MATHEMATICS 300 — SPRING 1997

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 10. March 13, 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 a statement, your opponent is not convinced, and it is up to you to provide a convincing argument by giving a proof.

The trouble with all this is that it is not very clear what counts 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? (For example, suppose that at some point you use the fact that "two things equal to a third thing are equal to each other," that is, that if $x = z$ and $y = z$ then $x = y$. Suppose your opponent says "I don't see why that should be true." What do you do? How do you *convince* your opponent that this fact *is* true? If you think it over for a minute, you should persuade yourself that, 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 "what is the justification for that step?"

So you should think of giving formal proofs as similar to playing a game such as chess: you are given very rigid, 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.

FORMAL PROOFS

A *theorem* has one or several *assumptions* (or *hypotheses*, or *premises*), 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 either

(a) an *axiom* (or "postulate"),
(b) a *definition*,
(c) one of the *hypotheses*,
(d) something that was proved before,
(e) something that follows from previous steps by applying a valid *rule of inference.*

You should think of giving formal proofs of theorems as a game similar to chess:

1. You have to obey very strict rules telling you which moves are permitted. Each move has to be justified by explaining exactly which rule you are using and how you are using it.
2. On the other hand, if all you know is the rules, then that is not enough to tell you how to win. If you want to win (that is, if you want to get to the conclusion) then you have to **think**, plan a strategy, make a move now because it will put a piece in a position that will make it useful later, etc.

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:

$$\frac{\begin{array}{r}\text{All men are mortal}\\ \text{Socrates is a man}\end{array}}{\text{Socrates is mortal}} \tag{1}$$

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

$$\frac{\begin{array}{r}\text{All men are immortal}\\ \text{Socrates is a man}\end{array}}{\text{Socrates is immortal}} \tag{2}$$

or

$$\frac{\begin{array}{r}\text{All men are mortal}\\ \text{Donald Duck is a man}\end{array}}{\text{Donald Duck is mortal}} \tag{3}$$

or

$$\frac{\begin{array}{r}\text{All borogoves are mimsy}\\ \text{The Mad Hatter is a borogove}\end{array}}{\text{The Mad Hatter is mimsy}} \tag{4}$$

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,*

$$\frac{\begin{array}{r}\text{All } X \text{ are } Y\\ Z \text{ is an } X\end{array}}{Z \text{ is a } Y} \tag{5}$$

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:

$$\frac{\begin{array}{r} X \text{ is } Z \\ Y \text{ is } Z \end{array}}{X \text{ and } Y \text{ are } Z} \tag{6}$$

Examples of inferences of the form (6) are:

$$\frac{\begin{array}{r} \text{John is happy} \\ \text{Mary is happy} \end{array}}{\text{John and Mary are happy}} \tag{7}$$

and

$$\frac{\begin{array}{r} \text{My mother is smart} \\ \text{My father is smart} \end{array}}{\text{My mother and my father are smart}} \tag{8}$$

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

$$\frac{\begin{array}{r} \text{All men are equal} \\ \text{Socrates is a man} \end{array}}{\text{Socrates is equal}} \tag{9}$$

and

$$\frac{\begin{array}{r} \text{Bob Dole is married} \\ \text{Hillary Clinton is married} \end{array}}{\text{Bob Dole and Hillary Clinton are married}} \tag{10}$$

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

$$\frac{\begin{array}{r} (\forall x)(p(x) \to q(x)) \\ p(a) \end{array}}{q(a)} \tag{11}$$

(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 $(\forall x)(\forall y)((M(x)\wedge M(y))\rightarrow E(x,y))$ 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.

BASIC INFERENCE RULES FOR PROOFS

In the predicate calculus there are expressions that are names of "things" and expressions that —when we plug in values for the variables— are sentences or statements. The former are called **terms** and the latter are called **formulas.** 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:

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

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.

Now, here are the eight basic rules of inference that you are allowed to use in a formal proof.

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

RULE 2. If you have p and $p\rightarrow q$ 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 $p\rightarrow q$.

