MATHEMATICS 300 — FALL 1998

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 10. October 28, 1998

Revised November 2, 1998. Second revision: November 22, 1998.

HOMEWORK ASSIGNMENT NO. 7, DUE ON WEDNESDAY, NOVEMBER 4

1. Problems 13, 14 and 16 in pages 72-73, nonstarred parts only.
2. Do problem 12 of page 72 using the rules of Handout 10, the definitions of $\subseteq$, $\cup$, $\cap$, $\emptyset$ and $=$ (given in the book) **and nothing else**.
3. Prove or disprove: the product of 5 consecutive natural numbers is always divisible by 120.

THE STRUCTURE OF A PROOF

A **formal proof** is going to be a sequence of **steps**. Each step consists of a **statement**, accompanied by a **justification**. The justification of a step consists of showing that it is permitted by the rules, given the previous steps.

Let us recall that a **statement** is a **closed formula**. This means that a statement cannot have open variables. For example, $\diamond + 3 = 7$ is **not** a statement if $\diamond$ is a letter such as x, which is considered a **variable**. If, on the other hand, $\diamond$ is a letter such as a, thought of as a **constant**, then $\diamond + 3 = 7$ **is** a statement, but in that case the letter—say "a"— must have been introduced as such.

CONSTANTS MUST BE PROPERLY INTRODUCED

There will be exactly three ways to introduce a symbol such as the letter a as a constant:

(C.1) a could be a **reserved constant**, that is a special symbol fixed once and for all to denote a particular object. For example, in real-number arithmetic 0, 1, 2, π, e, are resreved constants. In set theory, $\emptyset$ is a reserved constant.

(C.2) a could be an "arbitrary object." For example, the letter a could be introduced as a constant by saying "Let a be arbitrary."

(C.3) a could be an "object that has a particular property." For example, we could say "Let a be such that $a.3 = 7$." From that moment on, we can freely use the fact that $a.3 = 7$.

REMARK: Actually, (C.2) is not really that different from (C.3), if you think about it for a minute. You can think of "Let a be arbitrary" as a way of saying "Let a be such that $a = a$." So, really, we could have dispensed with (C.2) altogether, and just used (C.3).

In practice, any letter can be used as a constant or as a variable. We can say things like

$$(\forall a)(\forall b)((a + b)^2 = a^2 + 2a.b + b^2)\,,$$

in which a and b are clearly variables. Also, we can use x or y as constants, if we wish. For example, we can say "Let $x = 4$," or "Let x be arbitrary," and if we do that then we are starting a "proof within a proof" (see below) within which x will play the role of a constant.

To make things even more confusing (sorry!), we often use the same letter in both capacities, in the same proof. For example, suppose I want to prove

$$(\forall \varepsilon)(\varepsilon > 0 \Longrightarrow (\exists \delta)(0 < \delta \wedge \delta < \varepsilon))\,. \qquad (\%)$$

(In other words, I want to prove that "for every positive number there is another positive number which is smaller.")

Then I could write

(1.&)	Let ε be arbitrary.
(2.&.&)	Assume that $\varepsilon > 0$.
(3.&.&.&)	Let $\delta = \frac{\varepsilon}{2}$.
(4.&.&.&)	$0 < \delta \wedge \delta < \varepsilon$.
(5.&.&)	$(\exists\delta)(0 < \delta \wedge \delta < \varepsilon)$.
(6.&)	$\varepsilon > 0 \Longrightarrow (\exists\delta)(0 < \delta \wedge \delta < \varepsilon)$.
(7)	$(\forall\varepsilon)(\varepsilon > 0 \Longrightarrow (\exists\delta)(0 < \delta \wedge \delta < \varepsilon))$. QED

In this proof, in the first line I am introducing a new **constant**, but I am perversely calling it ε, exactly like the variable ε that occurs in Formula (%). When I do so, I start a subproof (or "proof within a proof"), and I indicate this by using an extra "&", so the first line is (1.&), meaning that this is step 1 and we are in a subproof, on level 2, one level down from the top level. Then in the second line I go even deeper to a "sub-subproof", or "proof within the subproof," by introducing an assumption. I indicate this by using another "&", so the second line is (2.&.&), meaning "step 2, and we are in level 3, that is, in a sub-subproof.". Finally, in the third line I go even deeper to a "sub-sub-subproof", or "proof within the proof within the proof within the proof," by introducing a constant δ that satisfies a condition. I indicate this by using a third "&", so the third line is (3.&.&&), meaning "step 3 and we are in level 4, that is, in sub-sub-subproof.". Moreover, I am being perverse here too, and I am using the letter δ, which is a variable in (%), as a constant in the level 4 sub-sub-subproof.

