MATHEMATICS 300 — SPRING 2000

Introduction to Mathematical Reasoning

H. J. Sussmann

HANDOUT NO. 4 — March 9, 2000

Revised March 20, 2000. 2nd. revision: March 27, 2000.

---

1. SOME CORRECTIONS

(With thanks to Nancy Rothman, Nick Bennette, and several other students who found mistakes in the previous versions.)

The March 9 version of this handout was incorrectly labeled "Handout No. 5." The correct number is 4.

Also: the March 9 version incorrectly asserted that the March 6 handout should have been number 4 rather than 3. The 3 was O.K. If you changed the 3 to a 4, please correct the number again.

---

2. READING FOR THE WEEK AFTER THE SPRING BREAK

For the week after the spring break, you should have read carefully Chapters 1,2,3,4 of the book, and handouts 1,2,3,4,5.

---

3. HOMEWORK DUE ON THURSDAY MARCH 23 (revised version)

1. Do all the problems in the midterm, in your own handwriting.
2. Copy all the rules for proofs in Chapter 4 of the book.
3. Write down the following:

   a. To prove an existential statement I can do it by exhibiting an example (that is, a "witness"). But to prove a universal statement I **cannot** do it by exhibiting an example; I need an **argument**. For example: suppose $h(x)$ stands for "x is wearing a hat." To prove $\exists x\, h(x)$ it suffices for me to point to someone who is wearing a hat. But to prove $\forall x\, h(x)$ I cannot do it by giving an example of a person wearing a hat. I need a **general argument.** In exactly the same way: the statement that some sentence is logically valid is a universal statement (for **all possible interpretations** ...); therefore, if I want to prove that a statement is law of logic I cannot do it by giving an example of an interpretation where the statement is true; I have to show that it is true for **all possible interpretations**, and that requires a general argument. But to prove that the statement is *not* a law of logic I have to show that there is *some* interpretation for which it is false, and that I can do by exhibiting a particular example of an interpretation.

b. If I want to translate a sentence involving certain free variables, then the translation should have the same free variables. For example, if I want to translate "x has a son" into the formal language of Problem 1 of the midterm, then the translation should have x as a free variable and nothing else; so something like $s(y, x)$ cannot possibly be a correct translation because it involves the free variable y which was not in the original statement. (A correct translation is "$\exists y\, s(y, x)$.")

c. If I am asked to translate a statement into a sentence involving certain symbols **and nothing else**, then what I should do is translate the statement into a sentence involving those symbols **and nothing else**.

NOTE: you are exempted from doing Problem 3 if you can show that in your midterm test you never violated the principles laid out in Problem 3. If you wish to avail yourself of that exemption, then hand in your test together with the homework.

4. For what natural numbers k is it true that "the sum of k consecutive natural numbers is always divisible by k"? (In case you don't see what I mean by this question, let me give you an example: if I ask you "for what natural numbers k is it true that k^2 is divisible by 3?", your answer should be "the numbers whose square is divisible by 3 are exactly the numbers that are themselves divisible by 3.") JUSTIFY YOUR ANSWER (that is, give a proof.)

5. For all the "translation" problems in the midterm, every time you translated something wrong, take the translation you gave and translate it back into the original language. (For example, if you were asked to translate "everybody has a son" from English to the formal language of Problem 1, and your translation was "$s(x, y)$", then when you translate back you get "x is y's son," which is not at all the same thing. If you were asked to translate $\forall x \exists y (y.y = x)$ from formal language to English, and you translated this as "x has a square root," then when you translate back you get $\exists y (y.y = x)$,which is not at all the same thing.)

6. Problems 11 and 12 in page 70 of the book.

7. Problems 6 and 10 in page 90.

8. Problems 9, 16, 17, 18 in pages 106, 107.

---

4. THE STRUCTURE OF A PROOF

Suppose we are given,

- a first order predicate calculus,
- a collection of closed formulas, called *axioms*,
- another collection of closed formulas called *definitions*.

If, in addition, we are also given a collection $\mathcal{H}$ of closed formulas called *hypotheses*, then a **proof under hypotheses** $\mathcal{H}$ is a sequence of **steps**, each of which is a statement together with a justification. The statement is either

- a sentence of the predicate calculus, in which case the justification must show that the statement is either:
  - an axiom,

   - a definition,
   - a hypothesis,

  or

   - a consequence of previous steps by a rule of inference,

or

- an introduction of a new assumption or a new name, in which case the justification must show why this is permitted. (The introduction of a new assumption, or of an arbitrary object, is always permitted, so no justification for this is needed. The introduction of a new object characterized by a condition—for example, by saying "let a be such that $p(a)$," or "pick a such that $p(a)$," or "choose a such that $p(a)$," or "choose an a such that $p(a)$," or "fix an a such that $p(a)$"—will be permitted by Rule 6, provided that we have an earlier step saying "$\exists x\, p(x)$." So when this is done the justification has to state that it is permitted by Rule 6 and indicate which is the previous step where "$\exists x\, p(x)$" is proved.)

