from $p \Longrightarrow q$ and $(p \Longrightarrow q) \Longrightarrow ((q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q))$ you get $(q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q)$ by Modus Ponens (Rule 2). If you can also prove p assuming q, then you get $q \Longrightarrow p$ by Rule 3. But then from $q \Longrightarrow p$ and $(q \Longrightarrow p) \Longrightarrow (p \Longleftrightarrow q)$ you get $p \Longleftrightarrow q$ by Modus Ponens (Rule 2).

DERIVED RULE 17. If you have $(\forall x \in S)p(x)$ and you have $s \in S$, you can go to $p(s)$.

JUSTIFICATION: $(\forall x \in S)p(x)$ is an abbreviation of $(\forall x)(x \in S \Longrightarrow p(x))$. If you have $(\forall x)(x \in S \Longrightarrow p(x))$, then by specialization (Rule 4) you can get $s \in S \Longrightarrow p(s)$. So, if you have in addition $s \in S$, then by Modus Ponens (Rule 2) you get $p(s)$.

DERIVED RULE 18. To prove a statement of the form $(\forall x \in S)p(x)$, you start by saying "Let a be an arbitrary element of S" (that is, "let a be arbitrary; assume $a \in S$") and then try to prove $p(a)$. (Here, again, instead of "a" you could use "b," or "z," or "α," or "β," or "$\aleph$," or "$\diamond$," or any symbol you want. What is important that what you do should apply to a *completely arbitrary* element of S.)

JUSTIFICATION: $(\forall x \in S)p(x)$ is an abbreviation of $(\forall x)(x \in S \Longrightarrow p(x))$. If, starting from "let a be arbitrary" and "assume $a \in S$" you get $p(a)$, it means that starting with "let a be arbitrary" you can get $a \in S \Longrightarrow p(a)$ by Rule 3. So by Rule 5 you have proved that $(\forall x)(x \in S \Longrightarrow p(x))$, i.e. that $(\forall x \in S)p(x)$.

DERIVED RULE 19. If you have $(\exists x \in S)p(x)$ then you can introduce a new object and give it a letter name such as a or α or anything you want, provided that this name has not been used before, and stipulate that $a \in S$ and $p(a)$.

JUSTIFICATION: $(\exists x \in S)p(x)$ is an abbreviation of $(\exists x)(x \in S \wedge p(x))$. So, if you have $(\exists x \in S)p(x)$, then you have $(\exists x)(x \in S \wedge p(x))$. So by Rule 6 you can introduce a new object and give it the letter name a, and stipulate that $a \in S \wedge p(a)$. But then, by Derived Rules 2 and 3, once you got $a \in S \wedge p(a)$, you can go to $a \in S$ and to $p(a)$.

DERIVED RULE 20. If you have $p(a)$ and $a \in S$ then you can go to $(\exists x \in S)p(x)$.

JUSTIFICATION: $(\exists x \in S)p(x)$ is an abbreviation of $(\exists x)(x \in S \wedge p(x))$. So, if you have $a \in S$ and $p(a)$ then you can go to $a \in S \wedge p(a)$ by Derived Rule 4. Then you get $(\exists x)(x \in S \wedge p(x))$ by Rule 7.

DERIVED RULE 21. If you have $(\forall x)p(x)$ and y is some other variable that does not appear in $p(x)$, then you can go to $(\forall y)p(y)$.

JUSTIFICATION: Let a be a new letter. Then you can introduce a new constant by saying "let a be arbitrary," and then by specialization (Rule 4) you can go from $(\forall x)p(x)$ to $p(a)$. Since a was arbitrary, you can go to $(\forall y)p(y)$.

DERIVED RULE 22. If you have $(\exists x)p(x)$ and y is some other variable that does not appear in $p(x)$, then you can go to $(\exists y)p(y)$.

JUSTIFICATION: Let a be a new letter. Then, since you have $(\exists x)p(x)$, you can introduce a new constant via Rule 6 by saying "let a be such that $p(a)$." Then by Rule 7 you can go to $(\exists y)p(y)$.