RULE 4. If you have a formula $(\forall x)p(x)$ and s is any term, then you can go to $p(s)$, **provided** that

(R) *the term s does not contain any variable that appears in $(\forall x)p(x)$ under the scope of a quantifier.*

This rule is called *specialization.*

REMARK. Why do we insist on the restriction (R)? Here is an example of what could happen if we did not make this requirement.

If the universe of discourse is the set **R** of real numbers, then we know that the formula $(\forall x)(\exists y)(\sim x = y)$ is true. Suppose we were allowed to apply the specialization rule indiscriminately, without demanding that condition (R) be met. Then:

> Our formula is of the form $(\forall x)p(x)$, where $p(x)$ stands for $(\exists y)(\sim x = y)$. Let s be the term y. Specialization would then yield: $(\exists y)(\sim y = y)$. But this is **false!** So we have been able to go from the true formula $(\forall x)(\exists y)(\sim x = y)$ to the false formula $(\exists y)(\sim y = y)$. So the "specialization rule," without the extra restriction (R), would allow us to go from a true statement to a false one, and this is the one thing that a valid rule of inference should **not** do.

RULE 5. To prove a statement of the form $(\forall x)p(x)$, you start by saying "Let a be arbitrary," and then try to prove $p(a)$. (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 **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.) If you do that, that is, if you can prove $p(a)$ for an arbitrary object a, then you can go to $(\forall x)p(x)$.

RULE 6. If you have $(\exists x)p(x)$ 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 $p(a)$. (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 $p(\text{the killer})$. 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 $p(\text{Hamlet})$, i.e. that Hamlet killed Polonius, or that $p(\text{Laertes})$, 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.)

RULE 7. If you have an object a such that $p(a)$, then 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 everywhere, and from a statement involving b to the statement in which a is substituted for b everywhere. (Example: 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 $0 \leq a \leq 1$.)

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 $(\forall x)(p(x) \rightarrow q(x))$ and $p(a)$ to $q(a)$. (For example, you want to deduce the conclusion that "Socrates is mortal" from the premises "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 premises are precisely $(\forall x)(p(x) \rightarrow q(x))$ and $p(a)$, and what you want to get is $q(a)$.) Then you could do it as follows:

(1) $(\forall x)(p(x) \rightarrow q(x))$ (hypothesis);
(2) $p(a)$ (hypothesis);
(3) $p(a) \rightarrow q(a)$ (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 $(\forall x)(p(x) \rightarrow q(x))$ 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: 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 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: $p \wedge q \rightarrow p$ 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 $p \wedge q \rightarrow p$ you get p by Modus Ponens (Rule 2).

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

JUSTIFICATION: $(p \wedge q) \rightarrow q$ 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 $(p \wedge q) \rightarrow q$ 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: $p \rightarrow (q \rightarrow (p \wedge q))$ 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 $p \rightarrow (q \rightarrow (p \wedge q))$ you get $q \rightarrow (p \wedge q)$ by Modus Ponens (Rule 2), and then from q and $q \rightarrow (p \wedge q)$ you get $p \wedge q$.

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

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

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

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

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

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

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

JUSTIFICATION: $(p \leftrightarrow q) \to (q \to p)$ is a tautology, so you can bring it in any time you want. If in addition you have $p \leftrightarrow q$, then from $p \leftrightarrow q$ and $(p \leftrightarrow q) \to (q \to p)$ you get $q \to p$ 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 $\sim q \to c$ by Rule 3. Now, if c is a contradiction, then $(\sim q \to c) \to q$ is a tautology (why?), so you can bring it in. Since you have $\sim q \to c$, then from $\sim q \to c$ and $(\sim q \to c) \to q$ you get q by Modus Ponens (Rule 2).

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

JUSTIFICATION: $(\sim p) \to ((p \vee q) \to q)$ is a tautology, so you can bring it in any time you want. If in addition you have $\sim p$, then you get $(p \vee q) \to q$ 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: $(\sim q) \to ((p \vee q) \to p)$ is a tautology, so you can bring it in any time you want. If in addition you have $\sim q$, then you get $(p \vee q) \to p$ 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 $p \to q$.