To complete this definition of "proof," we have to list the rules of inference. This will be done below.

Before we give the complete list, we give some examples of rules and of steps involving them.

One of our rules (called "Modus Ponens") will say that if you have two formulas of the form P and $P \rightarrow Q$, then you can go to Q. So, for example, suppose that you are writing a proof, and you just finished Step 95. Suppose you get to the following in Step 25:

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

and, later, in Step 47, you have:

(47) $3 > 0 \rightarrow \exists x(x^2 = 3)$ [. . . . .]

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

(95) $\exists x(x^2 = 3)$ [Modus Ponens, from (25) and (47)]

Another rule will tell us that you can always bring in a tautology. (In other words, *every tautology is an axiom.*) 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)	$(3 > 0 \vee 3 < 0) \longrightarrow ((\sim 3 < 0) \longrightarrow 3 > 0)$	[Tautology $(P \vee Q) \rightarrow ((\sim Q) \longrightarrow P)$]
(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 $(P \vee Q) \rightarrow ((\sim Q) \longrightarrow P)$ to be false.)

(B) If by "**why?**" you mean "what for?" (that is, "what is the purpose of picking this particular tautology?"), then the answer 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.

---

5. 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. (This is the rule called "conditional proof" in the book, page 81.) *If assuming P you get to Q, then you can go, without assuming P, to $P \to Q$.*

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

(3591)	$P \to Q$	[.....................]
(4507)	$Q \to R$	[.....................]

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

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

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

Notice that we have used extra indentation to indicate that we are writing a proof within a proof. The way we have organized our proof makes it clear that *at no point are we proving Q or R*. We are proving Q and R *under the assumption P*, from which we can conclude that $P \longrightarrow R$, 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 $P \to R$, 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, if we are working in the world of natural numbers, this is translated as: $\forall n(2 \mid n^2 + n)$.) 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 $\forall n(2 \mid n^2 + n)$."

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

We could organize this as follows:

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

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

6. THE SEVEN INFERENCE RULES FOR PROOFS

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

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

(P.b) It is always permitted to bring in a *definition* as a new step.

(P.c) It is always permitted to bring in one of the *hypotheses* 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 introducing any sentence you want as an assumption, or by bringing in a **new** letter as an arbitrary constant. However, whatever is proved after this is done, is only valid in the "proof within a proof," and one can only get out of it by applying Rule 3 or Rule 5 or Rule 6.

And here, finally, are the seven basic rules of inference.

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

RULE 2. If you have p and $p \to q$ then you can go to q. (This is called *Modus Ponens*; see the book, page 79.).

RULE 3. If you have proved q under the assumption p (that is, if you have assumed p and proved q), then you can go to $p \longrightarrow q$.[2] *(To apply this rule, start a "proof within a proof" by saying "Assume p." Everything you prove after this assumption has been made is "proved under Assumption p." If you ever prove q, then you can get out from being "under Assumption p," and go to $p \longrightarrow q$.)*

RULE 4. Suppose x is a variable, $p(x)$ is a formula where there is no quantifier involving x, and t is a constant term. *(The precise definition of "term" will be given in Handout No. 6. A "constant term" is a term that contains no variables at all.)* Let $p(t)$ be what you get from $p(x)$ by substituting t for x in **all** the occurrences of x in $p(x)$. Then, if you have $\forall x\, p(x)$, you can go to $p(t)$.

NOTE: Rule 4 is the "specialization" rule. It is easy to understand and easy to remember. All the rule says is: if you know that something is true for all things, then you can plug in any particular thing and you will get a true statement. (For example: if you know that "everybody is smart" you can conclude that "Alice is smart.") The name *specialization* comes from the fact that when you go from $\forall x\, p(x)$ to $p(t)$ you are going from a *general statement* (for example, "all people are smart") to a *special case* ("Alice is smart"). The "special case" can be a constant or a more general constant term. For example, suppose you have, in Step (43),

(43) $\quad \forall x(x + 0 = x)$

and t is the term $(3 + 5).6$. Then Rule 4 tells you that, if you want, you can later—say, in Step (99)—specialize x to the value $(3 + 5).6$" and get

(99) $\quad (3 + 5).6 + 0 = (3 + 5).6$ [Rule 4, specializing x to $(3 + 5).6$ in (43)]

The book calls this the "universal specification rule," and states it in a slightly different form. I don't like the name given in the book. More seriously, I am not happy with the form given in the book. The book says: "$\forall x\, P(x) \to P(t)$" is an axiom if "$t$ is a term that represents an object in the domain of the variable x." Here is why I am against the version in the book:

[1] The book, in page 79, has the rule *All tautologies are axioms*, which amounts exactly to the same thing.

