# MATHEMATICS 300 — SPRING 2001

*Introduction to Mathematical Reasoning*

*H. J. Sussmann*

## HANDOUT NO. 4—February 19, 2001

## 1 A CHANGE IN GRADING POLICY

Starting with Homework No. 6, the answer to every question will be graded as follows: a blank answer, or an "I don't know" answer, will get 40%. Correct answers will get 100% if they are perfect, and a little bit less if they are essentially right but contain minor mistakes. Incorrect answers that are judged by me not to be serious will get 0. For example, suppose you are asked to prove that every year must have a Friday the 13th. Suppose this problem is worth 10 points. If you do it correctly, then you get 10 points. If you leave it blank, or write "I don't know how to do it," you will get 4 points. If you write something like "a year has 52 weeks, and $52 > 13$, so there must be a Friday the 13th," then you will get 0, because this cannot possibly be a serious answer, and looks a lot more like a random guess by a student who thought "I have no idea what to do, but let me write something, because in any case I've got nothing to lose by doing so." Under the new policy, *such students will have something to lose.*

The purpose of this new grading policy is to encourage students to be honest and not make up something at random when they do not know how to answer a question. The students who do not know how to answer something and say so deserve to be rewarded for their honesty. This new policy will reward them with 40% of the credit.

This policy agrees with the way we expect people to behave in the real world. If you go to a doctor, tell the doctor about your back pain, and the doctor has no idea what causes it, then you certainly would prefer that the doctor tell you "I don't know," and refer you to a specialist, than that he make up something. You would not want to reward the doctor who made up a diagnosis because "he gave me a diagnosis; it may have been wrong, but at least he tried" but you would be grateful to the honest doctor who told you the truth and did not waste your time by having you focus on a wrong diagnosis. If you are driving somewhere in some place you don't know, and stop to ask someone for directions—for example, "how do I get to the turnpike?"—then if the person does not know you would certainly prefer that he tell you that he does not know than that he make something up. *Exactly the same preferences apply in this course.*

**This policy will be used from now on, and will apply to the homework, the midterms, and the final exam.**

## 2 A REMARK ON THE FIRST MIDTERM EXAM

The first midterm exam will consists of problems similar to the ones in the homework, plus questions on the material of the book and the handouts. (Examples of possible questions: define "even number," explain what a tautology is, explain what a prime number is, explain what the Peano paradox is.)

## 3 PROOFS

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

You should think of proving statements as a **game** that you are playing against an opponent who does not believe that the statement you are proving is true. You make statements, your

opponent may find them convincing or not, and it is up to you to clear up all your opponent's doubts by arguing your case persuasively every time your opponent isn't convinced. (Maybe you should think that I, the instructor, am the "opponent." **You** have to convince **me**. If you convince me, then your proof has worked. Otherwise it has not.)

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

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

EXAMPLE: suppose you want to prove that,

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

  Equivalently—and more concisely—you want to show that

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

Or—even more concisely—you want to prove that ,

$$\forall x \in \mathbb{R}, \left( x \geq 4 \longrightarrow \sqrt{x} \leq \frac{x}{2} \right).$$

To prove this, you can proceed as follows:
To prove $\forall x \in \mathbb{R}, \left( x \geq 4 \longrightarrow \sqrt{x} \leq \frac{x}{2} \right)$, we pick an arbitrary real number $x$ and try to prove that $x \geq 4 \longrightarrow \sqrt{x} \leq \frac{x}{2}$.t

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

**Is this a truly convincing argument?**

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

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

In the proof, we have given justifications for each step. For example, at one point we went from

$$x \geq 4$$

to

$$x^2 \geq 4x\,,$$

and we said that this was done "multiplying both sides by $x$." Now, why is this step permissible?

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

$$\forall a \in \mathbb{R}, \forall b \in \mathbb{R}, \forall c \in \mathbb{R}, (a \geq b \longrightarrow ac \geq bc)\,,$$

using the language of a predicate calculus that we will discuss later.)

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

Now, here is a second try. You can say: "because there is a general rule that says if you take an inequality and multiply both sides by a nonnegative number, then you still get a valid inequality, that is, using symbolic notation:

$$\forall a \in \mathbb{R}, \forall b \in \mathbb{R}, \forall c \in \mathbb{R}, \Big((a \geq b \wedge c \geq 0) \longrightarrow ac \geq bc\Big)\,.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 4 THE STRUCTURE OF A PROOF

Suppose we specify a collection **H** of sentences called **hypotheses**. Suppose in addition that we have a collection **A** of sentences declared to be **axioms**, and a collection **D** of sentences declared to be **definitions**. Then a **proof under hypotheses H**—under the axioms **A** and the definitions **D**— is a sequence of **justified steps**, each of which is a sentence (called the "assertion" of—or in—that particular step) together with a valid justification.

A **proof of a sentence $\mathcal{A}$ under hypotheses H**—under the axioms **A** and the definitions **D**— is a proof under **A** and **D** for which the assertion in the last step is $\mathcal{A}$. A **valid justification** for a step is an explanation showing how the step's assertion is either:

- an axiom,
- a definition,
- a hypothesis,
- a consequence of previous steps by a rule of inference.