Now in (4)) I have established that, in the expression $0 < \square \wedge \square < \varepsilon$, there is something I can put in the box to make the resulting statement true. So I make this statement ("the box in $0 < \square \wedge \square < \varepsilon$ can be filled with something that makes the statement true") which, as you can see, does not contain the constant δ anywhere. One of my eight inference rules (Rule 7, see below) tells me that, since I have proved something not involving δ, I can go up one level. But then, perversely, I use the variable δ to denote the "box," so I end up with (5). This is in level 3, right underneath "Assume that $\varepsilon > 0$." In other words, this has been proved "under[1] the assumption that $\varepsilon > 0$." So one of my rules will tell me that I can go up one level and assert (6). Now, finally, (6) is "under" the condition that "ε is arbitrary." In other words, I have shown that, if I put a completely arbitrary ε in the box, in the expression

$$\square > 0 \Longrightarrow (\exists\delta)(0 < \delta \wedge \delta < \square),$$

then what I get is true. So I use one my rules, and conclude that I can go to the statement

$$\text{No matter what you put in the box,} \quad \square > 0 \Longrightarrow (\exists\delta)(0 < \delta \wedge \delta < \square) \quad \text{is true}, \qquad (@)$$

in the next higher level. Moreover, I act perversely once again, and use the variable ε for the thing one can put in the box, so I end up with (7). That is, I have landed in the top level and with the statement to be proved. This is exactly where I wanted to end up, so at this point I declare victory, and write **QED**, which is the fancy way to say "This is the end of the proof," using the Latin phrase "quod erat demonstrandum" (which means "which is what was to be proved").

If you think this is too messy because of the fact that the same letters are used sometimes as constants and sometimes as variables, you might find it easier never to do that. In other words, you could choose to use different symbols for constants and for variables. Then the previous proof would look like this:

[1] The word "under" is meant quite literally here!

(1.&)	Let $\bar{\varepsilon}$ be arbitrary.	
(2.&.&)	Assume that $\bar{\varepsilon} > 0$.	
(3.&.&.&)	Let $\bar{\delta} = \frac{\bar{\varepsilon}}{2}$.	
(4.&.&.&)	$0 < \bar{\delta} \wedge \bar{\delta} < \bar{\varepsilon}$.	
(5.&.&)	$(\exists\delta)(0 < \delta \wedge \delta < \bar{\varepsilon})$.	
(6.&)	$\bar{\varepsilon} > 0 \Longrightarrow (\exists\delta)(0 < \delta \wedge \delta < \bar{\varepsilon})$.	
(7)	$(\forall\varepsilon)(\varepsilon > 0 \Longrightarrow (\exists\delta)(0 < \delta \wedge \delta < \varepsilon))$.	QED

In this proof, $\bar{\varepsilon}$ and $\bar{\delta}$ are constants, ε and δ are variables, and no confusion is possible.

CONSTANTS CAN ONLY NAME THINGS THAT EXIST

In the previous box, (C.3) looks like a very nice method for introducing a constant. You can take any conditions you want, and introduce an object that satisfies them. For example, you can say:

(...) Let a be the person who killed Polonius,

or

(...) Let a be a solution of the equation $x^5 + 6x^4 - 3x + 8 = 0$.