Why do we insist, in Derived Rules 21 and 22, that y cannot occur in $p(x)$? Suppose, for example, that $p(x)$ is the formula $(\exists y)(y \neq x)$. Then "$(\forall x)p(x)$" says that "$(\forall x)(\exists y)(y \neq x)$." We can of course introduce an arbitrary constant a, and then use Rule 4 to get $p(a)$, i.e. $(\exists y)(y \neq a)$. Now, can we apply Rule 5 to go to $(\forall y)(\exists y)(y \neq a)$? No! Why? Because Rule 5 tells us that if we have proved $q(a)$, then we can go to $(\forall y)q(y)$, *if $q(y)$ is a formula having no y-quantifiers and $q(a)$ is what you get from $q(y)$ by substituting a for y wherever y occurs.*

AN EXAMPLE OF SOMETHING YOU **CANNOT** DO

Many students seem to think that the specialization rule allows you to go from

$$\sim (\forall x)p(x) \qquad \text{to} \qquad \sim p(s) \tag{A}$$

if s is a term that satisfies restriction (R).

Can one do this? The answer is **NO!!!!!**. Why not? Is it because the teacher says so? NO! It does not matter what I say! You cannot do it because plain common sense tells you that it cannot be done. All you need is to think a little bit. Here are some special instances of Inference (A). (Note: the (A) stands for "awful".)

1. From "not everybody is a Democrat" we can go to "I am not a Democrat."
2. From "not everybody is an actor" you can go to "Tom Hanks is not an actor."

Silly, isn't it? That's why you cannot do it! Because it suffices to **think** about it for ten seconds to see that it's silly! Never mind what I tell you or what the book tells you! If I told you that (A) is permitted, then you should reject what I have told you.

Incidentally: can you **prove** that (A) is **not**, cannot be, a valid derived rule? Yes, sure you can. Every single one of our basic rules takes you from true statements to true statements. Every derived rule does the same, because a derived rule never gives you anything that you cannot get by applying the basic rules. So every valid rule, basic or derived, will yield true statements when applied to true statements. "Rule (A)" does not do this, so it is not a valid rule.

HOW DO YOU KNOW WHETHER SOMETHING THAT LOOKS LIKE A VALID RULE REALLY IS VALID?

Let us look at two concrete examples:

(1) Can you go from $(\forall x)p(x) \wedge (\forall x)q(x)$ to $(\forall x)(p(x) \wedge q(x))$?

(2) Can you go from $(\exists x)p(x) \wedge (\exists x)q(x)$ to $(\exists x)(p(x) \wedge q(x))$?

Let us settle (2) first. The answer is **NO!!!**. Why? **Think!** If you know that "some people are rich" and "some people are happy," does it follow that there is a person that is **both** rich and happy? It doesn't, right? So, you see, you **cannot** go from $(\exists x)p(x) \wedge (\exists x)q(x)$ to $(\exists x)(p(x) \wedge q(x))$.

Now, how about (1)? Here, if you think for a minute, you see right away that *every time* $(\forall x)p(x) \wedge (\forall x)q(x)$ *is true, then* $(\forall x)(p(x) \wedge q(x))$ *has to be true too.* (Example: if you know that "everybody is rich and everybody is happy" then you can conclude that "everybody is both rich and happy.")

In order to be completely sure, let us check that you can do this using our rules:

Starting from $(\forall x)p(x) \wedge (\forall x)q(x)$,
you can go to $(\forall x)p(x)$, by Derived Rule 2,
and to $(\forall x)q(x)$ by Derived Rule 3.

Now, let a be arbitrary.
Since we have $(\forall x)p(x)$, by specialization we get $p(a)$.
Since we have $(\forall x)q(x)$, by specialization we get $q(a)$.
Since we have $p(a)$ and $q(a)$, by Derived Rule 4 we get $p(a) \wedge q(a)$.

So we have proved $p(a) \wedge q(a)$ for an arbitrary a. Therefore we can go to $(\forall x)(p(x) \wedge q(x))$ by Rule 5.

As you can see, **you can always go from** $(\forall x)p(x) \wedge (\forall x)q(x)$ **to** $(\forall x)(p(x) \wedge q(x))$ **by applying the rules.** In order words, you can make a new derived rule:

DERIVED RULE 23. From $(\forall x)p(x) \wedge (\forall x)q(x)$ you can go to $(\forall x)(p(x) \wedge q(x))$.

The justification of this derived rule is the sequence of steps given above.