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

## 4.1 Some examples

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

One of our rules (called "Modus Ponens") will say that if you have two sentences of the form $\mathcal{A}$ and $\mathcal{A} \longrightarrow \mathcal{B}$, then you can go to $\mathcal{B}$.

So, for example, suppose that you are writing a proof, and you just finished Step 94. Suppose you had the following in Step 25:

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

and, later, in Step 47:

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

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 ("Rule 3.U," or the "rule for using a conjunction") will tell us that if you have a step with a sentence of the form $\mathcal{A} \wedge \mathcal{B}$, then you can go to $\mathcal{A}$ and to $\mathcal{B}$. For example, suppose that at some point of a proof you have

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

Then, if you want to, you can have a later step

(455) $3 > 0$. (By the rule for using a conjunction, from (238).)

Another rule ("Rule 6.U," called the "rule for using a universal sentence," or "specialization rule") will tell us that if you have a universal sentence—say "all elephants have a trunk and tusks"—and a constant—say "Dumbo"—then you can apply the general statement to the special case, and conclude that "Dumbo has a trunk and tusks."

For example, suppose that at some point of a proof you have

(977) $\forall n, (n \in \mathbb{N} \longrightarrow (n+1)^2 = n^2 + 2 \cdot n + 1)$. (.....)

Then, if you want to, you can have a later step

(1088) $3 \in \mathbb{N} \longrightarrow (3+1)^2 = 3^2 + 2 \cdot 3 + 10$. (Specialization, plugging in 3 for $n$ in (977).)

## 4.2 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 assumption you want**. However, when you do that then all the things you prove are proved **under that assumption**.

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 4.P.** (The "conditional proof rule," or "rule for proving an implication.") *If assuming $\mathcal{A}$ you get to $\mathcal{B}$, then you can go, without assuming $\mathcal{A}$, to $\mathcal{A} \longrightarrow \mathcal{B}$.*

For example, suppose that, in some argument you are writing, you established that

(3591) If Gore wins Florida then Gore will become president. (.....)

and, later, that

(4507) If Gore becomes president then the next Attorney General will not be a conservative. (.....)

That means that, if we use the letters $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ to represent the sentences "Gore wins Florida," "Gore becomes president," and "the next Attorney General will not be a conservative," then we already got

(3591) $\mathcal{A} \longrightarrow \mathcal{B}$. (.....)
(4507) $\mathcal{B} \longrightarrow \mathcal{C}$. (.....)

Suppose you just finished writing Step 6812, and now you want to prove $\mathcal{A} \longrightarrow \mathcal{C}$. Here is one thing you could do:

| | | |
|---|---|---|
| (6813) | Assume $\mathcal{A}$. | (Preparation to apply Rule 4.P) |
| (6814) | $\mathcal{B}$. | (Modus Ponens from (3591) and (6813)) |
| (6815) | $\mathcal{C}$. | (Modus Ponens from (4507) and (6814)) |
| (6816) | $\mathcal{A} \longrightarrow \mathcal{C}$. | (Rule 4.P, from (6813) and (6815)) |

Steps 6813, 6814, 6815 constitute a "proof within a proof," in which you introduce the new assumption $\mathcal{A}$, and under this assumption you prove first $\mathcal{B}$ and then $\mathcal{C}$. Then in Step 6816 you go back to the main proof, using Rule 4.P.

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 $\mathcal{B}$ or $\mathcal{C}$*. We are proving $\mathcal{B}$ and $\mathcal{C}$ *under the assumption* $\mathcal{A}$, from which we can conclude that $\mathcal{A} \Rightarrow \mathcal{C}$, as we do in Step 6816. For all we know, $\mathcal{B}$ *and* $\mathcal{C}$ *could perfectly well be false*, and nothing in what we wrote says otherwise. (Actually, $\mathcal{B}$ and $\mathcal{C}$ *are* false.) All our "proof within a proof" says is that *if you assume that $\mathcal{A}$ is true, then $\mathcal{C}$ must be true.*

The "proof within a proof" tells us nothing about what happens if $\mathcal{A}$ is false. And our final conclusion, that $\mathcal{A} \to \mathcal{C}$, is of course valid if $\mathcal{A}$ is false, because **an implication such as $\mathcal{A} \to \mathcal{C}$ is true when $\mathcal{A}$ is false.**

**BOX NO. 1: HYPOTHESES (A.K.A. ASSUMPTIONS).**

**Hypotheses**, or **assumptions**, are statements that we **assume** to be true in a particular situation.
When we discuss proofs later on, we will see that that there are certain statements that you are free to bring in any time you want, because you know them to be true. (Such statements are called "axioms," or "postulates.") In additions, *definitions* function exactly like axioms, the only difference being that an axiom is something you *accept* as true (say, because you are convinced it is true but you do not know how to prove it) whereas a definition (say, for example, $2 = 1 + 1$) is something that you *declare*, or *decide* to be true.
**Within a particular proof, hypotheses/assumptions function exactly like axioms and definitions: they are statements that you can bring in any time.**
There is, however, a big difference. Axioms and definitions are things that we take to be true forever, because we believe they are true. Hypotheses/assumptions are taken to be true not because we believe they are true, but **because we want to know the consequences of their being true.**
For example: suppose we want to find out what the world would be like if pigs had wings. To do this, we first make the assumption "pigs have wings," by saying

(...) Assume that pigs have wings.