The catch is: **you cannot introduce something if you don't know it exists.** For example, you cannnot introduce a constant a with "Let a be such that $a.0 = 1$." (Once we state our axioms for the real numbers, we will be able to prove from them that $(\forall x)(x.0 = 0)$. If we could introduce a constant a such that $a.0 = 1$, then you could plug a into $x.0 = 0$—because $x.0 = 0$ is true for all x, so in particular is true for a; this is called "specialization"—and get $a.0 = 0$. But, since you also have $a.0 = 1$, you would end up with $0 = 1$. Since there also is an axiom saying that $\sim 0 = 1$, it will turn out that you have proved

$$0 = 1 \wedge (\sim 0 = 1)\,,$$

which is a **CONTRADICTION**. And once you have one contradiction, then it's a complete catastrophe! (See the next box.))

WHY IS A CONTRADICTION DISASTROUS?

Suppose you could prove a contradiction C. Take any statement S you want. Then $C \Longrightarrow S$ is an instance of a tautology, because $C \Longrightarrow S$ always has the truth value T, since C always has the truth value F.
So **once you have proved one contradiction you can prove any statement you want, whether or not it is true.**

CONSISTENCY

A mathematical theory where a contradiction can be proved is said to be **inconsistent**. A theory which is not inconsistent is said to be **consistent.**
As we saw in a previous box, **with an inconsistent theory you can prove every statement.** So you can prove things that are false as well as things that are true. Therefore the whole notion of "proof" and "provability" becomes useless. In a good theory you should not be able to prove false things. Otherwise, the fact that you have proved something will not tell you that it is true, and then the whole point of having proved it would be lost.

THE PEANO PARADOX

THEOREM: 1 is the largest natural number.

PROOF: Let n be the largest natural number. Then n^2 is a natural number too. Since n was the largest natural number, $n^2 \leq n$. On the other hand, $n \geq 1$, so $n^2 = n.n \geq n.1 = n$. So $n^2 \leq n$ and $n^2 \geq n$. Therefore $n^2 = n$. The only solutions x of $x^2 = x$ are $x = 1$ and $x = 0$. So $n = 1$ or $n = 0$. But 0 is not a natural number, so n cannot be 0. Therefore n has to be equal to 1. **QED**

QUESTION: What is wrong with the above proof? (*Something* must be wrong! You don't really believe that 1 is the largest natural number, do you?)

When we write a truly formal proof, it is a good idea to **number the steps**, so that every time you use some previous steps to justify a new step, you can refere to them by number.

For example, one of our rules (called $\boxed{\text{Modus Ponens}}$) 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 have just finished step 94. Suppose that earlier on, in the 25th step, you had the following

(25) $3 > 0$. (.....................)

and in the 47th step you had

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

Then you are permitted to add a new Step 95 to your proof, by saying:

(95) $(\exists x)(x^2 = 3)$. (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. There will be **three** such kinds of steps: we will always be permitted to bring in an **axiom** as a new step, or a **definition**, or one of the **hypotheses**.

In addition, one of our rules (Rule 1, to be precise) will tell us that you are always allowed to bring in an $\boxed{\text{instance of a tautology}}$. For example, suppose that at some point of a proof you have

(238) $3 > 0 \vee 3 < 0$. (.....................)

and then later you managed to get

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

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

AXIOMS

Axioms are statements that we accept as true. They are the starting points of any mathematical reasoning.
Mathematicians like to have the smallest possible number of axioms. If something can be **proved** from other axioms, then it is not nice to add it as an axiom. But **some** axioms are necessary to get started. Otherwise, you cannot move anywhere.
You should think of axioms as being similar to the starting positions of a game such as chess. The steps of a proof are like **moves**, and the theorems one proves are like the positions that one can attain from the starting position by making various moves.

DEFINITIONS

Definitions function very much like axioms, so much so that often it does not make any difference whether you call something an "axiom" or a "definition."
For example, later on, when we introudce axioms for the real number system, we will have at some point the following "axiom-definition":

$$(\forall x)(\forall y)(\forall z)(x - y = z \Longleftrightarrow y + z = x)\,. \qquad (SUB)$$