[2] The book calls this the "conditional proof rule," see page 81.

1. The phrase "a term represents an object in the domain of the variable x" is too vague. (Even more seriously: we are trying to define proof in a purely *syntactic* way, without resorting to *semantics*, that is, to "meaning" or "representing." If this sounds too abstruse to you, look at it this way: the whole point of a proof is that it is purely formal; you look at your strings and you ought to be able to see if Step 35 follows from Steps 28 and 31 by Rule 4, without invoking what these symbols "mean" or represent.")

2. As a concrete example of what could go wrong, consider the formula $\forall x \exists y(x < y)$, which is certainly true over the real numbers. Can we take $P(x)$ to be $\exists y(x < y)$ and the term t to be y? If you take the book's version of the rule seriously, I don't see why not. But if we do that we get the axiom $\forall x \exists y(x < y) \to \exists y(y < y)$. Since we can prove $\forall x \exists y(x < y)$, we can use Rule 2 (modus ponens) to get

$$\exists y(y < y)\,,$$

which is false!!!!!

To me, this shows that *the book's statement of the rule is wrong.*

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

NOTE: Rule 5 is called "universal generalization" in the book (see page 95). This is a good name, so I will use it too. My version differs from that of the book in that the book tells you that you can go from $P(x)$ to $\forall x P(x)$, whereas I am saying that you can go from $P(a)$ to $\forall x P(x)$, if a is a letter that has not appeared before. In other words, the book would tell you to write things like

Let x be arbitrary.

$\vdots$

$P(x)$.

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

while I am recommending that you write, instead,

Let a be arbitrary.

$\vdots$

$P(a)$.

$\forall x P(x)$.

I think my way is better, because it keeps *constants* such as a clearly distinct from *variables* such as x. Once you "pick an arbitrary a," this a is a constant. In the book's version, you treat x as a constant and then suddenly x becomes a variable again.

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 have $\exists x\, p(x)$ in a previous step. Then you can start a proof within a proof by introducing a new object, calling it a, and stipulating that $p(a)$. This effectively declares a to be a constant, locally, within the "proof within a proof." If you ever get to something that does *not* contain a, then you can use it outside your proof within a proof, in the main proof.

NOTE: Rule 6 is called "existential specification" in the book (see page 97). This is a reasonable name, so I will use it too.

This rule is also just plain common sense. All it says is that if you know that there exists an object of a certain kind, then you can introduce one such object and give it a name.

It is very 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.)

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

NOTE: Rule 7 is called "existential generalization" in the book (see page 99). This is also a good name, and I will keep it.

To illustrate the use of this rule, suppose we are working with the natural numbers, and we want to prove that $\exists n \exists m(28 = n.n - m.m)$. We first prove that

(&) $\quad 28 = 8.8 - 6.6$

and then we can apply Rule 7 (with m in the role of x, $p(m)$ being the formula $28 = 8.8 - m.m$, and t being 6) to conclude

(%) $\quad \exists m(28 = 8.8 - m.m)$ [Rule 7, from (&)]

Then we can apply Rule 7 again, this time with the variable n in the role of x, $p(n)$ being the formula $\exists m(28 = n.n - m.m)$, and t being 8) to conclude

(#) $\quad \exists n \exists m(28 = n.n - m.m)$ [Rule 7, from (%)]

As a second example, suppose we have proved

(&) $\quad 1 + 1 > 1$

Then we can use Rule 7, with n in the role of x, $p(n)$ being the formula $n > 1$, and t being $1+1$, to conclude that

(%) $\quad \exists n(n > 1)$ [Rule 7, from (&)]

That's it. These are **all** the rules of inference. There are exactly **seven** rules. Only seven!!!!