Then we would set out to explore the consequences of this assumption. That is, if you prefer, we would 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 might then be able to "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.*

(Proving these theorems might not be easy. For example, it is not true that "every animal that has wings can fly," since, for example, ostriches, penguins and dodos do not fly. But you might notice that all the exceptions to the general rule seem to be birds, so perhaps you could make a convincing case that "every animal that has wings and is not a bird can fly." If you manage to do that, then you might go on to argue that pigs can fly, since pigs clearly are not birds.)
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.

## 4.3 Introducing assumptions

Let us look at what what we have just said from a slightly different angle.

**In a proof you can introduce any assumption you want, at any time. It does not matter if the assumption is true, of if you know whether it is true.**

Students often find this statement shocking, and ask questions such as "how can I assume something if I do not know that it is true?"

The answer is that you can, and in fact you do precisely that most of the time, but for some mysterious reason when students write about mathematics they do not believe that the same thing that they are used to doing in their everyday life is O.K. and works the same way in mathematics.

In you everyday life, you often imagine some possibility in order to figure out what would happen if that was the case. For example, before the last presidential election you probably tried to imagine what would happen if Candidate $X$ won, and what would happen if Candidate $Y$

won. Then you compared the results and came to the conclusion that you liked better what would happen if one of those two candidates won, and decided for that reason to vote for that candidate.

To imagine what would happen if Candidate $X$ won, you almost certainly started thinking along the following lines: "let me suppose that $X$ been elected president; then I guess he would appoint so-and-so as secretary of state, and this person would probably push our foreign policy in sushc-and-such direction, given what I know about his views." And you would have continued like that.

In other words, **you made the assumption that $X$ won without knowing that it was true, and then you explored its consequences**.

You do the same kind of thing all the time. For example, to decide if you will go to Restaurant R for dinner, you would try to imagine what you would eat if you were there, and you might very well end up concluding that none of the dishes that you can imagine yourself ordering looks appealing, so in fact you will not go to Restaurant R. In other words: **you made the assumption that you had gone to Restaurant R and then concluded that you did not like its consequences, so in the end you rendered the assumption false by not going to the restaurant.**

In mathematics we do the same thing. We introduce assumptions, and then explore their consequences. We do not care if the assumptions are true, because all we are trying to find out is "what else would have to be the case if these assumptions were true?"

**BOX NO. 2: ENTERING AND LEAVING IMAGINARY WORLDS.**

As we explained in Box 1, 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 capture this very obvious idea as follows:

- You are always allowed to introduce anything you want as an assumption, any time you want.
- When you do that, whatever you have proved will have been proved **under your assumption**.
- If, assuming a statement $\mathcal{A}$, you prove some other statement $\mathcal{B}$, then you will be allowed to go back to "the real world" and assert there that $\mathcal{A} \longrightarrow \mathcal{B}$.
- If, in addition, you can prove $\mathcal{A}$, then the Modus Ponens rule allows you to go to $\mathcal{B}$.

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

EXAMPLE: If you prove that "pigs can fly" under the assumption that "pigs have wings," then the conclusion that "pigs have wings" will have been established in a world where pigs have wings. You can also go back from such an imaginary world to the real world by stating that "if pigs have wings then pigs can fly." This, however, is not enough to be able to conclude that in the real world pigs can fly, because in the real world you do not know that pigs have wings, and **if you do not know that pigs have wings then you cannot go from "if pigs have wings then pigs can fly" to "pigs can fly."**

**AN EXAMPLE OF A PROOF BY CONTRADICTION.** QUESTION: Prove that the number 30 cannot be expressed as the difference of the squares of two integers.

PROOF: Suppose 30 can be expressed as the difference of the squares of two integers. (*Comment: this is a typical proof by contradiction. We want to prove that something isn't true. To do so, we imagine it is true, that is, we explore what things would be like in an imaginary world where it is true. We then set out to show that this imaginary world is impossible, because in it something impossible would have to be true.*) Pick two integers $n$ and $m$ such that $n^2 - m^2 = 30$. Then $(n-m)(n+m) = 30$. Now $n+m = (n-m)+2m$. Therefore $n-m$ and $n+m$ are either both odd or both even. If $n-m$ and $n+m$ are both odd then their product, i.e., the number 30, would have to be odd. If $n-m$ and $n+m$ are both even then their product, i.e., the number 30, would have to be divisible by 4. So 30 is either odd or divisible by 4. But this is false, because 30 is neither odd nor divisible by 4. So the assumption that 30 can be expressed as the difference of the squares of two integers leads to an impossible conclusion. Therefore 30 cannot be expressed as the difference of the squares of two integers. ♢