Is this an "axiom"? Is it a "definition"? Or maybe it does not matter?
Let us see. You might, for example, have started with a language for the real numbers in which the given symbols include $+$ and $=$ but not $-$. In such a case, "we don't have the $-$ symbol" to begin with, and we have to introduce it. We do so by means of Formula (SUB). So this formula tells us what "$-$" means. Then (SUB) is the **definition** of $-$. Once we have this formula, every time we have a statement involving "$-$," we can **eliminate** the $-$ symbol altogether. (We will do that many times later.)
Another point of view is possible. We might have started with a language for the real numbers in which the given symbols include $+$ and $=$ and also $-$. So in this case "we do have the $-$ symbol" from the very beginning, and there is no need to introduce it. But we still have to say something about how this symbol is related to all the others. So we take Formula (SUB) as an **axiom**. From this perspective, formula tells us an important fact about "$-$," but is not the definition.
The important thing is that, whether (SUB) is regarded as an axiom or as a definition, **it is a formula that we can bring in as a step into a proof any time we want.** This is what really matters about (SUB), and the question whether it "really" is an axiom or a definition is much less important.

HYPOTHESES

Hypotheses are statements that we **assume** to be true in a particular situation.
If you compare this with what we said about "axioms" in a previous box, you will see that the difference appears to be very slight. In fact, **within a particular proof, hypotheses function exactly like axioms and definitions: they are statements that you are free to bring in any time you want.**
There is, however, a big difference. Axioms are things that we take to be true forever, because we believe they are true. Hypotheses are taken to be true not because we believe they are true, but **because we want to know the consequences of their being true.** On other words: we might want to know what else would have to be the case, for example, if pigs had wings. So we make the hypotheses that "pigs have wings," by saying

(...) Assume pigs have wings,

and we then set out to explore its consequences. Or, if you prefer, we set out to study an imaginary world in which pigs have wings and try to understand what that world would have to be like. We could then "prove" all kind of "theorems," such as

THEOREM 1: *Pigs can fly.*

THEOREM 2: *If a pigsty does not have a roof, then the pigs will fly away.*

All these theorems would be proved **under the hypothesis** that pigs have wings. That is, we would never be saying that we have proved that pigs can fly. All we would be saying is that **IF** pigs had wings **THEN** pigs could fly. In other words, all the facts we would "prove" about pigs under the "pigs have wings" hypothesis would be valid **in the imaginary world of pigs with wings**, which, in principle, is not our real world.

ENTERING AND LEAVING IMAGINARY WORLDS

When you assume something, you are setting out to explore an **imaginary world**, namely, a world in which that thing you are assuming is true. When can you leave that world and go back to the real world, taking with you the things you have discovered in your imaginary world? The answer is simple: if the thing you assumed is actually true in the real world, then everything you proved **under that assumption** is true, because in that case the imaginary world really is the real world.
Our rules of inference will capture this very obvious idea as follows:

- You will be always be allowed to introduce anything you want as an asumption, any time you want.
- When you do that, whatever you have proved will have been proved **under your assumption**.
- If, assuming P, you prove some other statement Q, then you will be allowed to go back to "the real world" and assert there that $P \Longrightarrow Q$.
- If, in addition, you can prove P, then the Modus Ponens rule will allow you to go to Q.

In simpler terms: whatever you prove under the assumption P will be valid unrestrictedly (that is, without having to assume that you are under the assumption P) if you can also prove P.

PROOFS BY CONTRADICTION

One of the most common reasons for assuming something is to prove it cannot happen. In other words, you set out to explore the consequences of something in order to prove it is impossible. This is called "proof by contradiction." We have already seen examples before: when we proved by contradiction that $\sqrt{2}$ is irrational, we assumed that $\sqrt{2}$ was rational, and ended up with an impossible fact, namely, that a certain natural number would have to be both even and odd. That is, **we set out to explore an imaginary world in which $\sqrt{2}$ was rational, until we saw that in this world impossible things would happen, and then we concluded that such a world could not exist, so $\sqrt{2}$ has to be irrational.**
This should answer once and for all one of the most frequently asked students' questions: **How can I assume something if I don't know it is is true?** Or, even worse, **how can I assume something if I know it is not true?**
The answer is very simple: you assume something that you don't know to be true because you want to find out what would happen if it was true. And often you assume it **precisely in order to prove it is not true.**

THE THREE "PROPOSITIONAL" RULES

The first three of our eight rules will tell you

- that you can always bring in an instance of a tautology,
- that from P and $P \Longrightarrow Q$ you can go to Q (Modus Ponens),
- that, if assuming P you prove Q, then you can go to $P \Longrightarrow Q$.