Do you need to memorize millions and millions of derived rules? NO!!!!! Do you need to memorize millions and millions of examples of things that are *not* valid? NO!!!! As the above examples show, it's always quite easy for you to figure out, in each case, whether you are dealing with a valid rule or not.

TWO EXAMPLES OF PROOFS FOLLOWING THE RULES

Here are two simple examples of proofs. We will show that, if $q(x)$ is a predicate over a domain of discourse U and r is a proposition, then

$$(\exists x)\Big(r \wedge q(x)\Big) \iff r \wedge (\exists x)(q(x)) \qquad (I)$$

and

$$(\forall x)\Big(r \vee q(x)\Big) \iff r \vee (\forall x)(q(x)) \qquad (II)$$

are theorems of the predicate calculus. Let us prove these two things using our rules.

PROOF OF (I), WITH SHORTCUTS:

(1)	Assume $(\exists x)\Big(r \wedge q(x)\Big)$.	(Preparation to apply Rule 3)
(2)	Let a be such that $r \wedge q(a)$.	(Rule 6, from (1))
(3)	r.	(Derived Rule 2, from (2))
(4)	$q(a)$.	(Derived Rule 3, from (2))
(5)	$(\exists x)q(x)$.	(Rule 7, from (4))
(6)	$r \wedge (\exists x)q(x)$.	(Derived Rule 4, from (3) and (5))
(7)	$r \wedge (\exists x)q(x)$.	(Rule 6, from (6))
(8)	Assume $r \wedge (\exists x)q(x)$.	(Preparation to apply Rule 3)
(9)	r.	(Derived Rule 2, from (8))
(10)	$(\exists x)q(x)$.	(Derived Rule 3, from (8))
(11)	Let a be such that $q(a)$.	(Rule 6, from (10))
(12)	$r \wedge q(a)$.	(Derived Rule 4, from (9) and (11))
(13)	$(\exists x)(r \wedge q(x))$.	(Rule 7, from (12))
(14)	$(\exists x)(r \wedge q(x))$.	(Rule 6, from (6))
(13)	$(\exists x)\Big(r \wedge q(x)\Big) \iff r \wedge (\exists x)q(x)$.	(Derived Rule 16, because we got to (6) from (1) and to (12) from (7))

Q.E.D.

PROOF OF (II), WITH SHORTCUTS:

(1) Assume $(\forall x)\Big(r \vee q(x)\Big)$. (Preparation to apply Rule 3)
(2) Assume $\sim r$. (Preparation to apply Rule 3)
(3) Let a be arbitrary. (Preparation to apply Rule 5)
(4) $r \vee q(a)$. (Rule 4, specializing to $x = a$ in (1))
(5) $q(a)$. (Derived Rule 11, from (2) and (4))
(6) $(\forall x)q(x)$. (Rule 5, from (3) and (5))
(7) $r \vee (\forall x)q(x)$. (Derived Rule 14, bec. we proved $(\forall x)q(x)$ assuming $\sim r$)
(8) Assume $r \vee (\forall x)q(x)$. (Preparation to apply Rule 3)
(9) Assume $\sim r$. (Preparation to apply Rule 3)
(10) $(\forall x)q(x)$. (Derived Rule 11, from (8) and (9))
(11) Let a be arbitrary. (Preparation to apply Rule 5)
(12) $q(a)$. (Rule 4, specializing to $x = a$ in (10))
(13) $r \vee q(a)$. (Derived Rule 6, from (12))
(14) $(\forall x)(r \vee q(x))$. (Rule 5, because we proved $r \vee q(a)$ for arbitrary a)
(15) Assume r. (Preparation to apply Rule 5)
(16) Let a be arbitrary. (Preparation to apply Rule 5)
(17) $r \vee q(a)$. (Derived Rule 5, from (16))
(18) $(\forall x)(r \vee q(x))$. (Rule 5, because we proved $r \vee q(a)$ for arbitrary a)
(19) $(\forall x)(r \vee q(x))$. (Derived Rule 15, because we proved the formula $(\forall x)(r \vee q(x))$ assuming $\sim r$ and also assuming r)

Now let us write A for $(\forall x)(r \vee q(x))$, and B for $r \vee (\forall x)q(x)$.
(20) $A \iff B$. (Derived Rule 16, because we proved A assuming B and B assuming A.)