**BOX NO. 3: 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 just seen an example: to prove by contradiction that 30 cannot be expressed as the difference of the squares of two integers, we assumed that 30 could be expressed as the difference of the squares of two integers, and ended up with something false, namely, that 30 is either odd or divisible by 4. That is, **we set out to explore an imaginary world in which** 30 **can be expressed as the difference of the squares of two integers, until we saw that in this world impossible things would happen, and then we concluded that such a world could not exist, so** 30 **cannot be expressed as the difference of the squares of two integers.**
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.**

**ANOTHER EXAMPLE OF A PROOF BY CONTRADICTION.** QUESTION: Prove that the number 2 is not the square of a rational number. (That is, "prove that $\sqrt{2}$ is irrational.")

PROOF: Suppose 2 is the square of a rational number. This means that 2 can be expressed as the quotient of the square of an integer divided by the square of a nonzero integer. Pick two integers $n$ and $m$ such that $2 = \frac{n^2}{m^2}$ and $m \neq 0$. Then, after cancelling all common factors $> 1$, we may assume that $n$ and $m$ have no common factors $> 1$. In particular, $n$ and $m$ are not both even, for if they were both even then they would have the factor 2 in common. Now, the equality $2 = \frac{n^2}{m^2}$ implies $2m^2 = n^2$. So $n^2$ is even. But then $n$ is even, because if $n$ was odd then $n^2$ would be odd. So $n = 2k$ for some integer $k$. But then $2m^2 = n^2 = (2k)^2 = 4k^2$. So $m^2 = 2k^2$. So $m^2$ is even. Then $m$ is even, because if $m$ was odd then $m^2$ would be odd. Therefore $n$ and $m$ are both even, and at the same time $n$ and $m$ are not both even. These two assertions together add up to an impossible conclusion. Therefore 2 is not the square of a rational number. ♢

## 4.4 Introducing arbitrary objects

A very important way of starting subproofs by introducing assumptions is to introduce *arbitrary objects*. (See Box 4 for a detailed explanation of how this works.)

**BOX NO. 4: ARBITRARY OBJECTS.**

An *arbitrary object* is a fixed object about which we know nothing. Arbitrary objects can be subjected to certain conditions; for example, an "arbitrary integer" is an arbitrary object that cannot be anything whatsoever (it cannot be, for instance, the State of New Jersey, or a cow, or the number 3/5; it has to be an integer), but other than that it is an integer about which we know nothing whatsoever.
The way you should think about "arbitrary objects" is as follows: imagine that there is somebody (a friend, a computer, a seven-foot tall rabbit called Harvey, or an alien from a planet called Metaluna) whose job is, every time you write "let $a$ be an arbitrary object," to pick one such object, write down what it is on a piece of paper, and then put the paper in an envelope and seal the envelope.
We will call such a person (or computer, or giant rabbit, or alien) the **CAT** ("creator of arbitrary things"). So, for example, if you say "let $a$ be arbitrary; suppose $a$ is an integer" then the **CAT** will pick an integer—say 23—and write "$a = 23$" on the paper that will go inside the envelope. (Actually, the **CAT** is also allowed pick other objects such as Mount Everest or the king of Norway, which are not integers, but, as we shall soon see, a reasonable **CAT** would never do that.)
The crucial facts are:

1. the **CAT** is allowed to pick any object whatsoever and assign it to be the value of your constant;
2. only the **CAT** knows which object he has picked;
3. the **CAT** wants to prove you wrong;
4. the **CAT** is allowed to wait up to the last moment before disclosure time before choosing the values of your arbitrary objects;
5. at the end of your argument, the **CAT** will disclose the chosen values of all the arbitrary constants that you had introduced, and *if these values satisfy all the conditions that were imposed on them but fail to satisfy at least one of the conclusions that you drew about them in your argument the* **CAT** *wins and you lose.* (If the values do not satisfy all the conditions, the **CAT** loses. If the values satisfy all the conclusions, the **CAT** loses.)

So, for example, suppose you say:

Let $a, b, c$ be a arbitrary integers such that $ab = ac$. Then $b = c$.

Then the **CAT** is obliged to choose $a$, $b$ and $c$ to be integers, and to pick them so that $ab = ac$, because if he does not choose them that way then she will lose for sure, because she will fail to satisfy your conditions. So she could pick $a = 3$, $b = 4$, $c = 4$, for example. But, since she is allowed to wait until you have said all you were going to say, she will wait, and when she hears that you said "then $b = c$," she will pick $a = 0$, $b = 3$, $c = 5$, for example, because *with these choices all the conditions you imposed ($a$, $b$, $c$ are integers, and $ab = ac$) are satisfied, but your conclusion is not, so you lose and the* **CAT** *wins.*

For example, suppose you want to argue that every prime number other than 2 is odd. Then you could write the following:

> Let $p$ be arbitrary. Suppose that $p$ is a prime number such that $p \neq 2$. Assume that $p$ was even. Then $p$ is divisible by 2 (because the definition of "even integer" says that an integer is *even* if it is divisible by 2). But, since $p$ is prime, $p$ cannot be divisible by any natural number other that 1 and $p$. Now, 2 is not $p$, because we are assuming that $p \neq 2$. Moreover, $2 \neq 1$. So $p$ *is* divisible by an integer other than 1 or 2. We have thus reached a contradiction, assuming that $p$ was even. So $p$ is odd. (1)

The introduction of an arbitrary constant must always take the form

> Let $a$ be arbitrary. Suppose that $A$ and $B$ and ... and $X$.