Using these rules, you can justify formally all kinds of things we do in mathematical reasoning.

EXAMPLE 1. Suppose you have proved two statements, say P and Q, and now you want to get to the statement $P \wedge Q$. You just bring in the instance of tautology
$P \Longrightarrow (Q \Longrightarrow (P \wedge Q))$,
then use Modus Ponens once to conclude that
$Q \Longrightarrow (P \wedge Q)$,
and then use Modus Ponens again to conclude that $P \wedge Q$.

EXAMPLE 2. Suppose you have proved $P \wedge Q$ and now you want to get to P. You just bring in the instance of tautology
$(P \wedge Q) \Longrightarrow P$,
and then use Modus Ponens to get P.

EXAMPLE 3. (*Proof by contradiction.*) Suppose you are trying to prove P. You know that one way to do that is to assume $\sim P$ and get a contradiction. How is that justifed with our rules? It's very easy! Let us say that assuming $\sim P$ you get the contradiction C. By one of our propositional rules, you can now go to $(\sim P) \Longrightarrow C$. But then you bring in the instance of tautology $((\sim P) \Longrightarrow C) \Longrightarrow P$, and hit it with Modus Ponens (using $(\sim P) \Longrightarrow C$), and you get P, as desired.

(You may ask: why did I bring in this particular tautology here? The answer is "because it works!" How do I know it is a tautology? That's easy. If you want to, you can do it with truth tables, but you can also see it directly. Just ask yourself: could $((\sim P) \Longrightarrow C) \Longrightarrow P$ ever be F? This could only happen if $(\sim P) \Longrightarrow C$ is T and P is F. But then $\sim P$ would be T, and since $(\sim P) \Longrightarrow C$ is T it would follow that C is T. But this is out of the question because C is a contradiction.)

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 (6813.1))
(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 and a &** 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, assuming that your universe of discourse is $\mathbb{N}$, the set of natural numbers: $(\forall n)(2|n^2+n)$.) 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 $(\forall n)(2|n^2+n)$."

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 $(\forall n)(2|n^2+n)$. In our "proof within a proof," the letter k is treated as a constant.

We could organize this as follows (assuming, say, that we just wrote step 4289:

(4290.&)	Let k be arbitrary.	(Preparation to apply Rule 5)
	....	
	....	
	....	
(4365.&)	$(k \text{ is even}) \vee (k \text{ is odd})$.	(............)
(4366)	$(\forall n)\Big((n \text{ is even}) \vee (n \text{ is odd})\Big)$.	(Rule 5, from (4290) and (4365))

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

Finally, we are ready to give a truly precise definition of proof. A **proof** is a list of **statements**, each one accompanied by a **justification**.

We now list the conditions telling us when a step in a proof is valid:

> ## WHAT IS PERMITTED IN A PROOF?
>
> (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 a **definition** as a new step.
>
> (P.d) 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.e) It is always permitted to start a proof within a proof by either
>
> - introducing any statement you want as an assumption,
>
> or
>
> - bringing in a **new** letter as an arbitrary constant.
>
> or
>
> - bringing in a **new** letter assumed to satisfy some condition, provided it has been proved that something satsifying that condition exists.
>
> 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 or Rule 6.

Now, to wrap this up, I have to tell you what our **rules of inference** are. But, before I do that, I have to take care of an unpleasant and boring but important detail.

Suppose you have a formula such as $x+3 = 7-x$, and you call it $p(x)$. Suppose a is a constant. What do we mean by "$p(a)$"? Obviously, we mean "$a + 3 = 7 - a$," right? For example, $p(2)$ is the formula "$2 + 3 = 7 - 2$," so $p(2)$ is true. This suggests an obvious possibility:

(A) If $p(x)$ is a formula, and a is a constant, then by $p(a)$ we mean the formula obtained by substituting a for x wherever x occurs.