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 $p \to q$.

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

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

JUSTIFICATION: $(p \to q) \to ((q \to p) \to (p \leftrightarrow q))$ is a tautology, so you can bring it in any time you want. If you can prove q assuming p, then you get $p \to q$ by Rule 3. But then from $p \to q$ and $(p \to q) \to ((q \to p) \to (p \leftrightarrow q))$ you get $(q \to p) \to (p \leftrightarrow q)$ by Modus Ponens (Rule 2). If you can also prove p assuming q, then you get $q \to p$ by Rule 3. But then from $q \to p$ and $(q \to p) \to (p \leftrightarrow q)$ you get $p \leftrightarrow q$ 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 $(\forall x)(x \in S \to p(x))$. If you have $(\forall x)(x \in S \to p(x))$, then by specialization (Rule 4) you can get $s \in S \to p(s)$. 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 $(\forall x)(x \in S \to p(x))$. 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 $a \in S \to p(a)$ by Rule 3. So by Rule 5 you have proved that $(\forall x)(x \in S \to p(x))$, 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.

SOME EXAMPLES OF THINGS YOU **CANNOT** DO

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

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

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 COULD BE 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 80 years old" and "some people are 5 years old," does it follow that there is a person that is **both** 80 and 5 years old? 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 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 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 21. 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. In Problem 15, Page 102, of our textbook, we are told that, if $q(x)$ is a predicate over a domain of discourse U and r is a proposition, then

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

and

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

are theorems of the predicate calculus. The book does not tell you how you prove them. Let us see how you can prove these two things using our rules.

PROOF OF (I), WITH SHORTCUTS:

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

Q.E.D.

PROOF OF (II), WITH SHORTCUTS:

(1) Assume $(\forall x)\Big(r \vee q(x)\Big)$.

(2) Assume $\sim r$.

(3) Let a be arbitrary.

(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 $r \vee (\forall x)q(x)$.

(9) Assume $\sim r$.

(10) $(\forall x)q(x)$. (Derived Rule 11, from (8) and (9))

(11) Let a be arbitrary.

(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.

(16) Let a be arbitrary.

(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, bec. we proved $(\forall x)(r \vee q(x))$ assuming $\sim r$ and also assuming r)

Now let us write A for $(\forall x)(r \vee q(x))$, B for $r \vee (\forall x)q(x)$.

(20) $A \leftrightarrow B$. (Derived Rule 16, bec. 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 $A \leftrightarrow B$, 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 $A \leftrightarrow B$, 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 $(\exists x)\Big(r \wedge q(x)\Big)$.

(2) Let a be such that $r \wedge q(a)$. (Rule 6, from (1))

(3) $(r \wedge q(a)) \to r$ (Rule 1; instance of the tautology $(\alpha \wedge \beta) \to \alpha$)

(4) $(r \wedge q(a)) \to q(a)$ (Rule 1; instance of the tautology $(\alpha \wedge \beta) \to \beta$)

(5) r. (Rule 2, from (2) and (3))

(6) $q(a)$. (Rule 2, from (2) and (4))

(7) $(\exists x)q(x)$. (Rule 7, since $q(a)$)

(8) $r \to \Big((\exists x)q(x) \to \Big(r \wedge (\exists x)q(x)\Big)\Big)$. (Rule 1; tautology $\alpha \to (\beta \to (\alpha \wedge \beta))$)

(9) $(\exists x)q(x) \to \Big(r \wedge (\exists x)q(x)\Big)$. (Rule 2, from (5) and (8))

(10) $r \wedge (\exists x)q(x)$. (Rule 2, from (7) and (9))

(11) $(\exists x)\Big(r \wedge q(x)\Big) \to \Big(r \wedge (\exists x)q(x)\Big)$. (Rule 3, because we have proved $r \wedge (\exists x)q(x)$ assuming $(\exists x)\Big(r \wedge q(x)\Big)$)

(12) Assume $r \wedge (\exists x)q(x)$.