Here "let $a$ be arbitrary" is the actualy introduction of the local constant $a$, and $A$, $B$, ..., $X$ are extra conditions that are imposed on $a$.

In practice, the statement that $a$ is arbitrary and the other conditions could be stated together, as in

> Let $p$ be an arbitrary prime number. Suppose that $p \neq 2$.

or

> Let $p$ be an arbitrary prime number such that $p \neq 2$.

Moreover, the word "arbitrary" is often is omitted, and one writes things like

> Let $p$ be a prime number. Suppose that $p \neq 2$.

or, even more concisely,

> Let $p$ be a prime number such that $p \neq 2$.

**It is strongly recommended that you acquire the habit, whenever you see a statement like**

**Let $p$ be a prime number such that $p \neq 2$**

**to see it as really another way of saying**

**Let $p$ be arbitrary. Suppose that $p$ is a prime number and $p \neq 2$.**

**This way of thinking will turn out to make things much easier for you.**

Introducing arbitrary objects is usueful because there will be a rule ("Rule 6.P," called "universal generalization") telling us that, if you prove that something is true for an object $a$ under the assumption thet $a$ is arbitrary, then you can conclude that what you proved about $a$ is true *for all* objects.

**Example 4.4.1** 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, this is translated as

$$\forall n, (n \in \mathbb{N} \longrightarrow 2|(n^2+n)), \qquad \text{or} \qquad \forall n \in \mathbb{N}, 2|(n^2+n),$$

or, if it has been stated before that we are working in the world of natural numbers, we could just write $\forall n, (2|(n^2+n))$.)

Then you could say: "let us pick an **arbitrary** natural number and let us call it $k$. Then $k^2 + k = k(k + 1)$. So $k^2 + k$ is the product of two consecutive integers. Since one of these two integers must be even, it follows that $k^2 + k$ is even. So we have proved that $\forall n(2|n^2 + n)$."

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:

| | | |
|---|---|---|
| (***) | Let $k \in \mathbb{N}$ be arbitrary. | (Preparation to apply Rule 6.P) |
| | $\vdots$ | |
| (!!!) | $k^2 + k$ is even. | ( . . . . . ) |
| ($$$) | $\forall n \in \mathbb{N}, (n^2 + n$ is even). | (Rule 6.P, from (***) and (!!!)) |

or

| | | |
|---|---|---|
| (***) | Let $k$ be arbitrary. | (Preparation to apply Rule 6.P) |
| (&&&) | Assume $k \in \mathbb{N}$. | (Preparation to apply Rule 6.P) |
| | $\vdots$ | |
| (!!!) | $k^2 + k$ is even. | ( . . . . . ) |
| ($$$) | $k \in \mathbb{N} \longrightarrow (k^2 + k$ is even). | (Rule 6.P, from (&&&) and (!!!)) |
| (%%%) | $\forall n, (n \in \mathbb{N} \longrightarrow (n^2 + n$ is even)). | (Rule 6.P, from (***) and ($$$)) |

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

---

## 4.5 The basic logical 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, and in particular to bring 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 one of the rules that allow you to get out of a subproof (that is, Rules 1.P, 1.U, 3.P, 6.P, 7.U).

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

**BOX NO. 5: THE BASIC LOGICAL RULES.**

**RULE 0.** You are allowed to bring in any statement which is an instance of a tautology. (This is called the "tautology proof rule.")

**RULE 1.P.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have started a subproof $P'$ of a proof $P$ with "Assume $\mathcal{A}$" and have obtained $\mathcal{B}$ in a step of $P'$, and $\mathcal{B}$ is a contradiction, then you can get out of $P'$ and go to $\neg\mathcal{A}$ in $P$. (This is the "rule for proving a negation.")

**RULE 1.U.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have started a subproof $P'$ of a proof $P$ with "Assume $\neg\mathcal{B}$" and have obtained $\mathcal{A}$ in a step of $P'$, and you had $\neg\mathcal{A}$ in a previous step of $P$ before you started $P'$, then you can get out of $P'$ and go to $\mathcal{B}$ in $P$. (This is the "rule for using a negation."),

**RULE 2.P.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have $\mathcal{A}$ and $\mathcal{B}$ in previous steps, then you can go to $\mathcal{A} \wedge \mathcal{B}$. (This is called the "rule for proving a conjunction.")

