MATHEMATICS 300 — SPRING 2006

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Pages 1 to 88

(February 27, 2006)

Contents

1 Information on the course

1.1 Course schedule

Our class (Introduction to Mathematical Reasoning, Mathematics 300, section 04) meets on **Mondays and Wednesdays, 5th period (3:20 to 4:40 pm)** in Room 209, Tillett Hall (Livingston Campus).

1.2 About the instructor

My *name* is **H.J. Sussmann.** My *office* is **Hill 538**.
My *Rutgers phone extension* is 5-5407.
My *e-mail address* is **sussmann@math.rutgers.edu**.

1.3 Web page

I have set up a *Web page* for our Math 300 section:

http://www.math.rutgers.edu/~sussmann/math300page.html

All the instructor's notes will be available there.

1.4 Office hours

My office is **Hill 538**. My office hours will be:

- **Monday and Wednesday, 1:00 p.m. to 2:30 p.m.**, in my office,
- any other time, by appointment, in my office.

1.5 Lectures

We will have **26 lectures**, on

- January 18, 23, 25, 30,
- February 1, 6, 8, 13, 15, 20, 22, 27,
- March 6, 8, 20, 22, 27, 29,
- April 3, 5, 10, 12, 17, 19, 26,
- May 1

and **two midterm exams**, on **Monday, March 1** and **Monday April 24**.

1.6 Homework, midterms, final exam.

Homework and quizzes will count for about one third of your grade. There will be *two midterms*, which will count—together—for another third of your grade. The *final exam* will count for the remaining third.

Midterm dates: Monday, March 1 and **Monday, April 24**.

The **Final exam date** will be announced as soon as it becomes available.

1.7 The textbook and the instructor's notes

We will be using:

- the book *A Transition to Advanced Mathematics* (sixth edition), by Douglas Smith, Maurice Eggen, and Richard St. Andre;
- the notes written by the instructor.

The material of the instructor's notes is an integral part of the course, as much as that of the book. *Furthermore, the notes contain all kinds of important information. For example, in this set of notes there are lots of things you need to know in order to do your homework.*

1.8 Readings for the first 5 days (January 18, 23, 25, 30, and February 1)

- the book's "Preface to the student,"
- the book's Chapter 1 (**all of it!**),
- the instructor's notes, Part 1.

1.9 Homework assignment no. 1, due on Wednesday Jan. 25.

Before you start writing your homework, read carefully the rest of this handout, in particular §2 on writing mathematics and submitting homework." Pay special attention to §2.3, on "answering questions in this course."

1. Book, Exercises 1.1. (pages 8-9-10-11): Problems 1 (non-starred items), 2(d)(i)(j)(l), 3(non-starred items), 6(b)(c)(d), 8(non-starred items), 10(k)(l)(m), 11.
2. Prove that there exist integers x, y such that $x^2 - y^2 = 28$.
3. Prove that there exist integers x, y such that $x^2 - y^2 = 29$.
4. Prove that there exist integers x, y such that $x^2 - y^2 = 30$.
5. Prove that every prime number greater than 2 is odd. (*NOTE: The definitions of "odd" and "prime number" are given in the book, page xii. A* **natural number** *is an integer n such that $n \geq 1$.*)
6. Find a prime number p such that $p > 3$, $p + 2$ is prime, and $p + 4$ is prime. (*NOTE: If it wasn't for the requirement that $p > 3$, you could take $p = 3$, in which case $p + 2 = 5$ and $p + 4 = 7$, so p, $p + 2$ and $p + 4$ are prime. But I am asking you to find a p such that in addition $p > 3$, so choosing $p = 3$ will not do.*)
7. (Optional) Prove that every year must have a Friday the 13th.
8. (Optional) Prove that the statement of Problem 7 remains true even if we change the order of the months (without changing the names of the months or the number of days of each month) in an arbitrary .way.

2 Some remarks about mathematical writing

2.1 Write clearly in complete sentences

You should write so that you can be easily understood by a properly trained English-speaking individual. In particular, this means that you must

- Use *complete English sentences*, that make clearly identifiable *statements* with a *clear meaning* that can can be understood by anyone reading what you wrote. For example:
  - If you tell me that "she is very smart," but you haven't told me who "she" is, then I don't know who you are talking about, so you haven't made a statement with a clear meaning.
  - If you write "$x > 0$," but you haven't told me who "x" is, then I don't know what you are talking about, so you haven't made a statement.
  - If I ask you to state Pythagoras' theorem and your answer only says "$a^2 + b^2 = c^2$," then nobody will know what you are talking about [1], because you have not said what "a," "b," and "c" are supposed to be.[2]
- Avoid exaggerated or incorrect use of cryptic mathematical notation.
- Explain what you are doing.
- Make sure that letter "variables" are used correctly, that is that either: (i) it has been said before what these letters stand for, or (ii) they are "closed variables" (or "dummy variables," or "bound variables") in the sense that will be discussed in detail in class, and will also be explained later in these notes.
- Provide proper connectives between equations as well as between ideas.
- Make sure that all the rules of English grammar (including those of spelling and punctuation) are strictly obeyed.
- Try to say things correctly, following all the rules, but *in your own words.* Please *no rote learning.* If you have to memorize a definition or

[1] Of course, your teacher will know what you are trying to say, and anybody who already knows the statement of Pythagoras' theorem will know. But when you are asked to state a theorem or a definition **you should write it as if you were talking to somebody who does not know yet what the theorem or the definition say.**

[2] Here is a correct statement of Pyhtagoras' theorem: *Let c be the lenght of the hypothenuse of a right triangle, and let a, b be the lengths of the other two sides. Then $a^2 + b^2 = c^2$.*

a statement, then that is not a good sign, because it indicates lack of understanding.

- Please proofread carefully what you hand in. Ideally, you should read and reread and revise almost any formal communication. **Neatness and clarity count**, as you well know if you've tried to read any complicated document.
- *Do not assume that the people reading your paper can read your mind. Do assume that they are intelligent, but also assume that they are busy, and cannot and will not spend an excessive amount of time puzzling out your meaning. Communication is difficult, and written technical communication is close to an art.*

Effective written exposition will be worth at least 50% of your grade. Conversely, bad or unclear exposition may be penalized as much as 50% of the grade or even more.

- The best reference known to me on effective writing is *The Elements of Style* by Strunk and White, a very thin paperback published by Macmillan. It isn't expensive, and it is easy to read. I recommend it.

2.2 Your written work

You should pay attention to presentation, especially for the homework:

- A nicely typed homework (e.g., using a word processor) is preferable to handwritten work. Handwritten work is acceptable too, but in that case:
  - If you have to cross out lots of words, then you should rewrite the whole thing anew, **cleanly and neatly**. If you are not willing to spend some of your time doing this; if what you hand in shows

that you were in a hurry and that you did not make the effort to write things neatly and properly, then there is no reason for the instructor or the grader to spend any of our time reading what you wrote, and we will not do it.

  - Use a pen. Never use a pencil.
  - Use any color other than red (for example, black, blue, or green), but DO NOT USE RED. (Reason: The use of red is reserved for the instructor's and grader's comments.)
  - If you tear off the sheets from a spiral notebook, please make sure before you hand them in that there are none of those ugly hanging shreds of paper at the margins. Use scissors, or a cutter, if necessary.

- Make sure that **your name appears in every sheet of paper you hand in**, and that if you are handing in more than one sheet then the sheets are **stapled** and the pages are **numbered**.

If you hand in a homework assignment that has at least one of the following flaws:

- **it is written carelessly or in a hurry,**
- **it has lots of words crossed out,**
- **it has unreadable handwriting,**
- **it has pages that are unstapled or unnumbered or fail to show your name,**
- **it has shreds of paper at the margins,**
- **it is written using pencil rather than a pen,**
- **it is written in red,**

then the assignment will be marked "unacceptable" and returned unread.

2.3 Answering questions in this course

In this course, whenever you are given a problem where you are asked to do something, your answer should be either:

(a) doing what you were asked to do,

or

(b) showing—that is *proving*—that it cannot be done.

(See, for example, Problems 2, 4, 6, 7 below, where the correct answer is "what you asked me to do cannot be done.")

Notice that, when the answer is that "it cannot be done," it is not enough for you to *say* that it cannot be done. *You have to tell me why.* In other words, you have to *prove* that it cannot be done.

This remark is very important, and will apply throughout the semester, not just during the first week. And it applies to all your work, to the homework, the quizzes, the midterm exams, and the final exam. So please read it until you are sure you got the point. ♢

2.4 Some examples of problems with correct answers (including several examples of proofs)

Here are some examples of problems with correct solutions:

PROBLEM 1: Express the number 26 as a sum of two odd natural numbers.

ANSWER: $26 = 3 + 23$. ♢

REMARK: *There are lots of other solutions, of course! For example, here are two solutions different from the one given above:* $26 = 7 + 19$, $26 = 13 + 13$.

PROBLEM 2: Express the number 27 as the sum of two odd natural numbers.

SOLUTION: This is impossible. REASON: the sum of two odd numbers is always even. Since 27 is odd, it cannot be the sum of two odd numbers. ♢

PROBLEM 3: Prove that the number 26 can be expressed as the sum of the squares of two integers. That is, prove that there exist integers m, n such that $26 = m^2 + n^2$.

ANSWER: $26 = 5^1 + 1^2$. So, if we take $m = 5$, $n = 1$, then $26 = m^2 + n^2$. $\diamondsuit$

REMARK: What we have used here is the standard technique for proving that an object of a certain kind exists, namely, **exhibiting one**. We wanted to show that a pair m, n of integers having a certain property, namely, $m^2 + n^2 = 26$, exists, so we produced one such pair.

PROBLEM 4: Prove that the number 22 can be expressed as the sum of the squares of two integers. That is, prove that there exist integers m, n such that $22 = m^2 + n^2$.

SOLUTION: This cannot be proved because it is not true. REASON: Suppose it was possible to express 22 as the sum of the squares of two integers. Pick two integers m, n such that $m^2 + n^2 = 22$. Then we may assume that $m \geq 0$ and $n \geq 0$, because if m or n was < 0 then we could replace it by its negative and the equality $m^2 + n^2 = 22$ would still hold. Now, m cannot be > 4, because if $m > 4$ then $m \geq 5$, so $m^2 \geq 25$, and then $m^2 + n^2$ cannot be equal to 22, since $n^2 ge 0$. So the only possible values of m are 0, 1, 2, 3, and 4. If $m = 0$, then $m^2 + n^2 = n^2$, so $n^2 = 22$, which is not possible because 2 is not the square of an integer. If $m = 1$, then $22 = m^2 + n^2 = 1 + n^2$, so $n^2 = 21$, which is not possible because 21 is not the square of an integer. If $m = 2$, then $22 = m^2 + n^2 = 4 + n^2$, so $n^2 = 18$, which is not possible because 18 is not the square of an integer. If $m = 3$, then $22 = m^2 + n^2 = 9 + n^2$, so $n^2 = 13$, which is not possible because 13 is not the square of an integer. If $m = 4$, then $22 = m^2 + n^2 = 16 + n^2$, so $n^2 = 6$, which is not possible because 6 is not the square of an integer. So all five cases $m = 0, 1, 2, 3, 4$ have been excluded. Since we have shown that these are all the possible values of m, it follows that m, n cannot exist. $\diamondsuit$

PROBLEM 5: Prove that the number 22 can be expressed as the sum of the squares of three integers. That is, prove that there exist integers m, n, q such that $22 = m^2 + n^2 + q^2$.

SOLUTION: $22 = 3^2 + 3^2 + 2^2$. So we can take $m = 3$, $n = 3$, $q = 2$. $\diamondsuit$

PROBLEM 6: Prove that $2 + 2 = 5$.

SOLUTION: This cannot be done. REASON: The statement "$2 + 2 = 5$" is false, and false statements cannot be proved. $\diamondsuit$

PROBLEM 7: Express the number 15 as the sum of the squares of three integers.

SOLUTION: This cannot be done. REASON: If we are going to write 15 as the sum of three squares, then we should be able to write it as the sum of two nonnegative integers, one of which is a square, while the other is the sum of two squares.

So let us look at all the ways to write 15 as a sum of two nonnegative integers, see in which cases one of these numbers is square, and then see if the other number is the sum of two squares.

Here are all the ways to express 15 as a sum of two nonnegative integers:

$$\begin{array}{llll} 15 = 0 + 15, & 15 = 1 + 14, & 15 = 2 + 13, & 15 = 3 + 12, \\ 15 = 4 + 11, & 15 = 5 + 10, & 15 = 6 + 9, & 15 = 7 + 8\,. \end{array}$$

There are four expressions in the above list where one of the numbers is a square:

$$15 = 0 + 15, \quad 15 = 1 + 14, \quad 15 = 4 + 11, \quad 15 = 6 + 9\,.$$

In each case, we must ask whether the other number is a sum of two squares.