Q.E.D.

NOTE: You may think that these proofs are very complicated. They are not! Read them very carefully, and you will see that all we are doing is very simple and obvious things. The point of writing these particular proofs is to show you the rules —and the shortcuts— in action.

To understand what these two proofs really are about, let us rewrite them in plain English, i.e. in "informal language:"

INFORMAL PROOF OF (I):

We want to prove an equivalence of the form $A \iff B$, so we prove that we can get B from A and then that we can get A from B. To get from A to B, we notice that A says that $(\exists x)(r \wedge q(x))$, and we want to prove B, i.e. that $r \wedge (\exists x)q(x)$. Now, if $(\exists x)(r \wedge q(x))$ is true then we can pick an object a such that $r \wedge q(a)$ is true. So both r and $q(a)$ are true. But since $q(a)$ is true then $(\exists x)q(x)$ is true, and since r is true we get $r \wedge (\exists x)q(x)$, i.e. B. To get from B to A we use a similar strategy. B says that $r \wedge (\exists x)q(x)$. So if B is true then r is true and $(\exists x)q(x)$. But then we can pick an object a such that $q(a)$ holds. But then r and $q(a)$ hold, so $r \wedge q(a)$ is true. Therefore we can conclude that $(\exists x)(r \wedge q(x))$ holds, i.e. that A holds.

END OF PROOF

INFORMAL PROOF OF (II):

We want to prove an equivalence of the form $A \Longleftrightarrow B$, so we prove that we can get B from A and then that we can get A from B. To get from A to B, we notice that A says that $(\forall x)(r \vee q(x))$, and we want to prove B, i.e. that $r \vee (\forall x)q(x)$. Assume A is true. Consider first the case when r is true. Then $r \vee (\forall x)q(x)$ holds, i.e. B holds. Now suppose r is false. Let a be arbitrary. Then $r \vee q(a)$ is true. Since r is false, $q(a)$ must be true. But a is completely arbitrary, so $(\forall x)q(x)$ holds. So $r \vee (\forall x)q(x)$ holds, i.e. B holds. So we have shown that B follows from A both when r is true and when it is false. So B follows from A. Now let show that A followsfrom B. Suppose B is true. Then $r \vee (\forall x)q(x)$. Consider first the case when r is false. Then $(\forall x)q(x)$ is true. So, if a is arbitrary, we have $q(a)$, and then we get $r \vee q(a)$. So $(\forall x)(r \vee q(x))$ holds. Now suppose r is true. Then for arbitrary a $r \vee q(a)$ is true, so once again $(\forall x)(r \vee q(x))$ holds. In both cases —that is, when r is false and when r is true— we have shown that A follows from B. **END OF PROOF**

What is the difference between a formal proof and an informal one? **As long as you are able to translate an informal argument into a formal proof, you are free to write informal proofs.**

The trouble is (and believe me, **I know this from experience**), students usually write informal proofs with vague, imprecise justifications, and the reason is that they **do not know** what they are really trying to say. For example, students will often write justifications of steps such as the following:

(1) By the definition of real number,

(2) by the definition of equality,

(3) by tautology,

(4) by specialization,

(5) because it's in the book,

(6) because the teacher said something like that in class.

In this course, these tricks do not work:

If you tell me that something is true "by the definition of real number," then I will ask you to state precisely your definition of real number, and to tell me how it applies. If you cannot answer, then I will take it that you really did **not** know how to justify you step.

If you tell me that something is true "by the definition of equality," then I will ask you to state precisely your definition of equality, and to tell me how it applies. If you cannot answer, then I will take it that you really did **not** know how to justify you step.

If you tell me that something is true "by tautology," then I will ask you to tell me exactly which tautology you have in mind, and if you cannot answer then I will take it that you really did **not** know how to justify you step.

If you tell me that something is true "by specialization," then I will ask you to tell me exactly which variable you are specializing, into which value, and in which formula. If you cannot answer then I will take it that you really did **not** know how to justify you step.

If you tell me that something is true "because it is in the book," then I will ask you to show me exactly where it is and exactly how it applies here. If you cannot answer then I will take it that you really did **not** know how to justify you step.