(13) $\Big(r \wedge (\exists x)q(x)\Big) \to r$. (Rule 1; instance of the tautology $(\alpha \wedge \beta) \to \alpha$)

(14) $\Big(r \wedge (\exists x)q(x)\Big) \to (\exists x)q(x)$. (Rule 1; instance of the tautology $(\alpha \wedge \beta) \to \beta$)

(15) r. (Rule 2, from (12) and (13))

(16) $(\exists x)q(x)$. (Rule 2, from (12) and (14))

(17) Let a be such that $q(a)$. (Rule 6, from (16))

(18) $r \to (q(a) \to (r \wedge q(a)))$. (Rule 1; instance of the tautology $\alpha \to (\beta \to (\alpha \wedge \beta))$)

(19) $q(a) \to (r \wedge q(a))$. (Rule 2, from (15) and (18))

(20) $r \wedge q(a)$. (Rule 2, from (17) and (19))

(21) $(\exists x)(r \wedge q(x))$. (Rule 7, because $r \wedge q(a)$)

(22) $\Big(r \wedge (\exists x)q(x)\Big) \to (\exists x)\Big(r \wedge q(x)\Big)$. (Rule 3, 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 $r \wedge (\exists x)q(x)$.

(23) $(A \to B) \to ((B \to A) \to (A \leftrightarrow B))$. (tautology)

(24) $(B \to A) \to (A \leftrightarrow B)$. (Rule 2, from (11) —which says $A \to B$— and (23))

(25) $A \leftrightarrow B$. (Rule 2, from (22) —which says $B \to A$— and (24))

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

$$(\forall x)(p(x) \vee q(x)) \leftrightarrow ((\forall x)p(x) \vee (\forall x)q(x)).$$

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

$$\Big(\sim (\forall x)p(x)\Big) \leftrightarrow (\exists x)(\sim p(x)).$$

.

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

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

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

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

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.)

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. $(\forall x)(\forall y)(x = y \rightarrow y = x)$.

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

Let us prove, using these axioms, the following

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

PROOF (WITH 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:

$$(\forall x)(\forall y)(\forall z)((x+y=0 \wedge x+z=0) \to y=z)\,. \tag{@}$$

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) $(a+u=0 \wedge a+v=0) \to a+u=0$.

(9) $(a+u=0 \wedge a+v=0) \to a+v=0$.

(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) $(a+u=0 \wedge a+v=0) \to u=v$.

(28) $(\forall z)(a+u=0 \wedge a+z=0) \to u=z$.

(29) $(\forall y)(\forall z)(a+y=0 \wedge a+z=0) \to y=z$.

(30) $(\forall x)(\forall y)(\forall z)(x+y=0 \wedge x+z=0) \to y=z$.

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

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

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

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

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 $S \in S \leftrightarrow S \notin S$, 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 $S \in \{x : x \notin x\} \leftrightarrow S \notin S$. By Rule 8, since $\{x : x \notin x\} = S$, we get $S \in S \leftrightarrow S \notin S$.)

THE AXIOMS OF ARITHMETIC

These axioms deal with the set $\mathbf{R}$ of real numbers, the subset $\mathcal{P}$ of $\mathbf{R}$ consisting of all positive numbers, the operations of addition and multiplication, and the numbers 0 and 1.

A0. $\mathbf{R}$ is a set, $\mathcal{P}$ is a subset of $\mathbf{R}$, $0 \in \mathbf{R}$ and $1 \in \mathbf{R}$.

A1. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(x + y \in \mathbf{R})$.

A2. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(x.y \in \mathbf{R})$.

A3. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(x + y = y + x)$.

A4. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(x.y = y.x)$.

A5. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(\forall z \in \mathbf{R})\Big((x + y) + z = x + (y + z)\Big)$.