For "15=0+15," we have to see if 15 is the sum of two squares. The answer is "no," because we already have the list of all (eight) ways of writing 15 as a sum of two nonnegative integers, and in no case are both those numbers suqares.

For "15=1+14," we have to see if 14 is the sum of two squares. The answer is "no." (Reason: the only squares not greater than 14 are 0, 1, 4, and 9. So if are going to write 14 as a sum of two squares, the only possibilities are $14 = 0 + 14$, $14 = 1 + 13$, $14 = 4 + 10$, $14 = 9 + 6$. But in all these cases the other number—that is, 14, 13, 10, or 6—is not a square.)

For "15=4+11," we have to see if 11 is the sum of two squares. The answer is "no." (Reason: the only squares not greater than 11 are 0, 1, 4, and 9. So if are going to write 11 as a sum of two squares, the only possibilities are $11 = 0 + 11$, $11 = 1 + 10$, $11 = 4 + 7$, $14 = 9 + 5$. But in all these cases the other number (that is, 11, 10, 7, or 5) is not a square.)

Finally, for "15=6+9," we have to see if 6 is the sum of two squares. The answer is "no." (Reason: the only squares not greater than 6 are 0, 1, and

4. So if are going to write 6 as a sum of two squares, the only possibilities are $6 = 0 + 6$, $6 = 1 + 5$, $6 = 4 + 2$. But in all these cases the other number (that is, 6, 5, or 2) is not a square.) $\diamondsuit$

PROBLEM 8: Prove that the number 15 can be expressed as the sum of the squares of four integers. That is, prove that there exist integers m, n, p, q such that $m^2 + n^2 + p^2 + q^2 = 15$.

SOLUTION: $15 = 1 + 1 + 4 + 9 = 1^2 + 1^2 + 2^2 + 3^2$. So we can take $m = 1$, $n = 1$, $p = 2$, $q = 3$. $\diamondsuit$

PROBLEM 9: Prove that the number 674 can be expressed as the sum of the squares of four integers. That is, prove that there exist integers m, n, p, q such that $m^2 + n^2 + p^2 + q^2 = 674$.

SOLUTION: $674 = 144 + 400 + 121 + 9 = 12^2 + 20^2 + 11^2 + 3^2$. So we can take $m = 12$, $n = 20$, $p = 11$, $q = 3$. $\diamondsuit$

PROBLEM 10: Prove that the number 18778 can be expressed as the sum of the squares of four integers. That is, prove that there exist integers m, n, p, q such that $m^2 + n^2 + p^2 + q^2 = 18778$.

SOLUTION: $18778 = 10201 + 6724 + 1369 + 484$, $10201 = 101^2$, $6724 = 82^2$, $1369 = 37^2$, and $484 = 22^2$, so $18778 = 101^2 + 82^2 + 37^2 + 22^2$. Therefore, we can take $m = 101$, $n = 82$, $p = 37$, $q = 22$. $\diamondsuit$

REMARK: You may be thinking *how on Earth did the author of these notes figure out how to solve Problems 9 and 10?* That's a very good question. It turns out that there is a technique for doing this, but it's not easy to explain. Maybe we will talk about it later in the course. But keep in mind that the question "how did I find a solution to problem 14?" is quite different from the question "is $674 = 12^2 + 20^2 + 11^2 + 3^2$ a correct solution?" This second question is easy to answer: you just compute $12^2 + 20^2 + 11^2 + 3^2$ and verify that what you get is 674. Similarly, you can easily verify that my solution of Problem 10 is correct: all you have to do is compute the squares 101^2, 82^2, 37^2, and 22^2, and add them.

This illustrates a general point:

Often, **finding** a solution of a problem can be quite hard, while on the other hand **checking** whether or not something given to you is a solution may be very easy.

REMARK: The previous observation applies, in particular, to proofs:

If I ask you to find a proof of something, that may be very hard. On the other hand, once you have written what you think is a proof, or someone else has given you a purported proof, it is usually very easy to **check** whether or not it really is a proof.

REMARK: You may have noticed that I gave you examples of natural numbers that could be expressed as the sum of two squares, and of natural numbers that could not. Then I gave you examples of natural numbers that could be expressed as the sum of three squares, and of natural numbers that could not. But for *four* squares what I have done is different: I gave you examples of natural numbers that could be expressed as the sum of four squares, but I did not give you examples of natural numbers that could not. Is there a reason for this? The answer is **yes**. The mathematician Lagrange (1736-1813) proved that **every natural number can be expressed as the sum of the squares of four natural numbers.** This is a hard theorem, and I will try to say a few words about it later in the course. ♢

PROBLEM 11: Prove that $2 + 2 = 4$.

COMMENT: This statement is of course true, so it should be possible to prove it. Now, you will be asking, **don't we already know that the statement is true?** *The answer is "sure, we know." But then, if it is true, it should be either an axiom or a definition or something that we can prove from our axioms and definitions.*

Now, here are some of the definitions that we will introduce later when we do everything systematically:

DEFINITION D2. $2 = 1 + 1$.

DEFINITION D3. $3 = 2 + 1$.

DEFINITION D4. $4 = 3 + 1$.

In addition, let me give you a few axioms:

AXIOM AA: *(The associative law of addition) If x, y, and z are arbitrary real numbers, then $x + (y + z) = (x + y) + z$.*

AXIOM 1R: 1 *is a real number.*

AXIOM ACl: *(The closure axiom for addition) If x and y are arbitrary real numbers, then $x + y$ is a real number.*

As you can see, "$2 + 2 = 4$" is neither an axiom nor a definition. (The definition of 4 *says "$4 = 3 + 1$," which is not at all the same as "$2 + 2 = 4$.")*

And, finally, here is a **rule of inference**, i.e., a rule that enables us to obtain new statements from old ones.

RULE SEE: (The "substitution of equals for equals" rule) If a, b are terms. P is a statement, and Q is a statement obtained from P by substituting b for a in some or all the occurrences of a in P, then (i) from $a = b$ and P you can go to Q, and (ii) from $b = a$ and P you can go to Q.

We can now restate Problem 11 more precisely:

PROBLEM 11, PRECISELY STATED: Prove that $2 + 2 = 4$, using Axioms AA, 1R, ACl, Definitions D2, D3, D4, and Rule SEE.

SOLUTION (using "$\in \mathbb{R}$" as an abbreviation[3] for "is a real number"):

Step 1:	$1 \in \mathbb{R}$.	[Axiom 1R]
Step 2:	If $x \in \mathbb{R}$ and $y \in \mathbb{R}$, then $x + y \in \mathbb{R}$.	[Axiom ACl]
Step 3:	$1 + 1 \in \mathbb{R}$.	[From Steps 1, 2]
Step 4:	$2 = 1 + 1$.	[D2]
Step 5:	$2 \in \mathbb{R}$.	[From Steps 3,4 via Rule SEE]
Step 6:	If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $z \in \mathbb{R}$, then $x+(y+z)=(x+y)+z$.	[Ax. AA]
Step 7:	$2 + (1 + 1) = (2 + 1) + 1$.	[From Steps 1, 5, 6]
Step 8:	$3 = 2 + 1$.	[D3]
Step 9:	$2 + 2 = (2 + 1) + 1$.	[From Steps 4 and 7, via Rule SEE]
Step 10:	$2 + 2 = 3 + 1$.	[From Steps 9 and 8, via Rule SEE]
Step 11:	$4 = 3 + 1$.	[D4]
Step 12:	$2 + 2 = 4$.	[From Steps 10 and 11, via Rule SEE]

END

[3]From now on, we will *always* use "$\in \mathbb{R}$" as an abbreviation for "is a real number."

PROBLEM 12: Prove that $2 \cdot 2 = 4$.

COMMENT: Again, this statement is of course true, so it should be possible to prove it. And, again, you will be asking whether we don't already know that the statement is true. The answer, as before, is "sure, we know. But then, if the statement is true, it should be either an axiom or a definition or something that we can prove from our axioms and definitions.

Which axioms, definitions and rules should we allow ourselves to use? Obviously, since the result involves multiplication, we will need axioms that talk about multiplication. Actually, it turns out that two new axioms will do the job. .

AXIOM DIS: *(The distributive law) If x, y, and z are arbitrary real numbers, then $x \cdot (y + z) = x \cdot y + c \cdot z$.*

AXIOM 1M: *If x is an arbitrary real number, then $x \cdot 1 = x$.*

We can now restate Problem 12 more precisely:

PROBLEM 12, PRECISELY STATED: Prove that $2 \cdot 2 = 4$, using Axioms AA, 1R, ACl, DIS, 1M, Definitions D2, D3, D4, Rule SEE, and all the statements proved before in Problem 11.

SOLUTION:

Step 1:	$2 + 2 = 4$.	Proved in Problem 11]
Step 2:	If $x \in \mathbb{R}$ then $x \cdot 1 = x$.	[Axiom 1M]
Step 3:	$2 \in \mathbb{R}$.	[Proved in Problem 11]
Step 4:	$2 \cdot 1 = 2$.	From Steps 2, 3]
Step 5:	$2 \cdot 1 + 2 \cdot 1 = 4$.	[From Steps 1,4 via Rule SEE]
Step 6:	If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $z \in \mathbb{R}$, then $x(y+z) = x \cdot y + x \cdot z$.	[Ax. DIS]
Step 7:	$1 \in \mathbb{R}$.	[Axiom 1R]
Step 8:	$2 \cdot (1 + 1) = 2 \cdot 1 + 2 \cdot 1$.	[From Steps 3, 7, 6]
Step 9:	$2 = 1 + 1$.	[D2]
Step 10:	$2 \cdot 2 = 2 \cdot 1 + 2 \cdot 1$.	[From Steps 8 and 9, via Rule SEE]
Step 11:	$2 \cdot 2 = 4$.	[From Steps 5 and 10, via Rule SEE]

END

PROBLEM 13: Prove that $(\forall x \in \mathbb{R})\, x.0 = 0$. (That is, prove that $x.0 = 0$ for every real number x, i.e., that if x is an arbitrary real number, then $x.0 = 0$.)

COMMENT: So far, we haven't mentioned 0*, so if we are going to prove something involving* 0 *we need axioms about* 0*.*

In addition, we need a few new axioms about addition, multiplication, and equality, and one new rule of inference

AXIOM 0R: 0 is a real number.

AXIOM 0A: If x is a real number, then $x + 0 = x$.

AXIOM MCl: (The closure axiom for multiplication) If x and y are real numbers, then xy is a real number.

AXIOM ACa: (The cancellation law for addition) If x, y, z are real numbers and $x + y = x + z$ then $y = z$.

AXIOM ER: (The reflexive property of equality) $(\forall x)\, x = x$.

RULE $\forall_{get}$: (The rule for proving a "for all ... " statement.) If you prove a statement $P(a)$ involving an arbitrary object a, where a is a letter that has not been used before in your proof, then you can conclude that $(\forall x)\, P(x)$.

PROBLEM 13, PRECISELY STATED: Prove that $(\forall x \in \mathbb{R})\, x.0 = 0$, using Axioms AA, 1R, ACl, DIS, 1M, 0R, 0A, MCl, ACa, ER, Definitions D2, D3, D4, Rules SEE and IMP$_{get}$, and all the statements proved before in Problems 11 and 12.

SOLUTION:

Step 1:	$0 \in \mathbb{R}$.	[Axiom 0R]
Step 2:	If $x \in \mathbb{R}$ then $x + 0 = x$.	[Axiom 0A]
Step 3:	$0 + 0 = 0$.	[From Steps 1 and 2]
Step 4:	If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $z \in \mathbb{R}$, then $x(y+z) = xy + xz$.	[Ax. DIS]
Step 5:	If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $z \in \mathbb{R}$, then $x + (y+z) = (x+y) + z$.	[Ax. AA]
Step 6:	If $x \in \mathbb{R}$ and $y \in \mathbb{R}$ then $xy \in \mathbb{R}$.	[Ax. MCl]
Step 7:	If $x \in \mathbb{R}$, $y \in \mathbb{R}$, $z \in \mathbb{R}$, and $x + y = x + z$ then $y = z$.	[Ax. ACa]
Step 8:	If x is arbitrary then $x = x$.	[Axiom ER]
Step 9:	Let $a \in \mathbb{R}$ be arbitrary.	[INT]
Step 10:	$a(0+0) = a \cdot 0 + a \cdot 0$.	[From Steps 1, 9, 4]
Step 11:	$a \cdot 0 = a \cdot 0 + a \cdot 0$.	[From Steps 3 and 9 via SEE]
Step 12:	$a \cdot 0 \in \mathbb{R}$.	[From Steps 1, 9, and 6]
Step 13:	$a \cdot 0 + 0 = a \cdot 0$.	[From Steps 2 and 12]
Step 14:	$a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$.	[From Steps 11 and 13 via SEE]
Step 15:	$0 = a \cdot 0$.	[From Steps 7, 14, 1 and 12]
Step 16:	$0 = 0$.	[From Step 8]
Step 17:	$a \cdot 0 = 0$.	[From Steps 15 and 16 via SEE]
Step 18:	$(\forall x \in \mathbb{R})\, x \cdot 0 = 0$.	[Rule $\forall_{get}$, from Steps 9 and 17]

END

3 More information on the course

3.1 Always bring the book to class!

In the lectures, we are going to spend a lot of time looking at the book and analyzing definitions, arguments and proofs given there. So

Please always bring the book to class! You are going to need it.