That sounds quite easy. Unfortunately, things are not so simple.

Suppose for example that $p(x)$ was the formula $x + 3 = 7 - x \wedge (\exists x)(x + 3 = 8)$. What exactly do we mean by "$p(a)$"? Perhaps we mean

$$a + 3 = 7 - a \wedge (\exists a)(a + 3 = 8) \ . \qquad (\#)$$

But this is ridiculous, because a is a constant, so we cannot say "$(\exists a)$." (For example, what on Earth would "$2 + 3 = 7 - 2 \wedge (\exists 2)(2 + 3 = 8)$" mean?)

So maybe $p(a)$ should be

$$a + 3 = 7 - a \wedge (\exists x)(a + 3 = 8) \ , \qquad (*)$$

or

$$a + 3 = 7 - a \wedge (\exists x)(x + 3 = 8) \ , \qquad (\&)$$

Actually, (&) is the most reasonable choice, because, as we said earlier, when we write the formula "$(\exists x)(x + 3 = 8)$" the variable x is "bound" (or "dummy"), which means that "$(\exists x)(x + 3 = 8)$" is "really the same" as "$(\exists y)(y + 3 = 8)$," so "there really is no x there."

But then, **if we want to adopt (&) as the correct meaning of $p(a)$ when $p(x)$ is "$x+3=7-x\wedge(\exists x)(x+3=8)$," then we can no longer take (A) to be correct, because (A) inexorably leads us to (#), which is nonsense.**

In order to avoid these problems, **we will limit our use of the substitution of a constant a for a variable x to formulas $p(x)$ where is no quantifier involving x anywhere.**

Now, finally, we are ready to list the rules. There are exactly **EIGHT** of them. Here they are.

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 p is any statement whatsoever, then you are allowed to start a subproof (i.e. to go to level $k+1$, if you are at level k, and start a "proof within a proof") by saying "Assume p." If in that subproof you get to a statement q (that is, if you prove q under the assumption p), then you can get out of the subproof and carry $p \Longrightarrow q$ to the level k proof.

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, you can go to $p(a)$. (This is called *specialization.*)

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 are allowed to start a subproof (i.e. to go to level $k+1$, if you are at level k, and start a "proof within a proof") by saying "Let a be arbitrary." This effectively declares a to be a constant, locally, within the "proof within a proof." If in this subproof you get to $p(a)$ (that is, if you prove q under the assumption that a is arbitrary), then you can get out of the subproof and carry $(\forall x)p(x)$ to the level k proof.
COMMENT: 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.

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. Suppose you already have $(\exists x)p(x)$. Then you are allowed to start a subproof (i.e. to go to level $k+1$, if you are at level k, and 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, locally, within the "proof within a proof." If in this subproof you get to a statement q that does *not* contain a, (that is, if you prove q under the assumption that a satisfies $p(a)$, but q itself does not contain a), then you can get out of the subproof and carry q to the level k proof.

COMMENT: 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.

If you want a more mathematical example: suppose you prove that $1+1$ exists (that is, you prove that $(\exists x)(1+1=x)$). Suppose then that you decide to introduce a constant as in our rule, but you make the stupid mistake of calling this constant 1. Then you would get $1+1=1$, and from that you can prove anything you want! So you will have introduced an **inconsistency** and destroyed all your previous work!

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 t and s are constant terms, and you have proved that $t=s$, then you can go from a statement involving t to the statement in which s is substituted for t in all or some of its ocurrences, and from a statement involving s to the statement in which t is substituted for s in all or some of its ocurrences.

EXAMPLES ILLUSTRATING THE USE OF RULE 8

1. If a and b are constants and you have proved $a=b$ and $a.c=a.c$, then 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 $a\in\{x:0\leq x\leq 1\}$, by substituting "$\{x:0\leq x\leq 1\}$" for "$[0,1]$" in "$a\in[0,1]$."
3. After you have given the definitions
$$2=1+1,$$
and
$$3=2+1,$$
you can go[2]

AN EXAMPLE

Suppose p is a two-variable predicate letter.