**RULE 2.U.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have $\mathcal{A} \wedge \mathcal{B}$ in a previous step, then you can go to $\mathcal{A}$ and you can also go to $\mathcal{B}$. (This is called the "rule for using a conjunction.")

**RULE 3.P.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have started a subproof $P'$ of a proof with "Assume $\neg\mathcal{A}$" and have obtained $\mathcal{B}$ in a step of $P'$ (or if you started $P'$ with "Assume $\neg\mathcal{B}$" and obtained $\mathcal{A}$), then you can get out of $P'$ and go to $\mathcal{A} \vee \mathcal{B}$ in $P$. (This is the "rule for proving a disjunction.")

**RULE 3.U.** Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, be sentences. If you have $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \longrightarrow \mathcal{C}$, and $\mathcal{B} \longrightarrow \mathcal{C}$, in previous steps, then you can go to $\mathcal{C}$. (This is the "rule for using a disjunction," or "rule of proof by cases.")

**RULE 4.P.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have started a subproof $P'$ of a proof $P$ with "Assume $\mathcal{A}$" and have obtained $\mathcal{B}$ in a step of $P'$, then you can get out of $P'$ and go to $\mathcal{A} \longrightarrow \mathcal{B}$ in $P'$. (This is the "rule for proving an implication," or "conditional proof rule.")

**RULE 4.U.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have $\mathcal{A}$ and $\mathcal{A} \rightarrow \mathcal{B}$ in previous steps, then you can go to $\mathcal{B}$. (This is the "rule for using an implication," or "modus ponens.")

**RULE 5.P.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have $\mathcal{A} \longrightarrow \mathcal{B}$ and $\mathcal{B} \longrightarrow \mathcal{A}$ in previous steps then you can go to $\mathcal{A} \longleftrightarrow \mathcal{B}$ in your proof. (This is called the "rule for proving a biconditional.")

**RULE 5.U.** Let $\mathcal{A}$ and $\mathcal{B}$ be sentences. If you have $\mathcal{A} \longleftrightarrow \mathcal{B}$ in a previous step then you can go to $\mathcal{A} \longrightarrow \mathcal{B}$, and also to $\mathcal{B} \longrightarrow \mathcal{A}$, in your proof. (This is called the "rule for using a biconditional.")

**RULE 6.P** Suppose that

S1. $x$ is a variable and $\mathcal{A}(x)$ is a formula where there is no quantifier involving $x$,

S2. $a$ is a constant and $\mathcal{A}(a)$ is what you get from $\mathcal{A}(x)$ by substituting $a$ for $x$ in **all** the occurrences of $x$ in $\mathcal{A}(x)$.

Suppose you are in a proof $P$ (which may be itself be a subproof of some other proof) and you have started a subproof $P'$ of $P$ by saying "Let $a$ be arbitrary," and that until that point $a$ had never appeared in $P$. Suppose that in $P'$ you got to $\mathcal{A}(a)$. Then you can get out of $P'$ and go to $\forall x, \mathcal{A}(x)$ in $P$. (This the "rule for proving a universal statement," or "universal generalization rule.")

**RULE 6.U** Suppose S1, S2 are true. Then, if you have $\forall x, \mathcal{A}(x)$ in a previous step, you can go to $\mathcal{A}(a)$. (This is the "rule for using a universal statement," or "specialization rule.")

**RULE 7.P.** Suppose S1, S2 are true. Suppose you got $\mathcal{A}(a)$ in a previous step. Then you can go to $\exists x, \mathcal{A}(x)$. (This is the "rule for proving an existential statement, or "existential generalization rule.")

**RULE 7.U.** Suppose S1, S2 are true. Suppose you have started a subsubproof $P''$ within a proof $P$ by saying "Let $a$ be arbitrary," and "Assume $\mathcal{A}(a)$." Suppose that until that point $a$ had never appeared in $P$. Suppose that in $P''$ you got to $\mathcal{B}$, where $\mathcal{B}$ is a sentence that does not contain the constant $a$. Suppose that in a previous step of $P$, before you started $P''$, you had $(\exists x, \mathcal{A}(x))$. Then you can get out of $P''$ and go to $\mathcal{B}$ in $P$. (This is the "rule for using an existential statement, or "existential specification rule.")

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

## 4.6 Comments on the logical rules

There are fifteen rules. Maybe you think this is too much, and that remembering 15 rules requires a lot of effort on your part. I will show you now that this is not so, because **the rules of Box 5 are just plain common sense, so you should have no difficulty understanding them and remembering them**.

Actually, there is no need to have 15 rules. The number of rules can be cut down a lot, because several of the rules in Box 5 are really not needed. On the other hand, having these 15 rules makes it much easier to write proofs than if you had fewer rules. (In many cases, our rules enable you to do in one step what might require five or six steps without using the rule.)