3.2 Homework assignment no. 2, due on Wednesday February 1

1. Book, Exercises 1.2. (pages 17-18-19-20): Problems 4 (non-starred items), 5 (non-starred items), 8 (non-starred items), 13 (non-starred items).

2. Book, Exercises 1.3. (pages 26-27-28): Problems 1 (non-starred items), 3, 5 (non-starred items), 6 (non-starred items), 7 (non-starred items).

3. Book, Exercises 1.4. (pages 37-38-39): Problem 5(b)(c).

4 Connectives and sentence structure

One can form new sentences from one or more given sentences by combining them using ***logical connectives***. Each logical connective admits a specified number of ***input sentences***. There are exactly ***seven*** logical connectives, each one of which is represented by a symbol, and has a name. Three of them admit ***one*** input sentence, and the other four take ***two*** input sentences.

4.1 The seven logical connectives

Here are the seven connectives, together with their symbols, number of inputs, and the way a sentence involving them must be read:

Symbol	Name	Number of arguments	Reading
$\sim$	negation	1	"$\sim A$" is read as "not A", or as "it is not the case that A"
$\vee$	disjunction	2	"$A \vee B$" is read as "A or B"
$\wedge$	conjunction	2	"$A \wedge B$" is read as "A and B"
$\Rightarrow$	implication	2	"$A \Rightarrow B$" is read as "if A then B" or as "A implies B"
$\Leftrightarrow$	biconditional	2	"$A \Leftrightarrow B$" is read as "A if and only if B"
$\exists$	existential quantifier	1	"$(\exists x)A$" is read as "there exists x such that A"
$\forall$	universal quantifier	1	"$(\forall x)A$" is read as "for all x, A", or as "for every x, A"

The first five (negation, disjunction, conjunction, implication, and biconditional) are the ***propositional connectives***.

The symbols $\exists$ and $\forall$ are the ***quantifiers***: " $\exists$ " is the ***existential quantifier***, and " $\forall$ " is the ***universal quantifier***.

A sentence of the form "$\sim A$" is a ***negation***. We read it as "it's not the case that A". Often, "$\sim A$" can also be read by inserting the word "not" somewhere in the middle of A. (For example, if A is the statement "7 is a prime number", then we can read $\sim A$ as "it's not the case that 7 is a prime number", but a much nicer reading would be "7 is not a prime number".)

A general remark about various ways to read a sentence: *Translation from mathematical language to English is like translation from some other foreign language to English. You first translate literally, word by word and symbol by symbol. But then, if you can think of another way to say the same thing in English which is nicer and simpler,* ***has exactly the same meaning****, and sounds more like English, then this second way is also O.K., and usually is much better.*

Example: The sentence

$$(\forall x)((x \in \mathbb{R} \wedge x \geq 0) \Rightarrow (\exists y \in \mathbb{R})y^2 = x)$$

can be read as

> For every x, if x is a real number and x is nonnegative, then there exists a real number y such that y-squared is equal to x.

This is a literal translation, and it's awful, like most literal transaltions. If, however, you think for a minute about what this sentence actually amounts to, you will see that you can say the same thing by just saying

> Every nonnegative real number has a real square root.

This is clearly much simpler and nicer, so it is a much better way to read our sentence.

A sentence of the form "$A \vee B$" is a ***disjunction***. We read it as "A or B". For example, if A is the statement "7 is a prime number", and B is the statement "7 is not prime", then we can read $A \vee B$ as "7 is prime or 7 is not prime" or, even better, "7 is prime or not", or "either 7 is prime or it isn't".

A sentence of the form "$A \wedge B$" is a ***conjunction***. We read it as "A and B". For example, if A is the statement "7 is a prime number", and B is the statement "8 is not prime", then we can read $A \wedge B$ as "7 is a prime number and 8 is not prime", In accordance with the "general principle" of

the previous box, it sounds nicer to say "7 is a prime number but 8 is not prime", so this second reading is also O.K., and probably even better.

A sentence of the form "$A \Rightarrow B$" is an ***implication***. We read it as "A implies B", or "if A then B", or "A entails B", or "B follows from A". For example, if A is the statement "7 is a prime number", and B is the statement "7 is not divisible by 3", then we can read $A \Rightarrow B$ as "if 7 is prime then 7 is not divisible by 3".

A sentence of the form "$A \Leftrightarrow B$" is a ***biconditional***. We read it as "A if and only if B". For example, if A is the sentence "$x \geq 0$", and B is the statement "x has a square root", then we can read $A \Leftrightarrow B$ as "if $x \geq 0$ then x has a square root".

A sentence of the form "$(\forall x)$A", where x is an individual variable, and A is a sentence, is a ***universal sentence***. We read it "For all x, A", or "for every x, A". We can also read it as "If x is arbitrary then A".

And, as explained before, after you have figured out how to read the sentence literally, it is usually better to reformulate it in a more English-sounding way.

Example 1. Consider the sentence

$$(\forall p \in \mathbb{N})((p \text{ is prime} \wedge p > 2) \Rightarrow p \text{ is odd}) .$$

How shall we read it?

ANSWER: a literal reading would be "for every natural number p, if p is prime and p is greater than 2, then p is odd". But it is much nicer, and better English, to say "every prime grater than two is odd". $\diamondsuit$

A sentence of the form "$(\exists x)A$" is an ***existential sentence***. We read it "There exists x such that A", or "there is an x such that A". We could also read it, if you wish, as "it is possible to pick an x such that A".

Example 2. The sentence

$$(\exists x)(x \text{ is a cow})$$

is read as

There exists an x such that x is a cow,

or, better yet,

There exists a cow,

or, even better,

Cows exist,

or

There are cows.

IMPORTANT! The 3-symbol string "$(\exists x)$" is read "there exists x such that," or "there exists an x such that," or "there is an x such that." Similarly, the string "$(\exists x \in \mathbb{R})$" is read "there exists a real number x such that," or "there is a real number such that." ***Do not forget the "such that."*** Students sometimes read "$(\exists x)$" as "there exists x and". This is wrong and could be very confusing. (Think about this, and ask the instructor if you don't see why "there exists x and" is bad.)

Example 3. The sentence

$$(\exists x)(x \text{ believes that Elvis is alive})$$

is read as

There exists an x such that x believes that Elvis is alive,

or, much more nicely,

Somebody believes that Elvis is alive.

Example 4. The sentence

$$(\exists x)(x \in \mathbb{R} \wedge x^2 = 2)$$

is read as

There exists an x such that x is a real number and x-squared is equal to 2,

or, much more nicely,

2 has a real square root.

When we write $(\forall x)A$***, does*** A ***have to contain*** x***?***
Usually, the sentence A will contain x. For example, A could be the sentence

$$x \in \mathbb{R} \Rightarrow x^2 \geq 0\,,$$

in which case $(\forall x)A$ is the sentence

$$(\forall x)(x \in \mathbb{R} \Rightarrow x^2 \geq 0)\,,$$

which is read as

> for every x, if x is a real number then x-squared is greater than or equal to zero,

or, even better

> for every real number x, x-squared is nonnegative,

or, better yet,

> The square of every real number is nonnegative.

(Notice that in this last reading the variable x completely disappears. This is consistent with the fact that the sentence $(\forall x)(x \in \mathbb{R} \Rightarrow x^2 \geq 0)$ is ***closed*** that is, is a sentence with no inputs at all, because the variable x that occurs in it is under the scope of a quantifier.)

However, there is no problem at all with a sentence such as $(\forall x)3 + 3 = 6$. This is a perfectly fine sentence (which happens to be true). In both cases, we figure out if the quantified sentence is true in the same way:

- If A is $x \in \mathbb{R} \Rightarrow x^2 \geq 0$, then to find out if $(\forall x)A$ is true, you have to look at all possible values of x, plug them into A, i.e., into $x \in \mathbb{R} \Rightarrow x^2 \geq 0$, and see if each of the sentences you get (such as, for example, $6 \in \mathbb{R} \Rightarrow 6^2 \geq 0$, $(-2) \in \mathbb{R} \Rightarrow (-2)^2 \geq 0$, (Ethel the frog) $\in \mathbb{R} \Rightarrow$ (Ethel the frog)$^2 \geq 0$, etc.), and see if in each case you get a true sentence. (The answer is "yes", you do. Why is the sentence "(Ethel the frog) $\in \mathbb{R} \Rightarrow$ (Ethel the frog)$^2 \geq 0$" true? Because "(Ethel the frog) $\in \mathbb{R}$" is false!)

- Similarly, if A is $3 + 3 = 6$, then to find out if $(\forall x)A$ is true, you have to look at all possible values of x, plug them into A, i.e., into $3 + 3 = 6$, and see if each of the sentences you get is true. The answer is "yes", because when you plug any object x into $3 + 3 = 6$ you always get $3 + 3 = 6$, which is true.

4.2 Atomic sentences

. A sentence that cannot be obtained from shorter sentences by means of connectives (that is, a sentence which is not a negation, a disjuction, a conjunction, an implication, a biconditional, or an existential or universal sentence) is called an ***atomic sentence***.

4.3 The eight types of sentences

.

Every mathematical sentence is of one of the following eight types:

negation ***disjunction***
conjunction ***implication***
biconditional ***existential***
universal ***atomic***

4.4 Propositional forms

If we start with a collection letters called "propositional variables" (usually, capital letters such as A, B, ..., or P, Q, R, ...) and combine then in various ways using the propositional connectives, we obtain expressions called ***propositional forms***. So, for example, the following are propositional forms, using the propositional variables A, B, C:

- A
- B
- $\sim A$
- $A \wedge B$
- $(A \wedge B) \vee C$
- $(A \wedge B) \vee A$
- $(A \wedge B) \vee (\sim (A \Rightarrow C))$
- $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$
- $(A \Rightarrow (B \Rightarrow C)) \Leftrightarrow ((A \wedge B) \Rightarrow C)$

We will give a precise definition of the notion of "propositional form" later. Notice that *not every string of symbols consisting of propositional variables and propositional connectives is a propositional form.* For example, here are some strings that are *not* propositional forms:

- $A \sim$
- AB
- $AB\vee$
- $(A\wedge)B$
- $A \wedge \vee B$

A question for you to think about. What would be a precise definition of "propositional form"? A good definition of "propositional form" should enable you to prove, for example, that $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$ is a propositional form but $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B)(B \Rightarrow A))$ is not.

Here is a different way to formulate this question: how would you write a computer program $\mathcal{P}$ such that, when you input into $\mathcal{P}$ a sequence of symbols which may be a propositional form or not (for example, the strings $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$ or $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B)(B \Rightarrow A))$), the program will produce the right answer to the question "is this string a propositional form?" (That is, you will get a "yes" answer if you input $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$, and a "no" answer if you input $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B)(B \Rightarrow A))$,

A definition of "propositional form" that cannot be translated into such a computer program is not a good definition. ***Think about this; we'll come back to it later.***

4.5 Truth tables

If a proposition P is obtained from other propositions by means of the propositional connectives, then we can decide if P is true or false by looking at the truth values of the propositions used to construct P. The rules for this are as follows:

The truth value of a negation. *If A is true then $\sim A$ is false. If A is false then $\sim A$ is true.* So the truth value of $\sim A$ is given in terms of the truth value of A by the following ***truth table***:

A	$\sim A$
T	F
F	T

The truth value of a disjunction. *If A and B are false then $A \vee B$ is false. In all other cases, $A \vee B$ is true.* So the truth value of $A \vee B$ is given in terms of the truth values of A and B by the following ***truth table***:

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

The truth value of a conjunction. *If A and B are true then $A \wedge B$ is true. In all other cases, $A \wedge B$ is false.* So the truth value of $A \wedge B$ is given in terms of the truth values of A and B by the following ***truth table***:

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

The truth value of an implication. *If A is true and B is false then $A \Rightarrow B$ is false. In all other cases, $A \Rightarrow B$ is true.* So the truth value of $A \Rightarrow B$ is given in terms of the truth values of A and B by the following ***truth table***:

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

The truth value of a biconditional. *If A and B are both true or both false then $A \Leftrightarrow B$ is true. If one of A, B is true and the other one is false, then $A \Leftrightarrow B$ is false.* So the truth value of $A \Leftrightarrow B$ is given in terms of the truth values of A and B by the following ***truth table***:

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

4.6 Do we need other connectives?

Suppose we wanted to have a connective $\veebar$ (called "exclusive or") such that $A \veebar B$ is true when *exactly one* of A, B is true and $A \veebar B$ is false when A and B are both true or both false. The truth table of such a connective would be

A	B	$A \veebar B$
T	T	F
T	F	T
F	T	T
F	F	F

If we wanted to, we could introduce such a connective, and then we would have six propositional connectives. This, however, is completely unnecessary, because we can say exactly the same thing as "$A \veebar B$" by just saying "$(A \vee B) \wedge (\sim (A \wedge B))$". Indeed, here is the truth table of the propositional form $(A \vee B) \wedge (\sim (A \wedge B))$.