A6. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(\forall z \in \mathbf{R})\Big((x.y).z = x.(y.z)\Big)$.

A7. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(\forall z \in \mathbf{R})\Big((x + y).z = x.z + y.z\Big)$.

A8. $(\forall x \in \mathbf{R})(0 + x = x)$.

A9. $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(x + y = 0)$.

A10. $(\forall x \in \mathbf{R})(1.x = x)$.

A11. $(\forall x \in \mathbf{R})\Big(x \neq 0 \rightarrow (\exists y \in \mathbf{R})(y.x = 1)\Big)$.

A12. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})\Big((x \in \mathcal{P} \wedge y \in \mathcal{P}) \rightarrow x + y \in \mathcal{P}\Big)$.

A13. $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})\Big((x \in \mathcal{P} \wedge y \in \mathcal{P}) \rightarrow x.y \in \mathcal{P}\Big)$.

A14. $(\forall x \in \mathbf{R})(x \in \mathcal{P} \vee x = 0 \vee (\forall y \in \mathbf{R})(y + x = 0 \rightarrow y \in \mathcal{P}))$.

A15. $0 \notin \mathcal{P}$.

A16. $1 \neq 0$.

COMMENTS: These axioms are essentially the same as those given in the book, Pages 288 and 296. Using the terminology of the book, the axioms say that $\mathbf{R}$ is an *ordered field.*
Axioms A1 and A2 are *closure properties.* They say that the sum and the product of two real numbers is a real number, that is, that the set of real numbers is closed under the operations of addition and multiplication, in the sense that applying these operations to things in the set always results in things in the set.
Axioms A3 and A4 are the *commutative laws* of addition and multiplication.
Axioms A5 and A6 are the *associative laws* of addition and multiplication.
Axiom A7 is the *distributive law* of multiplication with respect to addition.
Axiom A8 says that 0 is an additive identity, that is, that adding 0 to any number leaves the number unchanged.
Axiom A9 says that every real number has an additive inverse.
Axiom A10 says that 1 is a mutiplicative identity, that is, that mutiplying any number by 1 leaves the number unchanged.
Axiom A11 says that every nonzero real number has a multiplicative inverse.
Axiom A12 says that the sum of two positive numbers is positive.
Axiom A13 says that the product of two positive numbers is positive.
Axioms A14 says that every number x is either positive, negative, or zero. We say it in a roundabout way because we have not yet defined "negative number." Instead of saying "x is negative," we say "$(\forall y)(y + x = 0 \rightarrow y \in \mathcal{P})$."
Axiom A15 says that 0 is not positive.
Finally, Axiom A16 says that 0 and 1 are different. If you do not believe that A16 is necessary, take a look at the other axioms. Notice that they would all be satisfied if $\mathbf{R}$ consisted of just 0 and nothing else, and 1 was equal to 0. So unless we put in Axiom A16 we will never be able to prove that $1 \neq 0$.

QUESTION: what would have happened if we had stated Axiom 11 by saying instead: $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(y.x = 1)$? (ANSWER: it would follow from this that $0 = 1$ and that $(\forall x \in \mathbf{R})(\forall y \in \mathbf{R})(x = y)$, that is, that all real numbers are equal. EXERCISE: prove this. HINT: prove first that $(\forall z)(z.0 = 0)$. To do this, use $0 + 0 = 0$ —Axiom A8— together with A4 and A7 to conclude that $z.0 + z.0 = z.0$, and then hit both sides with an additive inverse of $z.0$ using Axiom A9.)

HARD QUESTION: Consider the following statement:

(#) Every interval is of one of the nine types listed in Definition 3 of Page 8 of the textbook.

Do you think it will be possible to prove (#) using the above axioms?

NOTE: the definition of "interval" is given in Page 8 of the textbook. Here it is, again:

DEFINITION OF INTERVAL : A subset I of $\mathbf{R}$ is an *interval* if

$$(\forall x \in I)(\forall y \in I)(\forall z \in \mathbf{R})(x < z < y \rightarrow z \in I).$$