Let us notice that the rules obey a nice simple pattern. In addition to the "tautology rule" (i.e., Rule 0), our rules are neatly organized into seven pairs consisting of two rules each. The seven pairs correspond to the **seven logical connectives**:

$$\neg \qquad \wedge \qquad \vee \qquad \longrightarrow \qquad \longleftrightarrow \qquad \forall \qquad \exists \quad .$$

Remember that **every mathematical sentence is of one and only one of the following eight types**:

- negation ("not", i.e, "$\neg$"),
- conjunction ("and", i.e, "$\wedge$"),
- disjunction ("or", i.e, "$\vee$"),
- implication ("implies", or "if ... then", i.e, "$\longrightarrow$"),
- biconditional ("if and only if", i.e, "$\longleftrightarrow$"),
- universal ("for all", i.e, "$\forall$"),
- existential ("for some", or "there exists ... such that", i.e, "$\exists$"),
- atomic.

*Atomic sentences* (for example, $2 + 2 = 4$) cannot be analyzed into smaller parts put together by logical connectives. This means that if you want to prove or use an atomic sentence you need to do mathematics, rather than pure logic. The main part of the course will be devoted to the mathematics, but at this point we are concentrating on the logical part. That is why we are presenting rules that tell us how to work with non-atomic sentences and use their logical structure to figure out how to use them and how to prove them.

As we indicated before, all the rules other than Rule 0, come in pairs of two rules each. There are seven such pairs, one for each of the seven logical connectives. For each connective, there are two rules: one rule (the "P" rule) tells you how to *prove* a sentence whose type is that of the corresponding connective, and the other rule (the "U" rule) tells you how to *use* such a sentence.

Now let us look at the rules one at a time, and show that they are no more than plain common sense.

- Rule 0 just expresses the fact that instances of tautologies are guaranteed to be true, so it is perfectly reasonable to allow yourself to bring them in any time you want.

- Rule 1.$P$ and 1.$U$ enable us to do proofs by contradiction: to prove something, assume it is not true and get to something that is known to be false, because it is a contradiction (as in Rule 1.$P$) or something that had been proved false in a previous step (as in Rule 1.$U$).

- Rule 1.P is a "prove" rule. It gives us a way to get to $\neg\mathcal{A}$: assume $\mathcal{A}$ and try to get a contradiction.

- Rule 1.U is a "use" rule. It gives us something to do if we have a sentence of the form $\neg\mathcal{A}$ and we want to prove another sentence $\mathcal{B}$: assume $\neg\mathcal{B}$ and try to get to $\mathcal{A}$.

- Rule 2.$P$ is a "prove" rule. It tells us how to prove a conjunction, using the evident fact that if you know that two things are true then you can conclude that their conjunction is true.

- Rule 2.$U$ is a "use" rule. It tells us how to make use of a conjunction: if you know that the conjunction of two things is true then you can conclude that each one of them is true.

- Rule 3.$P$ is a "prove" rule. It gives us a way to prove a disjunction: to prove that one of two things is true, assume one isn't true and prove that the other one is true. (For example: if I want to argue that somebody did something because he is crazy or has some inside information that we don't have, I could try to show that if he doesn't have some inside information that we don't have then he must be crazy.)

- Rule 3.$U$ is a "use" rule. It gives us a way to put to use the information that a disjunction is true. The way we normally do this is by arguing by cases. If we want to conclude $\mathcal{C}$ and we know $\mathcal{A} \wedge \mathcal{B}$, then we consider the case when $\mathcal{A}$ is true, and then the case when $\mathcal{B}$ is true, and show that in each case $\mathcal{C}$ must be true.

- Rule 4.$P$ is a "prove" rule. It gives us a way to prove an implication: to prove $\mathcal{A} \longrightarrow \mathcal{B}$, assume $\mathcal{A}$ and prove $\mathcal{B}$.

- Rule 4.$U$—Modus Ponens—is one of the most important of all the rules. It is a "use" rule. It gives us a way to put to use an implication $\mathcal{A} \longrightarrow \mathcal{B}$. If you manage in addition to prove $\mathcal{A}$, then the rule tells you that you can go to $\mathcal{B}$.

- Rule 5.$P$ is an obvious "prove" rule. It tells us that you can prove a biconditional of the form $\mathcal{A} \longleftrightarrow \mathcal{B}$ by proving $\mathcal{A} \longrightarrow \mathcal{B}$ and $\mathcal{B} \longrightarrow \mathcal{A}$.

- Rule 5.$U$ is a trivial "use" rule. It tells us that if you have a biconditional $\mathcal{A} \longleftrightarrow \mathcal{B}$ then you can use it by concluding from it the implications $\mathcal{A} \longrightarrow \mathcal{B}$ and $\mathcal{B} \longrightarrow \mathcal{A}$.

- Rule 6.$P$ is a "prove" rule. It gives us a way to prove a universal statement: to prove that some statement $S$ is true for all possible values of the variable $x$, pick an arbitrary object, call it $a$, and prove that $S$ is true of $a$.