A	B	$A \vee B$	$A \wedge B$	$\sim (A \wedge B)$	$(A \vee B) \wedge (\sim (A \wedge B))$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

As you can see, this is the same as the truth table of $A \veebar B$, in the sense that *for every choice of truth values for A and B the truth value of $(A \vee B) \wedge (\sim (A \wedge B))$ is the same as that of "$A \veebar B$".*

It turns out that this example illustrates a general truth: *any possible truth table you can manufacture, involving any number of propositional variables, can always be obtained using our five propositional connectives.*

4.7 Do we need all five propositional connectives?

The answer is "no". You can actually cut down the number of propositional connectives from five to two.

Example. Suppose we decide to use only $\sim$ and $\Rightarrow$. Can we say all the things that we can say using also $\vee$, $\wedge$ and $\Leftrightarrow$? The answer is "yes, we can". Here is how.

Instead of $A \vee B$, you can say $(\sim A) \Rightarrow B$. (Why? Because $(\sim A) \Rightarrow B$ is false in precisely one case, namely, when $\sim A$ is true and B, that is, when A and B are both false. And this is exactly the one and only case when $A \vee B$ is false.)

Instead of $A \wedge B$, you can say $\sim (A \Rightarrow (\sim B))$. (Why? Because $\sim (A \Rightarrow (\sim B))$ is true in only one case, namely, when $A \Rightarrow (\sim B)$ is false; this happens exactly when A is true and $\sim B$ is false, i.e., when when A and B are both true. And this is exactly the one and only case when $A \wedge B$ is true.)

Finally, instead of $A \Leftrightarrow B$, you can say $(A \Rightarrow B) \wedge (B \Rightarrow A)$, and then get rid of the $\wedge$ by saying $\sim ((A \Rightarrow B) \Rightarrow (\sim (B \Rightarrow A)))$.

Problem. Show that the two connectives $\sim$ and $\wedge$ suffice, in the sense that everything we can say using $\sim$, $\vee$, $\wedge$, $\Rightarrow$ and $\Leftrightarrow$ can be said using just $\sim$ and $\wedge$.

Problem. Show that the two connectives $\sim$ and $\Leftrightarrow$ do not suffice.

4.8 What are propositional forms good for?

Propositional forms can be used in two ways:

- as a way to ***abbreviate*** certain sentences;
- ***to represent the logical form of sentences on the level of the propositional calculus.***

Propositional forms as abbreviations. The first use is easy to explain: we can, for example, decide to use the letter A to stand for the sentence "Alice is a Democrat", and use B for the sentence "Alice is a Republican". Then, instead of writing, for example, "Alice is a Democrat and Alice is not a Republican", we can just write $A \wedge (\sim B)$. Similarly, instead of writing

$(\mathcal{S})$	If Alice is a Democrat or a Republican, and Alice is not a Democrat, then Alice is a Republican.

we could write $((A \vee B) \wedge (\sim A)) \Rightarrow B$.

Propositional forms as representations of logical forms of sentences. The second way sounds more complicated, so let us explain carefully what it means.

Take a propositional form such as $((A \vee B) \wedge (\sim A)) \Rightarrow B$. Let us call this particular propositional form $\mathcal{F}$. Now suppose we take two propositions,

such as "Alice is a Democrat" and "Alice is a Republican", and we plug them into $\mathcal{F}$ in place of A and B. We get the same sentence $(\mathcal{S})$ as above.

When a sentence is obtained from a propositional form $\mathcal{F}$ by plugging in sentences for the propositinal variables, we say that ***$\mathcal{F}$ is a propositional form of the sentence***, or that ***the sentence is of the form $\mathcal{F}$***, or that ***the sentence has the form $\mathcal{F}$***. For example: the sentence that we have called $(\mathcal{S})$ is of the form $((A \vee B) \wedge (\sim A)) \Rightarrow B$, because it can be obtained from $((A \vee B) \wedge (\sim A)) \Rightarrow B$ by plugging in "Alice is a Democrat" for A and "Alice is a Republican" for B.

Remark. ***A sentence typically has several different propositional forms.*** For example, let us look again at our sentence $(\mathcal{S})$. We can

- obtain $(\mathcal{S})$ from $((A \vee B) \wedge (\sim A)) \Rightarrow B$ by plugging in "Alice is a Democrat" for A and "Alice is a Republican" for B,

but we can also, for example,

- obtain $(\mathcal{S})$ from $((A \vee B) \wedge C \Rightarrow B$ by plugging in "Alice is a Democrat" for A, "Alice is a Republican" for B, and "Alice is not a Democrat" for C,
- obtain $(\mathcal{S})$ from $A \Rightarrow B$ by plugging in "Alice is a Democrat or a Republican and Alice is not a Democrat" for A, and "Alice is a Republican" for B,
- obtain $(\mathcal{S})$ from $(A \wedge B) \Rightarrow C$ by plugging in "Alice is a Democrat or a Republican" for A, "Alice is not a Democrat" for B, and "Alice is a Republican" for C,
- obtain $(\mathcal{S})$ from $A \Rightarrow B$ by plugging in "Alice is a Democrat or a Republican and Alice is not a Democrat" for A, and "Alice is a Republican" for B,
- obtain $(\mathcal{S})$ from A by plugging in "If Alice is a Democrat or a Republican, and Alice is not a Democrat, then Alice is a Republican" for A.

Hence $(\mathcal{S})$ has at least the following five propositional forms:

(1) $((A \vee B) \wedge (\sim A)) \Rightarrow B$,

(2) $((A \vee B) \wedge C \Rightarrow B$,

(3) $(A \wedge B) \Rightarrow C$,

(4) $A \Rightarrow B$.

(5) A.

4.9 Tautologies and contradictions

Definition. A ***tautology*** is a propositional form P whose truth value is T for all possible choices of truth values for the propositional variables that occur in P. $\diamondsuit$

Definition. A ***contradiction*** is a propositional form P whose truth value is F for all possible choices of truth values for the propositional variables that occur in P. $\diamondsuit$

Definition. An ***instance of a tautology*** is a sentence that has a propositional form which is a tautology. $\diamondsuit$

Definition. An ***instance of a contradiction*** is a sentence that has a propositional form which is a contradiction. $\diamondsuit$

Example 1. The propositional form $A \vee (\sim A)$ is a tautology. You can prove this by writing out the truth table, but it is much easier to observe that the truth values of A and $\sim A$ are always going to be opposite, so one of them is going to be T, and then $A \vee (\sim A)$ is true. So $A \vee (\sim A)$ is always true.

Example 2. The propositional form $A \wedge (\sim A)$ is a contradiction. You can prove this by writing out the truth table, but it is much easier to observe that the truth values of A and $\sim A$ are always going to be opposite, so one of them is going to be F, and then $A \wedge (\sim A)$ is false. So $A \vee (\sim A)$ is always false.

Example 3. The sentence "Either Elvis is alive or he is not" is an instance of a tautology, because it is of the form $A \vee (\sim A)$, and $A \vee (\sim A)$ is a tautology.

Example 4. The sentence "Elvis is alive and he isn't" is an instance of a contradiction, because it is of the form $A \wedge (\sim A)$, and $A \wedge (\sim A)$ is a contradiction.

Example 5. The propositional form

$$(A \Rightarrow (B \Rightarrow (C \Rightarrow D))) \Rightarrow (((A \wedge B) \wedge C) \Rightarrow D)$$

is a tautology. You can prove this by writing out the truth table. (Just give it a try!) But it is much easier to reason as follows.

Let us use P as a name for our propositional form. How could P be false? Well, P is an implication, so P can only be false when the premiss of the implication is true and the conclusion is false.

More precisely, P is $Q \Rightarrow R$, where Q is $A \Rightarrow (B \Rightarrow (C \Rightarrow D))$ and R is $((A \wedge B) \wedge C) \Rightarrow D$. Suppose P is false. Then Q is true and R is false .But R is $((A \wedge B) \wedge C) \Rightarrow D$, so $(A \wedge B) \wedge C$ is true and D is false. Since $(A \wedge B) \wedge C$ is true, it follows that $A \wedge B$ is true and C is true. Since $A \wedge B$ is true, we can conclude that A is true and B is true. So we have shown (assuming that P is false) that A, B and C are true, and D is false. Since C is true and D is false, the implication $C \Rightarrow D$ is false. Since B is true and $C \Rightarrow D$ is false, the implication $B \Rightarrow (C \Rightarrow D)$ is false. Since A is true and $B \Rightarrow (C \Rightarrow D)$ is false, the implication $A \Rightarrow (B \Rightarrow (C \Rightarrow D))$ is false. So Q is false. But this is impossible because we have shown that Q is true. So the assumption that P is false has led us to an impossible conclusion. Hence P cannot be false. So P is always true.

Example 6. The propositional form

$$((A \wedge B) \wedge (C \wedge D)) \wedge (((\sim A) \vee (\sim B)) \vee ((\sim C) \vee (\sim D)))$$

is a contradiction. You can prove this by writing out the truth table. But it is much easier to reason as follows.

Let us use P as a name for our propositional form. P is a conjunction $Q \wedge R$, where Q is $(A \wedge B) \wedge (C \wedge D)$ and R is $((\sim A) \vee (\sim B)) \vee ((\sim C) \vee (\sim D))$. Assume P is true. Then Q and R are both true. But Q is the conjunction of A, B, C and D, so A, B, C and D are all four true. This means that $\sim A$, $\sim B$, $\sim C$ and $\sim D$ are all four false. On the other hand, R is the disjunction of $\sim A$, $\sim B$, $\sim C$ and $\sim D$. Since $\sim A$, $\sim B$, $\sim C$ and $\sim D$ are false, it follows that R is false. But this is impossible because we have shown that R is true. So the assumption that P is true has led us to an impossible conclusion. Hence P can never be true. So P is always false.

Example 7. The propositional form

$$A \Rightarrow (\sim A)$$

is neither a tautology nor a contradiction. Indeed, if A is true then $\sim A$ is false, so $A \Rightarrow (\sim A)$ is false. On the other hand, if A is false then $A \Rightarrow (\sim A)$ is true. So $A \Rightarrow (\sim A)$ is neither "always true" nor "always false".

Remark. *What is the point of including the above example?* It's very simple. My experience teaching this course tells me that, when I ask this question in one of the midterms, about 90% of the students say that $A \Rightarrow (\sim A)$ is a contradiction. *If you don't believe me, wait until after the first midterm, and then we will talk again.*

An important remark on the definition of "tautology" and "contradiction". You should ***never*** write things such as a "a tautology is a true statement", or "a tautology is a statement that is always true". For example, "H. J. Sussmann is the greatest teacher in the universe" is (evidently!) a true statement, but it is definitely *not* a tautology, or even an instance of a tautology. Furthermore, for a statement, or proposition, what could it possibly mean to say that it is "always" true? A statement is true or false, but what does it means to say that it is "always true" as opposed to just being "true"?

"Always true" is the kind of property that does not make sense for *statements*. It does, however, make sense for things that have the form of statements but are made of *propositional variables* instead of statements, so we can *vary* the actual statements we plug in, and in particular we can vary the truth values of these statements. For example, in the propositional form $A \vee (\sim A)$ we can plug in "Elvis is alive" (which is false) for A, and we can also plug in "Mozart loved music", which is true. In either case, the statement we get ("Elvis is alive or he isn't", "Mozart loved music or he didn't") is true. That's what why we say of the *propositional form* "$A \vee (\sim A)$" that it is "always true", whereas it would not make sense to say of the true statement "Mozart loved music" that is is "always true." This statement is just true, but not "always" true.

Naturally, similar remarks apply to contradictions. You should ***never*** write things such as a "a contradiction is a false statement", or "a contradiction is a statement that is always false". (For example, "$1 = 0$" is just false, but is not a contradiction. On the other hand, the sentence "$1 = 0 \wedge (\sim 1 = 0)$" is a contradiction.)