THEOREM: $(\exists y)(\forall x)p(x,y)\Longrightarrow(\forall x)(\exists y)p(x,y)$.

PROOF:

(1.&)	Assume $(\exists y)(\forall x)p(x,y)$.	[Preparation to apply Rule 3]
(2.&.&)	Let a be such that $(\forall x)p(x,a)$.	[Preparation to apply Rule 6, from (1.1)]
(3.&.&.&)	Let b be arbitrary.	[Preparation to apply Rule 5]
(4.&.&.&)	$p(b,a)$.	[Rule 4, from (2)]
(5.&.&.&)	$(\exists y)p(b,y)$.	[Rule 7, from (4)]
(6.&.&)	$(\forall x)(\exists y)p(x,y)$.	[Rule 5, from (5)]
(7.&)	$(\forall x)(\exists y)p(x,y)$.	[Rule 6, from (6)]
(8)	$(\exists y)(\forall x)p(x,y)\Longrightarrow(\forall x)(\exists y)p(x,y)$.	[Rule 3, from (1) and (7)]

QED

[2] A truly nitpicking student could (and should) object to this. Strictly speaking, when you substitute "$1+1$" for 2 in "$3=2+1$", what you get is "$3=1+1+1$", not "$3=(1+1)+1$." If you really want to get "$3=(1+1)+1$", then you should have used "$3=(2)+1$." This is one of many examples of the annoying complications created by the use of parentheses. The issue **cannot be ignored.** For example, if you were writing a computer program to check proofs, then the issue would come up: if you program Rule 8 into the computer carelessly, then the computer would not accept "$3=(1+1)+1$" as arising from the susbtitution of "$1+1$" for 2 in "$3=2+1$".

COMMENT: Can you prove the converse of the above theorem, that is

$$(\forall x)(\exists y)p(x,y) \Longrightarrow (\exists y)(\forall x)p(x,y) \ ?$$

If our rules are any good, then you should **not** be able to prove it, because you know that this is not logically valid. (If everybody eats something, it does **not** mean that there is something that's eaten by everybody!)

You should try to prove this, and see by yourself why you cannot do it.

Here is one possible attempt:

(1.&)	Assume $(\forall x)(\exists y)p(x,y)$.	
(2.&.&)	Let b be arbitrary.	
(3.&.&)	$(\exists y)p(b,y)$.	[Rule 4]
(4.&.&.&)	Let a be such that $p(b,a)$.	[Preparation to apply Rule 6, from (3)]

And now you are stuck! You are in level 4, and you entered it by introducing a. So the only way to get out and go back to level 3 would be to apply Rule 6. For that you need to prove something that does not involve a. You could, of course, go to $(\exists y)p(b,y)$. That would indeed get you out of level 4, but you would not have gained anything, because you already had $(\exists y)p(b,y)$ anyhow, in step (3). (This is called "going around in circles." It's not a very useful thing to do if you actually want to **get** somewhere!)

What else could you do? It would be nice if you could go to $(\forall x)p(x,a)$, because then you would apply Rule 7 and write $(\exists y)(\forall x)p(x,y)$, which is exactly what you want. But you **cannot** go to $(\forall x)p(x,a)$, because Rule 5 tells you that, if you start a subproof with "Let b be arbitrary" and then prove $q(b)$ **in the same level** then you can carry $(\forall x)q(x)$ to the previous level. Here you have proved $p(b,a)$ in level 4, whereas you introduced b as an arbitrary constant in level 3.

Notice that this restriction, that you cannot prove $q(b)$ in a deeper level and then use it in the higher level, is very much in agreement with common sense. To prove $(\forall x)q(x)$ you have to be able to prove $q(b)$ for a completely arbitrary b, that is, a b that could be absolutely anything. If you go to a deeper level, you will be introducing a new assumption, so b will no longer be completely arbitrary. (Example: let us prove that all real numbers are equal to 47. Proof: let a be arbitrary. Assume that $a = 47$. Then $a = 47$ and, since a was arbitrary, we can conclude that $(\forall x)(x = 47)$. Ridiculous, isn't it? QUESTION: how does this "proof" violate our rules?)

(to be continued)