- Rule 6.$U$—the specialization rule— is a "use" rule. It is extremely easy to understand, and the name is easy to remember. The rule basically says: 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 in going from $\forall x, \mathcal{A}(x)$ to $\mathcal{A}(a)$, you are going from a *general statement* (for example, "all people are smart") to a *special case* ("Alice is smart").

- Rule 7.$P$ is a "prove" rule. It gives us a way to prove an existential statement: to prove that $\exists x, \mathcal{A}(x)$, exhibit an $a$ such that $\mathcal{A}(a)$.

- Finally, Rule 7.$U$ is another "use" rule which just reflects 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.

  The most common way you would apply this rule is this. Say you are trying to prove $\mathcal{B}$ and you know that $\exists x, \mathcal{A}(x)$. Then you would say "since I know that there exists an $x$ such that $\mathcal{A}(x)$, let me pick one and call it $a$." You could do that by starting a subproof with "Let $a$ be arbitrary," and then a subsubproof with "Assume $\mathcal{A}(a)$." Suppose you then work your way to $\mathcal{B}$. Then you can get out of the subsubproof and land in the proof with $\mathcal{B}$.

  **It is very important that the new object $a$ be given a name that has not been used before.** For example, suppose "$\mathcal{A}(x)$" stands for "$x$ killed Polonius," and we are told that $\exists x, \mathcal{A}(x)$, 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 "$\mathcal{A}(a)$" or that "$\mathcal{A}$(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 $\mathcal{A}$(Hamlet), i.e. that Hamlet killed Polonius, or that $\mathcal{A}$(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.)

**Also, notice that the rule only allows you to conclude that $\mathcal{B}$ holds if you know that $\exists x, \mathcal{A}(x)$.** If you do not know that such an $x$ exists, then you cannot do anything with the rule, and in particular you cannot get to $\mathcal{B}$.

For a typical example of the kind of outrageous mistakes that one can make by failing to pay attention to the requirement that you must know that $\exists x, \mathcal{A}(x)$, look carefully at the Peano paradox, described in Box No. 6 below. **Make sure you understand and can explain what is wrong with that proof.**

**BOX NO. 6: 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 $n$ is the largest natural number, $n^2 \leq n$. On the other hand, $n^2 \geq n$. (Proof by cases: either $n \geq 1$ or $n = 0$. If $n \geq 1$ then so $n^2 = n.n \geq n.1 = n$. So $n^2 \geq n$. If $n = 0$ then $n^2 = 0$, so $n^2 = n$ and then $n^2 \geq n$.) 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 $n$ is the largest natural number, so $n$ cannot be 0 because $1 > 0$. Therefore $n$ has to be equal to 1. **QED**

## 4.7 An example of a completely formal proof

The definition of the empty set says:

$$\forall x, (\neg x \in \emptyset)\,.$$

(That is, "nothing belongs to the empty set.")

The definition of *set inclusion* says that if $X$, $Y$ are sets then

$$X \subseteq Y \longleftrightarrow (\forall x, (x \in X \longrightarrow x \in Y))\,.$$

(That is, "$X$ is a subset of $Y$ if and only if every member of $X$ belongs to $Y$.")

Using these two definitions plus our logical rules, let us give a completely formal proof of the following.

**Theorem 4.7.1** *If $A$ is any set then $\emptyset \subseteq A$.*

**PROOF:**

| | | |
|---|---|---|
| (1) | $\forall x, (\neg x \in \emptyset)$. | [Definition of $\emptyset$] |
| (2) | Let $a$ be arbitrary. | [Preparation to apply Rule 6.P] |
| (3) | Assume $a \in \emptyset$. | [Preparation to apply Rule 6.P] |
| (4) | Assume $\neg(a \in A)$. | [Preparation to apply Rule 4.P] |
| (5) | $\neg a \in \emptyset$. | [Rule 6.U, plugging $a$ for $x$ in (a)] |
| (6) | $a \in \emptyset \wedge (\neg a \in \emptyset)$. | [Rule 2.P, from (3) and (5)] |
| (7) | $\neg(\neg(a \in A))$. | [Rule 1.P, from (4) and (6), since $a \in \emptyset \wedge (\neg a \in \emptyset)$ is a contradiction] |
| (8) | $(\neg(\neg(a \in A))) \longrightarrow a \in A$. | [Rule 0] |
| (9) | $a \in A$. | [Rule 4.U, from (7) and (8)] |
| (10) | $a \in \emptyset \longrightarrow a \in A$. | [Rule 4.P, from (3) and (9)] |
| (11) | $\forall x, (x \in \emptyset \longrightarrow x \in A)$. | [Rule 6.P, from (2) and (10)] |
| (12) | $\emptyset \subseteq A \longleftrightarrow (\forall x, (x \in \emptyset \longrightarrow x \in A))$. | [Definition of $\subseteq$] |
| (13) | $(\forall x, (x \in \emptyset \longrightarrow x \in A)) \longrightarrow \emptyset \subseteq A$. | [Rule 5.U, from (12)] |
| (14) | $\emptyset \subseteq A$. | [Rule 4.U, from (11) and (13).] |

**END OF PROOF**