4.10 Restricted (a.k.a. conditional) quantifiers

It would be very silly to say $(\forall x)x^2 \geq 0$, because if we take this literally (as we always should, in mathematics!) then this says that "the square of every object in the universe is nonnegative". In particular, this would say that "the square of Elvis is nonnegative", "the square of the planet Jupiter is nonnegative", and lots of other truly stupid things. What you really want to say is "the square of every real number is nonnegative". To say this, we use a ***restricted universal quantifier*** instead of a universal quantifier. That is, we write $(\forall x \in \mathbb{R})x^2 \geq 0$. We read this as

> For all real numbers x, x-squared is greater than or equal to zero

or, even better, as

> The square of every real number is nonnegative.

An expression of the form $(\forall\xi)$, where ξ is a variable[4], or of the form $(\forall\xi\mathcal{C})$, where ξ is a variable and $\mathcal{C}$ is a condition such as "$\in \mathbb{R}$", or "$\in \mathbb{N}$", or "$\in \mathbb{Z}$", or "$\in \mathbb{Q}$", is a ***universal quantifier***. A universal quantifier of the form $(\forall\xi)$ is an ***unrestricted universal quantifier***, while one of the form $(\forall\xi\mathcal{C})$ is a ***restricted*** or ***conditional universal quantifier***.

If we take a sentence $\mathcal{A}$ and add a quantifier $(\forall\xi)$ or $(\forall x\mathcal{C})$ to its left, we have ***universally quantified*** $\mathcal{A}$. For example, from the sentence $x^2 \geq 0$, we can get $(\forall x)\, x^2 \geq 0$, or $(\forall x \in \mathbb{R})\, x^2 \geq 0$.

An ***existential quantifier*** is an expression of the form $(\exists\xi)$, where ξ is a variable, or of the form $(\exists\xi\mathcal{C})$, where ξ is a variable and $\mathcal{C}$ is a condition such as "$\in \mathbb{R}$", or "$\in \mathbb{N}$", or "$\in \mathbb{Z}$", or "$\in \mathbb{Q}$". A quantifier of the form $(\exists\xi)$ is an ***unrestricted existential quantifier***, while one of the form $(\exists\xi\mathcal{C})$ is a ***restricted*** or ***conditional existential quantifier***.

If we take a sentence $\mathcal{A}$ and add a quantifier $(\exists x)$ or $(\exists x\mathcal{C})$ to its left, we have ***existentially quantified*** $\mathcal{A}$. For example, from the sentence $y^2 = x$ we can get $(\exists y)\, y^2 = x$, or $(\exists y \in \mathbb{R})\, y^2 = x$, $(\exists x)\, y^2 = x$, or $(\exists x \in \mathbb{R})\, y^2 = x$.

4.11 Building and parsing sentences

The operations of negation, disjunction, conjunction, implication, biconditional, existential and universal quantification can be applied repeatedly, to

[4]Notice that here I am using the symbol ξ as a "variable whose values are variables". That is, when I say that "ξ is a variable" is say that ξ could be x, or y, or z, or w, or a, for example. So the quantifier $(\forall\xi)$ could be, for example, $(\forall x)$ or $(\forall y)$.

construct complex sentences starting from simple ones.

A simple example. Let us start with the atomic sentence

$$y^2 = x\,,$$

We can existentially quantify it to obtain

$$(\exists y \in \mathbb{R})\, y^2 = x\,,$$

then take the sentence

$$x \geq 0$$

and combine it with $(\exists y \in \mathbb{R})\, y^2 = x$ via implication, which results in

$$x \geq 0 \Rightarrow (\exists y \in \mathbb{R})\, y^2 = x\,,$$

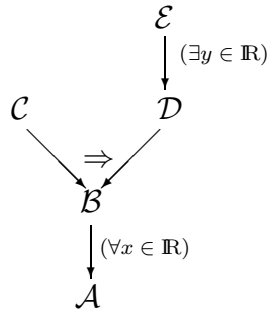
and, finally, universally quantify this, obtaining a statement

$$(\forall x \in \mathbb{R})(x \geq 0 \Rightarrow (\exists y \in \mathbb{R})\, y^2 = x)\,.$$

that we will call $\mathcal{A}$. (NOTE: This $\mathcal{A}$ says "every nonnegative real number has a square root".)

We can describe the structure and construction of $\mathcal{A}$ by means of a diagram, in which the letters $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ stand for sentences as follows:

$\mathcal{B}$ stands for $x \geq 0 \Rightarrow (\exists y \in \mathbb{R})\, y^2 = x$,
$\mathcal{C}$ stands for $x \geq 0$
$\mathcal{D}$ stands for $(\exists y \in \mathbb{R})\, y^2 = x$,
$\mathcal{E}$ stands for $y^2 = x$.



This diagram can be viewed in two ways:

- If we read it from top to bottom, the diagram tells us how, starting from the atomic sentence $\mathcal{E}$, the sentence $\mathcal{A}$ is constructed by successively combining sentences using connectives.
- If we read it from the $\mathcal{A}$ node up, it tells us how to ***parse*** the sentence $\mathcal{A}$, by displaying its structure.

We now look at a more complicated example of parsing a sentence.

A harder example. Let us parse the sentence[5]

$$\boxed{(\exists L \in \mathbb{R})(\forall \varepsilon \in \mathbb{R})(\varepsilon > 0 \Rightarrow (\exists \delta \in \mathbb{R})(\delta > 0 \wedge (\forall x \in \mathbb{R})(0 < |x-a| < \delta \Rightarrow |x^2 - L| < \varepsilon)))}$$

(NOTE: The expression "$0 < |x - a| < \delta$" is an abbreviation of "$0 < |x - a| \wedge < |x - a| < \delta$".)

Step 1. Let us use $\mathcal{A}$ as a name for our sentence. Then $\mathcal{A}$ is of the form

$$(\exists L \in \mathbb{R})\mathcal{B}\,,$$

where $\mathcal{B}$ is the sentence

$$(\forall \varepsilon \in \mathbb{R})(\varepsilon > 0 \Rightarrow (\exists \delta \in \mathbb{R})(\delta > 0 \wedge (\forall x \in \mathbb{R})(0 < |x - a| < \delta \Rightarrow |x^2 - L| < \varepsilon)))$$

In particular, $\mathcal{A}$ ***is an existential sentence***.

Step 2. $\mathcal{B}$ is of the form

$$(\forall \varepsilon \in \mathbb{R})\mathcal{C}\,,$$

where $\mathcal{C}$ is the sentence

$$\varepsilon > 0 \Rightarrow (\exists \delta \in \mathbb{R})(\delta > 0 \wedge (\forall x \in \mathbb{R})(0 < |x - a| < \delta \Rightarrow |x^2 - L| < \varepsilon))\,.$$

In particular, $\mathcal{B}$ ***is a universal sentence***.

Step 3. $\mathcal{C}$ is of the form

$$\mathcal{D} \Rightarrow \mathcal{E}$$

where $\mathcal{D}$ is the sentence

$$\varepsilon > 0$$

and $\mathcal{E}$ is the sentence

$$(\exists \delta \in \mathbb{R})(\delta > 0 \wedge (\forall x \in \mathbb{R})(0 < |x - a| < \delta \Rightarrow |x^2 - L| < \varepsilon))\,.$$

In particular, $\mathcal{C}$ ***is an implication***.

Step 4. $\mathcal{D}$ ***atomic***, so it cannot be broken up into smaller pieces.

Step 5. $\mathcal{E}$ is of the form

$$(\exists \delta \in \mathbb{R})\mathcal{F}$$

where $\mathcal{F}$ is the sentence

$$\delta > 0 \wedge (\forall x \in \mathbb{R})(0 < |x - a| < \delta \Rightarrow |x^2 - L| < \varepsilon)\,.$$

In particular, $\mathcal{E}$ ***is an existential sentence***.

[5] As we will see later, this sentence says that "$\lim_{x \to a} x^2$ exists".

Step 6. $\mathcal{F}$ is of the form

$$\mathcal{G} \wedge \mathcal{H}$$

where $\mathcal{G}$ is the sentence

$$\delta > 0\,,$$

and $\mathcal{H}$ is the sentence

$$(\forall x \in \mathbb{R})(0 < |x - a| < \delta \Rightarrow |x^2 - L| < \varepsilon)\,.$$

In particular, $\mathcal{F}$ ***is a conjunction***.

Step 7. $\mathcal{G}$ ***is atomic***, so it cannot be broken up into smaller pieces.

Step 8. $\mathcal{H}$ is of the form

$$(\forall x \in \mathbb{R})\mathcal{I}$$

where $\mathcal{I}$ is the sentence

$$0 < |x - a| < \delta \Rightarrow |x^2 - L| < \varepsilon\,.$$

In particular, $\mathcal{H}$ ***is a universal sentence***.

Step 9. $\mathcal{I}$ is of the form

$$\mathcal{J} \Rightarrow \mathcal{K}$$

where $\mathcal{J}$ is the sentence

$$0 < |x - a| < \delta\,,$$

that is, the sentence

$$0 < |x - a| \wedge |x - a| < \delta\,,$$

and $\mathcal{K}$ is the sentence

$$|x^2 - L| < \varepsilon\,.$$

In particular, $\mathcal{I}$ ***is an implication***.

Step 10. $\mathcal{J}$ is of the form

$$\mathcal{L} \wedge \mathcal{M}$$

where $\mathcal{L}$ is the sentence

$$0 < |x - a|\,,$$

and $\mathcal{M}$ is the sentence

$$|x - a| < \delta\,.$$

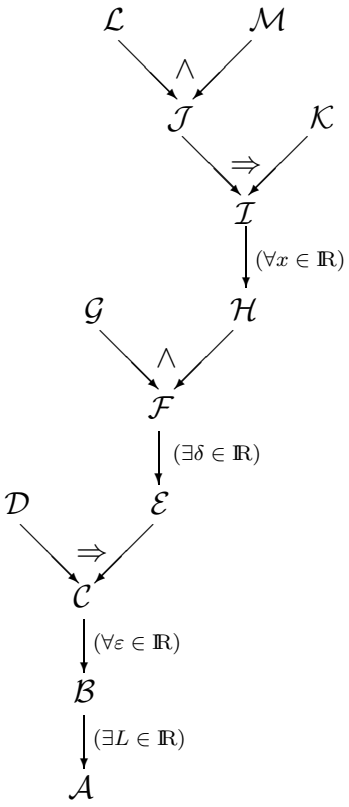
In particular, $\mathcal{J}$ ***is a conjunction***.

Step 11. $\mathcal{L}$ ***is atomic***, so it cannot be broken up into smaller pieces.

Step 12. $\mathcal{M}$ ***is atomic***, so it cannot be broken up into smaller pieces.

Step 13. $\mathcal{K}$ ***is atomic***, so it cannot be broken up into smaller pieces.

The following diagram shows the structure of $\mathcal{A}$, by telling us how $\mathcal{A}$ is constructed by combining the atomic sentences $\mathcal{D}$, $\mathcal{G}$, $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{K}$ by means of logical connectives.



4.12 Some parsing problems.

Now I am now going to write three parsing problems for you to solve. But first you should read the following explanantion.

In the following three sentences, "Pr(n)" means "n is prime" (no matter what n is; in particular, "Pr(p)" means "p is prime".). Also, $GCD(a, b)$ means "the greatest common divisor of a and b".

$$(\forall p \in \mathbb{Z})(\mathrm{Pr}(p) \Leftrightarrow (p > 1 \wedge (\sim ((\exists a \in \mathbb{Z})(\exists b \in \mathbb{Z})(p = ab \wedge (a > 1 \wedge b > 1))))))$$

$$(\forall p{\in}\mathbb{Z})(\mathrm{Pr}(p) \Rightarrow (\forall a{\in}\mathbb{Z})(\forall b{\in}\mathbb{Z})((\exists k{\in}\mathbb{Z})ab = kp \Rightarrow ((\exists k{\in}\mathbb{Z})a = kp \vee (\exists k{\in}\mathbb{Z})b = kp)))$$

$$\begin{gathered}(\forall n{\in}\mathbb{Z})(\forall a{\in}\mathbb{Z})(\forall b{\in}\mathbb{Z})(((\sim a = 0){\vee} \sim b = 0) \Rightarrow (n = GCD(a,b) \Leftrightarrow \\ ((n > 0 \wedge ((\exists k \in \mathbb{Z})a = kn \wedge (\exists k \in \mathbb{Z})b = kn)) \wedge (\forall m{\in}\mathbb{Z})(((\exists k \in \mathbb{Z}) \\ a = km \wedge (\exists k \in \mathbb{Z})b = km) \Rightarrow m \leq n))))\end{gathered}$$

The first sentence is the definition[6] of "prime number". It says that

- if p is an arbitary integer, then p is ***prime*** if and only if
  - $p > 1$,
  - there do not exist two integers that are both greater than and are such that their product is p.