The book, in Chapter 4, gives you lots of other rules, but you don't really need them. **Everything you can do with the rules given in the book can be done using just the seven rules in my list.** Of course, having a larger supply of rules makes it easier to work, because there are more things you can do. But having a smaller set of rules has its own advantages: **with a smaller set of rules there are fewer rules to remember.**

My own preference is in favor of fewer rules, so that one gets a cleaner, more streamlined logical calculus. But on this particular issue **the only disagreement between me and the book is on a matter of taste.**

7. SOME SIMPLE TRICKS

I. Suppose you can prove two formulas P and Q, and you want to go to $P \wedge Q$. How can you do that? Easy! Here is how:

	$\vdots$	
(#)	P	
	$\vdots$	
(&)	Q	
	$\vdots$	
(%)	$P \longrightarrow (Q \longrightarrow (P \wedge Q))$	[Tautology]
(*)	$Q \longrightarrow (P \wedge Q)$	[Rule 2, from (#) and (%)]
($)	$P \wedge Q$	[Rule 2, from (&) and (*)]

II. Suppose you can prove $P \wedge Q$, and you want to go to P. Here is how you can do it:

	$\vdots$	
(#)	$P \wedge Q$	
	$\vdots$	
(%)	$(P \wedge Q) \longrightarrow P$	[Tautology]
(*)	P	[Rule 2, from (#) and (%)]

III. Suppose you can prove $P \longleftrightarrow Q$ and P, and you want to go to Q. Here is how to do it:

	$\vdots$	
(&)	P	
	$\vdots$	
(#)	$P \longleftrightarrow Q$	
(%)	$(P \longleftrightarrow Q) \longrightarrow (P \longrightarrow Q)$	[Tautology]
(*)	$P \longrightarrow Q$	[Rule 2, from (#) and (%)]
($)	Q	[Rule 2, from (&) and (*)]

IV. Suppose you know how to prove Q from P and P from Q, and you want to go to $P \longleftrightarrow Q$. Here is how you can do it:

(&)	Assume P	
	$\vdots$	
(%)	Q	
(*)	$P \longrightarrow Q$	[Rule 3, from (&) and (%)]
($)	Assume Q	
	$\vdots$	
(#)	P	
(+)	$Q \longrightarrow P$	[Rule 3, from ($) and (#)]
(−)	$(P \longrightarrow Q) \longrightarrow ((Q \longrightarrow P) \longrightarrow (P \longleftrightarrow Q))$	[Tautology]
(!)	$(Q \longrightarrow P) \longrightarrow (P \longleftrightarrow Q)$	[Rule 2, from (*) and (−)]
(!!)	$P \longleftrightarrow Q$	[Rule 2, from (+) and (!)]

V. Suppose you have a complicated expression such as $((1+1)+1).(1+1)$ and you want to give it a name, for example you would like to call it a. Here is how you can do it. (This will require using one of the axioms for equality, namely, the one that says that $\forall x(x = x)$.

(&)	$\forall x(x = x)$	[Axiom]
(%)	$((1+1)+1).(1+1) = ((1+1)+1).(1+1)$	[Rule 4, from (&)]
(*)	$\exists x(x = ((1+1)+1).(1+1))$	[Rule 7, from (%), with "$x = ((1+1)+1).(1+1)$" in the role of $p(x)$ and $(1+1)+1).(1+1)$ in the role of t]
($)	Pick a such that $a = ((1+1)+1).(1+1)$	[Rule 6, from (*)]

VI. *(Proof by contradiction)* Suppose you know how to prove a contradiction C assuming $\sim P$, and you want to conclude P. Here is how to do it:

(&)	Assume $\sim P$	
	$\vdots$	
(%)	C	
(*)	$(\sim P) \longrightarrow C$	[Rule 3, from (&) and (%)]
($)	$((\sim P) \longrightarrow C) \longrightarrow P$	[Tautology]
(#)	P	[Rule 2, from (*) and ($)]

VII. *(A slightly different type of Proof by contradiction)* Suppose you know how to prove $\sim Q$ assuming $\sim P$, and you want to conclude P assuming Q. Here is how to do it:

(+)	Assume Q	
(&)	Assume $\sim P$	
	$\vdots$	
(%)	$\sim Q$	
(*)	$(\sim P) \longrightarrow (\sim Q)$	[Rule 3, from (&) and (%)]
($)	$((\sim P) \longrightarrow (\sim Q)) \longrightarrow (Q \longrightarrow P)$	[Tautology]
(#)	$Q \longrightarrow P$	[Rule 2, from (*) and ($)]
(!)	P	[Rule 2, from (+) and (#)]

Now, all we need to start doing formal proofs is some good axioms.
In subsequent handouts, you will get

- Axioms for equality,
- Axioms for the real numbers,
- Axioms for the natural numbers.
- Axioms for sets.