If you tell me that something is true "because the teacher said it in class," remember that **I am the teacher** and I usually remember quite well what I said. And if I said something

wrong—which is possible, because I can make mistakes too— then it's wrong, and the fact that I said it is not a justification.

Keep the following general principle in mind:

WHAT LOOKS LIKE A CONFUSED EXPRESSION OF A CLEAR THOUGHT IS OFTEN NO MORE THAN A CLEAR EXPRESSION OF A CONFUSED THOUGHT.

It is **your job** to persuade me that your thoughts are not confused. Good formal proofs will do the job. An informal proof may do it too, provided you know how to make it formal. If you do not know how to do it, then I will almost certainly know that you don't know.

In the other direction, you should also remember that proofs with shortcuts are just shortened versions of proofs with no shortcuts at all. To make this point, here is a proof of (I) without any shortcuts.

PROOF OF (I), WITHOUT USING DERIVED RULES:

(1)	Assume $(\exists x)\Big(r \wedge q(x)\Big)$.	(Preparation to apply Rule 3)
(2)	Let a be such that $r \wedge q(a)$.	(Rule 6, from (1))
(3)	$(r \wedge q(a)) \Longrightarrow r$	(Rule 1; instance of the tautology $(\alpha \wedge \beta) \Longrightarrow \alpha$)
(4)	$(r \wedge q(a)) \Longrightarrow q(a)$	(Rule 1; instance of the tautology $(\alpha \wedge \beta) \Longrightarrow \beta$)
(5)	r.	(Rule 2, from (2) and (3))
(6)	$q(a)$.	(Rule 2, from (2) and (4))
(7)	$(\exists x)q(x)$.	(Rule 7, from (6))
(8)	$r \Longrightarrow \Big((\exists x)q(x) \Longrightarrow \Big(r \wedge (\exists x)q(x)\Big)\Big)$.	(Rule 1; tautology $\alpha \Longrightarrow (\beta \Longrightarrow (\alpha \wedge \beta))$)
(9)	$(\exists x)q(x) \Longrightarrow \Big(r \wedge (\exists x)q(x)\Big)$.	(Rule 2, from (5) and (8))
(10)	$r \wedge (\exists x)q(x)$.	(Rule 2, from (7) and (9))
(11)	$r \wedge (\exists x)q(x)$.	(Rule 6)
(12)	$(\exists x)\Big(r \wedge q(x)\Big) \Longrightarrow \Big(r \wedge (\exists x)q(x)\Big)$.	(Rule 3, from (1) and (11), because we have proved $r \wedge (\exists x)q(x)$ assuming $(\exists x)\Big(r \wedge q(x)\Big)$)
(13)	Assume $r \wedge (\exists x)q(x)$.	(Preparation to apply Rule 3)
(14)	$\Big(r \wedge (\exists x)q(x)\Big) \Longrightarrow r$.	(Rule 1; instance of the tautology $(\alpha \wedge \beta) \Longrightarrow \alpha$)
(15)	$\Big(r \wedge (\exists x)q(x)\Big) \Longrightarrow (\exists x)q(x)$.	(Rule 1; instance of the tautology $(\alpha \wedge \beta) \Longrightarrow \beta$)
(16)	r.	(Rule 2, from (12) and (13))
(17)	$(\exists x)q(x)$.	(Rule 2, from (13) and (15))
(18)	Let a be such that $q(a)$.	(Rule 6, from (17))
(19)	$r \Longrightarrow (q(a) \Longrightarrow (r \wedge q(a)))$.	(Rule 1; instance of the tautology $\alpha \Longrightarrow (\beta \Longrightarrow (\alpha \wedge \beta))$)
(20)	$q(a) \Longrightarrow (r \wedge q(a))$.	(Rule 2, from (16) and (19))
(21)	$r \wedge q(a)$.	(Rule 2, from (18) and (20))
(22)	$(\exists x)(r \wedge q(x))$.	(Rule 7, from (21))
(23)	$(\exists x)(r \wedge q(x))$.	(Rule 6)

(24) $\Big(r \wedge (\exists x)q(x)\Big) \Longrightarrow (\exists x)\Big(r \wedge q(x)\Big)$. (Rule 3, from (13) and (23), because we have proved $(\exists x)\Big(r \wedge q(x)\Big)$ assuming $r \wedge (\exists x)q(x)$)

Now let us write A for $(\exists x)\Big(r \wedge q(x)\Big)$, B for $r \wedge (\exists x)q(x)$.