Notice that in this "translation into plain English" the letter symbols a and b do not occur. This is in perfect agreement with the fact that our definition says that p is prime if and only if something about p is true, and this "something about p" is the sentence

$$p > 1 \wedge (\sim ((\exists a \in \mathbb{Z})(\exists b \in \mathbb{Z})(p = ab \wedge (a > 1 \wedge b > 1)))) \ ,$$

which is a ***one input predicate***, whose only open variable is p. (The letters a and b are ***bound variables***, because they appear inside the scope of the quantifiers $(\exists a \in \mathbb{Z})$ and $(\exists b \in \mathbb{Z})$.) Hence in our first sentence the variables a and b "aren't really there, so it has to be possible to read it without using a and b.

How about p? Well, in the sentence

$$\mathrm{Pr}(p) \Leftrightarrow (p > 1 \wedge (\sim ((\exists a \in \mathbb{Z})(\exists b \in \mathbb{Z})(p = ab \wedge (a > 1 \wedge b > 1))))) \quad (4.12.1)$$

the letter p is an *open variable*, so this sentence really talks about p, and we cannot read it without using p. On the other hand, our first sentence is obtained from (4.12.1) by universally quantifying with respect to p. So the first sentence is closed, and it should be possible to translate it into English without using the letter p either. And, indeed, here is how you can do it:

[6] Or, better yet, one possible definition

> *An integer is prime if and only if it is greater than* 1 *and cannot be expressed as the product of two integers both of which are greater than* 1.

The second sentence makes an assertion about prime numbers. It says that

- if p is an arbitary integer, then
  - ∗ if p is prime, then
    - – if a, b are any two integers such that the product ab is divisible by p, then either a or b must be divisible by p.

Notice that this sentence is closed, that is, it is a ***proposition***, since each of the four variables that occur in it (that is, a, b, k and p) is always inside the scope of a corresponding quantifier.

Since this sentence has zero inputs, it ought to be possible to translate it into a statement without any letter variables. And, indeed, here is the translation:

> *If a prime number divides the product of two integers, then it must divide one of them*

The third sentence is the definition of "greatest common divisor" of two integers that are not both zero[7]. It says that

- if n, a, b are arbitary integers, then
  - ∗ if a or b is nonzero, then
    - # n is the greatest common divisor of a and b if and only if
      - a and b are divisible by n

      and
      - if m is any integer such that both a and b are divisible by m, then $m \leq n$.

Parsing problems. Parse the three boxed sentences of page 35.

A translation problem. Translate the third sentence into an English sentence without letter variables.

[7]Why do we require that the integers should not be both zero? What would happen if we try to take $a =$ and $b = 0$, and insist on defining $GCD(0, 0)$?

5 Three important announcements (Feb. 1)

5.1 Change in office hours

From now, my office hours on Wednesday are going to be: 1:20 to 2:50 pm. The Monday office hours remained unchanged, 1:00 to 2:30 pm.

5.2 Change in due date for Homework No. 2

Homework no. 2 should be handed in on Monday February 6, rather than on Wednesday February 1.

5.3 Trouble with Homework No. 1

More than half of the students had Homework No. 1 marked "unacceptable" and will get it back unread. The reason is that the students violated the rules clearly specified in the notes, page 6. **Please do not make this mistake again!**

6 Homework assignment no. 3, due on Wednesday February 8

1. Book, Exercises 1.4. (pages 37-38-39): Problems 6(a)(b)(e), 7(g)(i)(j)(k), 11(b).

2. Book, Exercises 1.5. (pages 44-45-46): Problems 3(f)(g)(h), 6(a)(d), 9, 10, 12(a)(c)(d).

3. Do the parsing problems stated on Page 36 of the notes. That is, parse the three boxed sentences of page 35.

7 The rules for formal proofs

A ***formal proof*** is a list of ***steps***, each one of which consists of a ***statement*** (i.e., a closed sentence) accompanied with a ***justification***. The justification of a step consists of a reason showing why the statement in that step follows

according to the rules), given the previous steps. The last step of a proof is called the ***conclusion***.

To ***prove*** a statement S using certain ***input statements*** means ***to produce a proof whose conclusion is*** S, in which each step is either an input statement or follows by the ***rules of inference***.

So, to be able to write a proof, one needs to know which are the input statements and which are the rules of inference.

7.1 Which statements are valid input statetements?

The following are input statements that can be brought into a proof at any time.

(V.1) ***axioms*** (also known as "postulates");

(V.2) ***definitions***;

(V.3) the ***hypotheses***;

(V.4) anything else that you are allowed to use; this may include

- statements that have already been proved before,
- statements that may not have been proved before but you are explicitly authorized to use.

(V.5) In addition, it is always permitted to start a proof within a proof in the following ways:

(a) by introducing any sentence you want as an ***assumption*** (for example, "Assume pigs can fly", or "Assume $1 > 01$", or "Assume $1 < 0$", or "Assume that Aunt Ethel is a frog", or "Assume that Elvis is alive".)

or

(b) by ***declaring a new letter*** (such as a or x or n or α or $\aleph$) or ***variable symbol*** (such as x_1 or $\bar{k}$) to have a particular value, which will be treated as a ***constant*** (that is, a fixed object) within the "proof within a proof". This value is ***an object which is completely arbitrary within a specified range***, that is, an object which is arbitrary within the set of all objects that satisfy some condition.

7.1.1 How do we start a "proof within a proof" by declaring a value for a letter or variable symbol?

Suppose we want to declare a value for a letter or variable symbol ξ that will be required to satisfy a condition $\mathcal{C}(\xi)$. Then we could write:

$$\text{Let } \xi \text{ be arbitrary such that } \mathcal{C}(\xi) \ .$$

or

$$\text{Let } \xi \text{ be such that } \mathcal{C}(\xi) \ .$$

or

$$\text{Pick a } \xi \text{ such that } \mathcal{C}(\xi) \ .$$

The condition $\mathcal{C}(\xi)$ can be void[8] (that is, no condition at all), in which case we would just say something like

$$\text{Let } a \text{ be arbitrary.}$$

or, at the other extreme, it can be so restrictive that only one object can satisfy it, in which case we would say things like

$$\text{Let } a = \sqrt{3} \ .$$

(instead of saying "Let a be such that $a = \sqrt{3}$."), or

$$\text{Let } \alpha = (a + 7b)^2 - c \ .$$

(instead of saying "Let α be such that $\alpha = (a + 7b)^2 - c$.").

In between those extreme cases, there is the more general situation when the value is declared to be an object that satisfies a condition that can actually be true of more than one object. In that case, you would say things such as

[8] If you don't feel comfortable with a void condition, you may equally well take as the condition something that every entity will have to satisfy, for example $\xi = \xi$.

Let n be an arbitrary integer.	[1.a]
Let n be an integer.	[1.b]
Pick an integer and call it n.	[1.c]
Pick an arbitrary integer and call it n.	[1.d]
Choose an arbitrary integer and call it n.	[1.e]
Let $x \in \mathbb{Z}$ be such that $x^3 + x > 5$.	[2.a]
Let x be an integer such that $x^3 + x > 5$.	[2.b]
Let x be an arbitrary integer such that $x^3 + x > 5$.	[2.c]
Pick an $x \in \mathbb{Z}$ be such that $x^3 + x > 5$.	[2.d]
Pick an integer x such that $x^3 + x > 5$.	[2.e]
Let $x \in \mathbb{R}$ be such that $x^2 = 3$.	[3.a]
Let x be a real number such that $x^2 = 3$.	[3.b]
Let x be a real solution of the equation $x^2 = 3$.	[3.c]
Pick an $x \in \mathbb{R}$ such that $x^2 = 3$.	[3.d]
Pick a real number x such that $x^2 = 3$,	[3.e]
Pick a real solution x of the equation $x^2 = 3$,	[3.f]
Let $x \in \mathbb{R}$ be such that $x^2 + 1 = 0$	[4.a]
Let x be a real number such that $x^2 + 1 = 0$	[4.b]
Let x be a real solution of the equation $x^2 + 1 = 0$	[4.c]
Pick an $x \in \mathbb{R}$ such that $x^2 + 1 = 03$	[4.d]
Pick a real number x such that $x^2 + 1 = 0$,	[4.e]
Pick a real solution x of the equation $x^2 + 1 = 0$,	[4.f]

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 tell us how to get out from a proof within a proof and go back to the main proof. (The rules that allow us to do this are: Rules 2, 8, 12, and 13.)

7.1.2 What is the difference between "let" and "pick"?

"Let" and "pick" are basically the same. However, I would recommend that you use "let" when you are ***imagining*** someone introducing something and giving it a name, and that you use "pick" you know that an object of the specified kind exists, and you think of yourself as going where those objects are and picking one. For example, if you say "let x be a cow" you are imagining that our CAT (creator of arbitrary things) found a cow somewhere and is holding it. You could equally well have said "let x be a unicorn", or "let x be a round square", or "let x be a six-legged elephant". It doesn't

matter whether cows, unicorns, round squares, and six-legged elephants exist, because one can always imagine that they do even if they do not. (In fact, in mathematics you often imagine objects that do not exist, and you do that imagining precisely in order to prove that they do not exist. For example, you may say "let x be a real number such that $x^2+1=0$", and then conclude that $x^2+1>0$, so $0>0$, which is not true. Hence you end up concluding that ***an*** $x \in \mathbb{R}$ ***such that*** $x^2+1=0$ ***cannot exist***, and the way you proved this was by imagining that one such x exists and showing that the imaginary world where this happens is an impossible world, because in such a world we would have to have $0>0$.)

On the other hand, when you say "pick a cow and call her Clarabelle", you are doing the picking, and you are only authorized to do it if you know that there are cows. You would ***not*** be able to say "pick a real number x such that $x^2+1=0$", because you do not know that there are such numbers.

There is, however, one important exception[9] to the above. When you take a fixed object with a complicated name, and decide to call it by a simpler name (say, a letter), you use "let". For example, you would say

> Let $a=\sqrt{2}+\sqrt{3}$. Then $a^2=2+3+2\sqrt{6}=5+2\sqrt{6}$. So $a^2-5=2\sqrt{6}$, and then $(a^2-5)^2=4\cdot 6=24$, that is, $a^4-10a^2+25=24$, so $a^4-10a^2+1=0$, proving that $(\exists x \in \mathbb{R})x^4-10x^2+1=0$.

7.1.3 How come we are allowed to assume anything we want?

The issue of proofs within proofs is very important, and we will have a lot more to say about it later. But at this point I wish to insist on two things:

- first, ***you can introduce anything you want as an assumption***, for example that "pigs can fly", or "$1<0$", or "$\sqrt{2}$ is rational", or "Aunt Ethel is a frog", or "Elvis is alive".

But

[9]Sorry about this. I did not invent mathematical language. Like English, mathematical language is the product of a centuries-long evolution, so the rules governing it have lots of exceptions. If this bothers you, think how much worse ordinary English is. (For example, what is the rule for forming the plural of a noun? How come we say "oxen" but we say "foxes", not "foxen"? How come we say "mice" but we say "houses", not "hice"? How come the plural of "sheep" is "sheep", not "sheeps"? What is the rule? Try and figure it out!!!!!

- what you prove is only valid in the "proof within a proof", that is, ***under the assumption you introduced***. To get out of a proof within a proof you have to apply one of the rules that allow you to do so, that is, Rules 2, 8, 12, and 13.)

For example, if you assume that "pigs can fly", as you are certainly permitted to do, then you can prove things under this assumption. For instance, you may be able to prove that "pigs have wings." However, you cannot just claim that you have proved that pigs have wings. ***You have only proved that pigs have wings under the assumption that pigs can fly.*** That is, you proved that pigs have wings in an imaginary world in which pigs can fly. Does that enable us to say something about the real world? Yes, it does, but what we can say is very little. Rule $\Longrightarrow_{get}$ will enable to conclude, for the "real world", that "if pigs can fly then pigs have wings", as follows:

Assume that pigs can fly
⋮
Pigs have wings.

If pigs can fly then pigs have wings.

You still cannot conclude that pigs have wings, since you do not know that pigs can fly. If you knew that pigs can fly, then you could use Rule $\Longrightarrow_{use}$ to infer that pigs have wings:

If pigs can fly then pigs have wings.
Pigs can fly.

Pigs have wings.

So in that case your complete proof that "pigs have wings" would go as follows:

Assume that pigs can fly
⋮
Pigs have wings.
If pigs can fly then pigs have wings.
Pigs can fly.
Pigs have wings.

Notice that

Proving that pigs have wings under the assumption that pigs can fly is very different from proving that pigs have wings.

7.2 The fourteen basic rules of inference.

Here are the basic rules of inference. You will see that there are exactly ***fourteen*** of them. We could get away with fewer rules but these fourteen rules are very easy to remember, so I very much prefer to have them this way.

RULE 1. (***The tautology proof rule***.) You are allowed to bring in any statement which is an instance of a tautology.