(25) $(A \Longrightarrow B) \Longrightarrow ((B \Longrightarrow A) \Longrightarrow (A \Longleftrightarrow B))$. (tautology)

(26) $(B \Longrightarrow A) \Longrightarrow (A \Longleftrightarrow B)$. (Rule 2, from (12) —which says $A \Longrightarrow B$— and (26))

(27) $A \Longleftrightarrow B$. (Rule 2, from (24) —which says $B \Longrightarrow A$— and (25))

Q.E.D.

PROBLEM 1: give a completely formal proof of (II), without shortcuts.

In the following problems, you must first decide whether the statement to be proved is true for all possible choices for the predicates under consideration. If your answer is "no," then you must give an example of a predicate or predicates for which the statement is false. If your answer is "yes," then you must give a proof. (Shortcuts are allowed, but you should provide full justification of each step by explaining which rule or derived rule you are using. You can create new derived rules if you wish, but then you have to give them a name and justify them.)

PROBLEM 2: prove or disprove that, if p and q are 1-variable predicates, then

$$(\forall x)(p(x) \vee q(x)) \Longleftrightarrow ((\forall x)p(x) \vee (\forall x)q(x))\,.$$

PROBLEM 3: prove or disprove that, if p is a 1-variable predicate, then

$$\Big(\sim (\forall x)p(x)\Big) \Longleftrightarrow (\exists x)(\sim p(x))\,.$$

.

PROBLEM 4: prove or disprove that, if p and q are 1-variable predicates, then

$$(\forall x)(p(x) \Longrightarrow q(x)) \Longrightarrow ((\forall x)p(x) \Longrightarrow (\forall x)q(x))\,.$$

PROBLEM 5: prove or disprove that, if p and q are 1-variable predicates, then

$$((\forall x)p(x) \Longrightarrow (\forall x)q(x)) \Longrightarrow (\forall x)(p(x) \Longrightarrow q(x))\,.$$

A SIMPLE PROOF FROM ARITHMETIC

We now consider a third example, namely, a simple proof from arithmetic. Here are some axioms about real numbers and addition. (The universe of discourse is $\mathbf{R}$, the set of real numbers.) *You will get the full list of axioms for arithmetic in the next handout.*

Add1. $(\forall x)(\forall y)(x + y = y + x)$.

Add2. $(\forall x)(\forall y)(\forall z)\Big(x + (y + z) = (x + y) + z)\Big)$.

Add3. $(\forall x)(x + 0 = x)$.

Add4. $(\forall x)(\exists y)(x + y = 0)$.

NOTE: These axioms express, respectively, the *commutative property* of addition, the *associative property* of addition, the fact that *zero is an additive identity*, and the fact that *every number has an additive inverse.*

In addition, we need three axioms about equality:

Eq1. $(\forall x)(x = x)$.

Eq2. $(\forall x)(\forall y)(x = y \Longrightarrow y = x)$.

Eq3. $(\forall x)(\forall y)(\forall z)((x = y \wedge y = z) \Longrightarrow x = z)$.

Let us prove, using these axioms, the following

THEOREM: *The additive inverse of a real number is unique.*

PROOF (WITH LOTS OF SHORTCUTS): Suppose x is a real number, and y, z are additive inverses of x. We have to prove that $y = z$. Now, the fact that y and z are additive inverses of x means that $x + y = 0$ and $x + z = 0$. Then

$$\begin{aligned}
y &= y + 0 && \text{(by Axiom Add3)} \\
&= 0 + y && \text{(by Axiom Add1)} \\
&= (x + z) + y && \text{(by Rule 8, because } 0 = x + z\text{)} \\
&= (z + x) + y && \text{(by Axiom Add1)} \\
&= z + (x + y) && \text{(by Axiom Add2)} \\
&= z + 0 && \text{(by Rule 8, because } x + y = 0\text{)} \\
&= z && \text{(by Axiom Add3)}.
\end{aligned}$$

A PROOF WITHOUT SHORTCUTS: We have to prove the following:

$$(\forall x)(\forall y)(\forall z)((x+y=0 \wedge x+z=0) \Longrightarrow y=z)\,. \qquad (@)$$