RULE 2. (The ***proof by contradiction*** rule.) This rule really has two parts:

(2.a) If, assuming $\sim P$, you get to C, and C is an instance of a contradiction, then you can go to P.

$$\begin{array}{l} \text{Assume } \sim P \\ \quad \vdots \\ C \qquad [\textit{contradiction}] \\ \hline P \end{array}$$

(2.b) If, assuming P, you get to C, and C is an instance of a contradiction, then you can go to $\sim P$.

$$\begin{array}{l} \text{Assume } P \\ \quad \vdots \\ C \qquad [\textit{contradiction}] \\ \hline \sim P \end{array}$$

RULE 3. (Rule $\vee_{use}$, a.k.a. ***proof by cases***.) If you have $P \vee Q$ and $P \Rightarrow R$ and $Q \Rightarrow R$ then you can go to R:

$$\begin{array}{l} P \vee Q \\ P \Rightarrow R \\ Q \Rightarrow R \\ \hline R \end{array}$$

RULE 4. (Rule $\vee_{get}$.) This is also a two-part rule:

(4.a) If you have P then you can go to $P \vee Q$;

$$\begin{array}{l} P \\ \hline P \vee Q \end{array}$$

(4.b) If you have Q then you can go to $P \vee Q$:

$$\begin{array}{l} Q \\ \hline P \vee Q \end{array}$$

RULE 5. (Rule $\wedge_{use}$.) This is another two-part rule:

(5.a) If you have $P \wedge Q$ then you can go to P:

$$\begin{array}{l} P \wedge Q \\ \hline P \end{array}$$

(5.b) Iif you have $P \wedge Q$ then you can go to Q:

$$\begin{array}{l} P \wedge Q \\ \hline Q \end{array}$$

RULE 6. (Rule $\wedge_{get}$.) If you have P and Q then you can go to $P \wedge Q$.

$$\begin{array}{l} P \\ Q \\ \hline P \wedge Q \end{array}$$

RULE 7. (Rule $\Rightarrow_{use}$, also called ***Modus Ponens***.) If you have P and $P \Rightarrow Q$ then you can go to Q:

$$\begin{array}{l} P \Rightarrow Q \\ P \\ \hline\hline Q \end{array}$$

RULE 8. (Rule $\Rightarrow_{get}$, also knows as the ***conditionalization*** rule.) If you have started a proof within a proof by assuming P, and have proved Q, then you can get out of the proof within a proof and go back to the main proof with $P \Longrightarrow Q$:

$$\begin{array}{l} \text{Assume } P \\ \quad \vdots \\ Q \\ \hline\hline P \Rightarrow Q \end{array}$$

RULE 9. (Rule $\Leftrightarrow_{use}$.) This ia two-part rule:

(9.a) If you have $P \Leftrightarrow Q$ then you can go to $P \Rightarrow Q$:

$$\begin{array}{l} P \Leftrightarrow Q \\ \hline\hline P \Rightarrow Q \end{array}$$

(9.b) If you have $P \Leftrightarrow Q$ then you can go to $Q \Rightarrow P$.

$$\begin{array}{l} P \Leftrightarrow Q \\ \hline\hline Q \Rightarrow P. \end{array}$$

RULE 10. (Rule $\Leftrightarrow_{get}$.) If you have $P \Rightarrow Q$ and $Q \Rightarrow P$ then you can go to $P \Leftrightarrow Q$:

$$\begin{array}{l} P \Rightarrow Q \\ Q \Rightarrow P \\ \hline\hline P \Leftrightarrow Q: \end{array}$$

In the following four rules,

- *x is a variable,*
- *P is a sentence which contains no quantifier involving the variable x,*
- *a is a symbol such as a letter or numeral,*
- *$P(x \to a)$ is what you get from P by substituting a for x in **all** the occurrences of x in P. (For example, P could be something like $x^2 + 2x \geq -1$, and a could be 3, in which case $P(x \to a)$ is $3^2 + 2 \cdot 3 \geq -1$.)*

RULE 11. (Rule $\forall_{use}$, a.k.a. the ***specialization rule***. If a is a constant whose value has been declared before, and you have $(\forall x)P$, then you can go to $P(x \to a)$. (Example: if you have $(\forall x)(x \in \mathbb{R} \Rightarrow x^2 + 2x \geq -1)$, and you have said before "let $a = 3$" or "let a be arbitrary", then you can go to $a \in \mathbb{R} \Rightarrow a^2 + 2a \geq -1$).)

RULE 12. (Rule $\forall_{get}$.) ***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 $P(x \to a)$, then you can go to $(\forall x)P$ in your main proof.

REMARK: 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 is true for ***all*** x. For example, it would not be O.K. to prove that $(\forall x)(x \in \mathbb{R} \Rightarrow (\exists y)y^2 = x)$ (i.e., that every real number has a real square root) by saying "Let a be arbitrary. Take $a = 9$. Then $(\exists y)y^2 = a$ is true, so $a \in \mathbb{R} \Rightarrow (\exists y)y^2 = a$ is true, so $(\forall x)(x \in \mathbb{R} \Rightarrow (\exists y)y^2 = x)$." What is wrong here? What is wrong is that if a is arbitrary we have no right to assume that $a = 9$. For all we know, a could be 8, or 7, or -22, or any other real number. Our CAT (creator of arbitrary things) will immediately prove us wrong, by picking x to be another

RULE 13. (Rule $\exists_{use}$.) ***Suppose that the letter a has NOT appeared before. Suppose you have proved*** $(\exists x)P$. Then

you can start a proof within a proof by introducing a new object, calling it a, and stipulating that $P(x \to a)$. 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.

REMARK: **It is important that the new object be given a name that has not been used before.** For example, suppose P stands for "x killed Polonius," and our universe of discourse is the set of all people. Suppose you are told that $(\exists x)P$, 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 $P(x \to a)$, i.e., that a killed Polonius. 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 $P(x \to \text{Hamlet})$, i.e. that Hamlet killed Polonius, or that $P(x \to \text{Laertes})$, i.e. that Laertes killed Polonius. One of these happens to be true, and the other one is false, but in either case you cannot just conclude that it is true by merely choosing a name for the killer.)

RULE 14. (Rule $\exists_{get}$, a.k.a. ***the witness rule***.) From $P(x \to a)$ you can go to $(\exists x)P$.

REMARK: Here is an example. Suppose we are working in $\mathbb{Z}$, and you want to prove that $(\exists x)x^2 + 3 \cdot x = 10$. You would first show that $2^2 + 3 \cdot 2 = 10$. Now, if P is the formula "$x^2 + 3 \cdot x = 10$", then $P(x \to 2)$ is the formula "$2^2 + 3 \cdot 2 = 10$". So we have proved $P(x \to 2)$, and Rule $\exists_{get}$ allows us to go to $(\exists x)x^2 + 3 \cdot x = 10$.

7.2.1 Proofs by contradiction (Rule 2)

Students sometimes find proofs by contradiction (i.e., Rule 2) hard to understand or hard to justify. However, the reason why proofs by contradiction work is quite trivial, and you should have no trouble understanding it.

What Rule 2 says is rather obvious and intuitive:

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

Or, if you prefer,

If you enter an imaginary world where P is not true, and end up showing that something impossible must happen in that world, then that world is an impossible world, so it cannot be the real world, so in the real world P has to be true.

7.2.2 Dealing with equality

In addition to our 14 logical rules, that have to do with the seven logical connectives, we need a rule and an axiom having to do with the equal sign.

RULE SEE: (*The* ***substitution of equals for equals*** *rule.*) If t, s are terms. P is a statement, and Q is a statement obtained from P by substituting t for s in some or all the occurrences of s in P, then (i) from $t = s$ and P you can go to Q, and (ii) from $s = t$ and P you can go to Q.

AXIOM EEI: (*The* ***everything is equal to itself*** *axiom.*)

EEI : $$(\forall x)x = x\,.$$

7.3 Some worked out examples of logical proofs

Example 1. Suppose $P(x)$ and $Q(x)$ are one-variable predicates. Prove the following:

$$(\forall x)(P(x) \wedge Q(x)) \Leftrightarrow ((\forall x)P(x) \wedge (\forall x)Q(x))\ .$$

SOLUTION. Here is a proof,

Step 1.	Assume $(\forall x)(P(x) \wedge Q(x))$.	[Assumption]
Step 2.	Let a be arbitrary.	[Declaration]
Step 3.	$P(a) \wedge Q(a)$	[Rule $\forall_{use}$, from 1 & 2]
Step 4.	$P(a)$	[Rule $\wedge_{use}$, from 3]
Step 5.	$(\forall x)P(x)$	[Rule $\forall_{get}$, from 2 & 4]

Step 6.	Let a be arbitrary.	[Declaration]
Step 7.	$P(a) \wedge Q(a)$	[Rule $\forall_{use}$, from 1 & 6]
Step 8.	$Q(a)$	[Rule $\wedge_{use}$, from 7]
Step 9.	$(\forall x)Q(x)$	[Rule $\forall_{get}$, from 6 & 8]
Step 10.	$(\forall x)P(x) \wedge (\forall x)Q(x)$	[Rule $\wedge_{get}$, from 5 & 9]
Step 11.	$(\forall x)(P(x) \wedge Q(x)) \Rightarrow ((\forall x)P(x) \wedge (\forall x)Q(x))$	[R. $\Rightarrow_{get}$, fr. 1 & 10]
Step 12.	Assume $(\forall x)P(x) \wedge (\forall x)Q(x)$.	[Assumption]
Step 13.	$(\forall x)P(x)$	[Rule $\wedge_{use}$, from 12]
Step 14.	$(\forall x)Q(x)$	[Rule $\wedge_{use}$, from 12]
Step 15.	Let a be arbitrary.	[Declaration]
Step 16.	$P(a)$.	[Rule $\forall_{use}$, from 13 & 15]
Step 17.	$Q(a)$	[Rule $\forall_{use}$, from 14 & 15]
Step 18.	$P(a) \wedge Q(a)$	[Rule $\wedge_{get}$, from 16 & 17]
Step 19.	$(\forall x)(P(x) \wedge Q(x))$	[Rule $\forall_{get}$, from 15 & 18]
Step 20.	$((\forall x)P(x) \wedge (\forall x)Q(x)) \Rightarrow (\forall x)(P(x) \wedge Q(x))$	[R. $\Rightarrow_{get}$, fr. 12 & 19]
Step 21.	$(\forall x)(P(x) \wedge Q(x)) \Leftrightarrow ((\forall x)P(x) \wedge (\forall x)Q(x))$	[R. $\Leftrightarrow_{get}$, fr. 11 & 20]

THE END

Example 2. Suppose $P(x, y)$ is a two-variable predicate. Prove the following:

$$(\forall x)(\forall y)P(x, y) \Rightarrow (\forall y)(\forall x)P(x, y)\,.$$

SOLUTION. Here is a proof.

Step 1.	Assume $(\forall x)(\forall y)P(x, y)$	[Assumption]
Step 2.	Let a be arbitrary	[Declaration]
Step 3.	Let b be arbitrary	[Declaration]
Step 4.	$(\forall y)P(b, y)$	[Rule $\forall_{use}$, from 1 & 3.]
Step 5.	$P(b, a)$	[Rule $\forall_{use}$, from 2 & 4.]
Step 6.	$(\forall x)P(x, a)$	[Rule $\forall_{get}$, from 3 & 5.]
Step 7.	$(\forall y)(\forall x)P(x, y)$	[Rule $\forall_{get}$, from 2 & 6.]
Step 8.	$(\forall x)(\forall y)P(x, y) \Rightarrow (\forall y)(\forall x)P(x, y)$.	[Rule $\Rightarrow_{get}$, from 1 & 7.]

THE END

Example 3. Suppose $P(x, y)$ is a two-variable predicate. Prove the following:

$$(\exists x)(\exists y)P(x, y) \Rightarrow (\exists y)(\exists x)P(x, y)\,.$$

SOLUTION. Here is a proof.

Step 1.	Assume $(\exists x)(\exists y)P(x, y)$.	[Assumption]

Step 2.	Pick a such that $(\exists y)P(a,y)$.	[Rule $\exists_{out}$, from 1]
Step 3.	Pick b such that $P(a,b)$.	[Rule $\exists_{out}$, from 2]
Step 4.	$(\exists x)P(x,b)$.	[Rule $\exists_{get}$, from 3]
Step 5.	$(\exists y)(\exists x)P(x,y)$.	[Rule $\exists_{get}$, from 4]
Step 6.	$(\exists y)(\exists x)P(x,y)$.	[Rule $\exists_{use}$, from 2, 3 & 5]
Step 7.	$(\exists y)(\exists x)P(x,y)$.	[Rule $\exists_{use}$, from 1, 2, & 6]
Step 8.	$(\exists x)(\exists y)P(x,y) \Rightarrow (\exists y)(\exists x)P(x,y)$.	[Rule $\Rightarrow_{get}$, from 1 & 7.]