Here is a proof:

(1) $(\forall x)(x+0=x)$.
(2) $(\forall x)(\forall y)(\forall z)\Big(x+(y+z)=(x+y)+z\Big)$.
(3) $(\forall x)(\forall y)\Big(x+y=y+x\Big)$.
(4) Let a be arbitrary.
(5) Let u be arbitrary.
(6) Let v be arbitrary.
(7) Assume $a+u=0 \wedge a+v=0$.
(8) $(a+u=0 \wedge a+v=0) \Longrightarrow a+u=0$.
(9) $(a+u=0 \wedge a+v=0) \Longrightarrow a+v=0$.
(10) $a+u=0$.
(11) $a+v=0$.
(12) $v+0=v$
(13) $v+(a+u)=v$
(14) $(\forall y)(\forall z)\Big(v+(y+z)=(v+y)+z\Big)$.
(15) $(\forall z)\Big(v+(a+z)=(v+a)+z\Big)$.
(16) $v+(a+u)=(v+a)+u$.
(17) $(\forall y)\Big(v+y=y+v\Big)$.
(18) $v+a=a+v$.
(19) $v+(a+u)=(a+v)+u$.
(20) $v+(a+u)=0+u$.
(21) $(\forall y)\Big(0+y=y+0\Big)$.
(22) $0+u=u+0$.
(23) $v+(a+u)=u+0$.
(24) $u+0=u$.
(25) $v+(a+u)=u$.
(26) $u=v$.
(27) $(a+u=0 \wedge a+v=0) \Longrightarrow u=v$.
(28) $(\forall z)(a+u=0 \wedge a+z=0) \Longrightarrow u=z$.
(29) $(\forall y)(\forall z)(a+y=0 \wedge a+z=0) \Longrightarrow y=z$.
(30) $(\forall x)(\forall y)(\forall z)(x+y=0 \wedge x+z=0) \Longrightarrow y=z$.

Q.E.D.

PROBLEM 6: provide the missing justifications for the steps in the preceding proof.

SET AXIOMS

SET AXIOM 1: If S, T are sets, then

$$S = T \iff (\forall x)(x \in S \iff x \in T)\,.$$

SET AXIOM 2: If S is a set and $p(x)$ is any formula containing the variable x, no quantifiers involving x, and no other free variable, then $\{x : x \in S \wedge p(x)\}$ (that is, $\{x \in S : p(x)\}$) is a set.

SET AXIOM 3: If $p(x)$ is any formula containing the variable x, and no quantifiers involving x, and $p(x)$ does not contain the variable y, then

$$(\forall y)(y \in \{x : p(x)\} \iff p(y))\,.$$

THE RUSSELL PARADOX. Set Axiom 2 should look strange to you. It says that if you have a set S, then you can form subsets of S by considering, for example, the set of all $x \in S$ that satisfy some property $p(x)$. It would be much nicer if we could just state a much simpler axiom as follows:

SET AXIOM 2': If $p(x)$ is any formula containing the variable x, no quantifiers involving x, and no other free variable, then $\{x : p(x)\}$ is a set.

Unfortunately, this is bad. Betrand Russell discovered that if you accept an axiom such as Set Axiom 2', then you can prove a contradiction. And, as you know, if you can prove one contradiction then you can prove everything, including things that are false, so proving theorems becomes useless.

Here is Russell's argument:

> Suppose Set Axiom 2' was valid. Form the set
>
> $$S = \{x : x \notin x\}\,.$$
>
> Does S belong to S or not? If $S \in S$ then S must be one of the x's that satisfy the condition defining S, namely, $x \notin x$. So $S \notin S$. If $S \notin S$ then S is one of the x's that satisfy the condition defining S, namely, $x \notin x$, so $S \in S$. So we have proved $S \in S \iff S \notin S$, which is a contradiction. (Using our axioms, we can say this more neatly: let $S = \{x : x \notin x\}$. Use Set Axiom 3, specializing to $y = S$, with $p(x)$ being $x \notin x$. Then $S \in \{x : x \notin x\} \iff S \notin S$. By Rule 8, since $\{x : x \notin x\} = S$, we get $S \in S \iff S \notin S$.)