THE END

Example 4. Suppose $P(x)$ and $Q(x)$ are one-variable predicates. Prove the following:

$$(\forall x)(P(x) \vee Q(x)) \Rightarrow ((\forall x)P(x) \vee (\forall x)Q(x)) \ . \tag{7.3.2}$$

SOLUTION. This cannot be proved because it need not be true. For example, suppose we take the universe of discourse to be the set of all U.S. senators. excluding the independents, if there are any. Suppose $P(x)$ stands for "x is a Democrat", and $Q(x)$ stands for "x is a Republican". Then the sentence "$(\forall x)(P(x)\vee Q(x))$" says that "every senator is a Democrat or a Republican", which is true, whereas "$(\forall x)P(x)$" says that "every senator is a Democrat", which is false, and "$(\forall x)Q(x)$" says that "every senator is a Republican", which is also false. Therefore the disjunction "$(\forall x)P(x) \vee (\forall x)Q(x)$" is false. Since "$(\forall x)(P(x) \vee Q(x))$" is true, as we have alreayd shown, it follows that the implication "$(\forall x)(P(x) \vee Q(x)) \Rightarrow ((\forall x)P(x) \vee (\forall x)Q(x))$" is false.

Remark. Notice that I did ***not*** say that "this cannot be proved because it isn't true." I said that "this cannot be proved because it need not be true," which is quite different. Whether or not a sentence such as (7.3.2) is true depends very much on which specific predicates you plug in for $P(x)$ and $Q(x)$. For example, you could take $P(x)$ to be any one-variable predicate you want (say, "x is a frog", or "$x > 32$") and then take $Q(x)$ to be the same as $P(x)$. Then (7.3.2) is true. (If you don't like this example, here is another one: take $P(x)$ to be "x is a frog", and $Q(x)$ to be "x is a Gila monster". Take the universe of discourse—i.e., the range of the variable x—to be the set of all animals. Then "$(\forall x)(P(x) \vee Q(x))$" says that "every animal is a frog or a Gila monster", which is obviously false, as can be proved by giving a counterexample, e.g., my dog Rex[10]. On the other hand,

[10]I am going through this to stress an important point. ***A counterexample has to be concrete and precise.*** For example, if you are trying to disprove the assertion that "every integer is even", and you say "well, pick any odd number," then I don't like that.

"$(\forall x)P(x)$" says that "every animal is a frog", which is false, and "$(\forall x)Q(x)$" says that "every animal is a Gila monster", which is also false. Hence the disjunction "$(\forall x)P(x) \vee (\forall x)Q(x)$" is false. Since both "$(\forall x)(P(x) \vee Q(x))$" and "$(\forall x)P(x) \vee (\forall x)Q(x)$" are false, the implication "$(\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall x)P(x) \vee (\forall x)Q(x)$" is true.

Example 5. Suppose $P(x)$ and $Q(x)$ are one-variable predicates. Prove the following:

$$((\forall x)P(x) \vee (\forall x)Q(x)) \Rightarrow (\forall x)(P(x) \vee Q(x)) \ . \tag{7.3.3}$$

SOLUTION. Here is a proof.

Step 1.	Assume $(\forall x)P(x) \vee (\forall x)Q(x)$	[Assumption]
Step 2.	Assume $(\forall x)P(x)$	[Assumption]
Step 3.	Let a be arbitrary	[Declaration]
Step 4.	$P(a)$	[Rule $\forall_{use}$, from 2 & 3]
Step 5.	$P(a) \vee Q(a)$	[Rule $\vee_{get}$, from 3]
Step 6.	$(\forall x)(P(x) \vee Q(x))$	[Rule $\forall_{get}$, from 3 & 5]
Step 7.	$(\forall x)P(x) \Rightarrow (\forall x)(P(x) \vee Q(x))$	[Rule $\Rightarrow_{get}$, from 2 & 6]
Step 8.	Assume $(\forall x)Q(x)$	[Assumption]
Step 9.	Let a be arbitrary	[Declaration]
Step 10.	$Q(a)$	[Rule $\forall_{use}$, from 8 & 9]
Step 11.	$P(a) \vee Q(a)$	[Rule $\vee_{get}$, from 10]
Step 12.	$(\forall x)(P(x) \vee Q(x))$	[Rule $\forall_{get}$, from 9 & 11]
Step 13.	$(\forall x)Q(x) \Rightarrow (\forall x)(P(x) \vee Q(x))$	[Rule $\Rightarrow_{get}$, from 8 & 12]
Step 14.	$(\forall x)(P(x) \vee Q(x))$	[Rule $\vee_{use}$, from 1, 7 & 13]
Step 15.	$((\forall x)P(x) \vee (\forall x)Q(x)) \Rightarrow (\forall x)(P(x) \vee Q(x))$	[Rule $\Rightarrow_{get}$, from 1 & 14]

THE END

Example 6. Suppose $P(x)$ and $Q(x)$ are one-variable predicates. Prove the following:

$$(\exists x)(P(x) \vee Q(x)) \Leftrightarrow ((\exists x)P(x) \vee (\exists x)Q(x)) \ . \tag{7.3.4}$$

SOLUTION. Here is a proof.

Step 1.	Assume $(\exists x)(P(x) \vee Q(x))$.	[Assumption]
Step 2.	Pick a such that $P(a) \vee Q(a)$.	[Rule $\exists_{use}$, from 1]
Step 3.	Assume $P(a)$	[Assumption]

I would very much prefer that you say "the number 3 is an integer but is not even". Similarly, if you said "pick any animal you want, say a cow or a giraffe," then I am not happy. I want a concrete, specific animal.

Step 4.	$(\exists x)P(x)$	[Rule $\exists_{get}$, from 3]
Step 5.	$(\exists x)P(x) \vee (\exists x)Q(x)$	[Rule $\vee_{get}$, from 4]
Step 6.	$P(a) \Rightarrow ((\exists x)P(x) \vee (\exists x)Q(x))$	[Rule $\Rightarrow_{get}$, from 3 & 5]
Step 7.	Assume $Q(a)$	[Assumption]
Step 8.	$(\exists x)Q(x)$	[Rule $\exists_{get}$, from 7]
Step 9.	$(\exists x)P(x) \vee (\exists x)Q(x)$	[Rule $\vee_{get}$, from 8]
Step 10.	$Q(a) \Rightarrow ((\exists x)P(x) \vee (\exists x)Q(x))$	[Rule $\Rightarrow_{get}$, from 7 & 9]
Step 11.	$(\exists x)P(x) \vee (\exists x)Q(x)$	[Rule $\vee_{use}$, from 2, 6,& 10]
Step 12.	$(\exists x)P(x) \vee (\exists x)Q(x)$	[Rule $\exists_{use}$, from 2 & 11]
Step 13.	$(\exists x)(P(x) \vee Q(x)) \Rightarrow ((\exists x)P(x) \vee (\exists x)Q(x))$	[Rule $\Rightarrow_{get}$, from 1 & 12]
Step 14.	Assume $(\exists x)P(x) \vee (\exists x)Q(x)$	[Assumption]
Step 15.	Assume $(\exists x)P(x)$	[Assumption]
Step 16.	Pick a such that $P(a)$.	[Rule $\exists_{use}$, from 15]
Step 17.	$P(a) \vee Q(a)$.	[Rule $\vee_{get}$, from 16]
Step 18.	$(\exists x)(P(x) \vee Q(x))$	[Rule $\exists_{get}$, from 17]
Step 19.	$(\exists x)P(x) \Rightarrow (\exists x)(P(x) \vee Q(x))$	[Rule $\Rightarrow_{get}$, from 15 & 18]
Step 20.	Assume $(\exists x)Q(x)$	[Assumption]
Step 21.	Pick a such that $Q(a)$.	[Rule $\exists_{use}$, from 20]
Step 22.	$P(a) \vee Q(a)$.	[Rule $\vee_{get}$, from 21]
Step 23.	$(\exists x)(P(x) \vee Q(x))$	[Rule $\exists_{get}$, from 22]
Step 24.	$(\exists x)Q(x) \Rightarrow (\exists x)(P(x) \vee Q(x))$	[Rule $\Rightarrow_{get}$, from 20 & 23]
Step 25.	$(\exists x)(P(x) \vee Q(x))$	[Rule $\vee_{use}$, from 14, 19 & 24]
Step 26.	$((\exists x)P(x) \vee (\exists x)Q(x)) \Rightarrow (\exists x)(P(x) \vee Q(x))$	[Rule $\Rightarrow_{get}$, from 14 & 25]
Step 27.	$((\exists x)P(x) \vee (\exists x)Q(x)) \Leftrightarrow (\exists x)(P(x) \vee Q(x))$	[Rule $\Leftrightarrow_{get}$, from 13 & 26]

THE END

Example 7. Suppose $P(x)$ and $Q(x)$ are one-variable predicates. Prove the following:

$$(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow ((\exists x)P(x) \wedge (\exists x)Q(x)) \ . \tag{7.3.5}$$

SOLUTION. This cannot be proved because it need not be true. For example, suppose we take the universe of discourse to be the set of all U.S. senators. Suppose $P(x)$ stands for "x is a Democrat", and $Q(x)$ stands for "x is a Republican". Then "$(\exists x)(P(x) \wedge Q(x))$" says that "some senators are both Democrat and Republican", which is false, whereas "$(\exists x)P(x)$" says that "some senators are Democrats", which is true, and "$(\exists x)Q(x)$" says that "some senators are Republicans," which is also true. Hence the conjunction "$(\exists x)P(x) \wedge (\exists x)Q(x)$" is true. Since "$(\exists x)(P(x) \wedge Q(x))$" is false, it follows that the biconditional "$(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow ((\exists x)P(x) \wedge (\exists x)Q(x))$" is false.

Example 8. Suppose $P(x)$ is a one-variable predicate. Prove the following:

$$(\exists x)P(x) \Leftrightarrow (\sim (\forall x) \sim P(x)) .$$

SOLUTION: Here is a proof:

Step 1.	Assume $(\exists x)P(x)$	[Assumption]
Step 2.	Assume $(\forall x) \sim P(x)$	[Assumption]
Step 3.	Pick a such that $P(a)$	[Rule $\exists_{use}$ from 1]
Step 4.	$\sim P(a)$	[Rule $\forall_{use}$ from 2]
Step 5.	$P(a) \wedge \sim P(a)$	[Rule $\wedge_{get}$ from 3 & 4]
Step 6.	$(P(a) \wedge \sim P(a)) \Rightarrow (0 = 0 \wedge \sim 0 = 0)$	[Instance of tautology]

[*Comment: the only reason I used* $0 = 0 \wedge \sim 0 = 0$ *here is that it is a contradiction. Any other contradiction would have served the same purpose. What did I need a contradiction for? Well, we already got a contradiction, namely,* $P(a) \wedge \sim P(a)$*. This contradiction, however, contains* a*, so we cannot get out of the proof within a proof that we started in Step 3. In order to do that, we need a contradiction that does not contain* a*. Any such contradiction will do. How do we get a contradiction not containing* a *from* $P(a) \wedge \sim P(a)$ *? Well, simply, a contradiction implies anything you want. (That is, if* C *is a contradiction then* $C \Rightarrow A$ *is a tautology no matter what* A *is.) So in particular* $P(a) \wedge \sim P(a)$ *implies* $0 = 0 \wedge \sim 0 = 0$.]

Step 7.	$0 = 0 \wedge \sim 0 = 0$	[Rule $\Rightarrow_{get}$ from 5 & 6]

[*Comment: now that we got a statement not involving* a*, we can get out of the proof within a proof that we started in Step 3.*]

Step 8.	$0 = 0 \wedge \sim 0 = 0$ (*contradiction*)	[Rule $\exists_{get}$ from 2, 3 & 7]
Step 9.	$\sim (\forall x) \sim P(x)$.	[Rule 2 from 2 & 8]
Step 10.	$(\exists x)P(x) \Rightarrow (\sim (\forall x) \sim P(x))$.	[Rule $\Rightarrow_{get}$ from 1 & 9]
Step 11.	Assume $\sim (\forall x) \sim P(x)$.	[Assumption]
Step 12.	Assume $\sim (\exists x)P(x)$.	[Assumption]
Step 13.	Let a be arbitrary.	[Declaration]
Step 14.	Assume $P(a)$.	[Assumption]
Step 15.	$(\exists x)P(x)$.	[Rule $\exists_{get}$ from 14]
Step 16.	$(\exists x)P(x) \wedge \sim (\exists x)P(x)$ (*contradiction*)	[Rule $\wedge_{get}$ from 12 & 15]
Step 17.	$\sim P(a)$	[Rule 2, from 14 & 16]
Step 18.	$(\forall x) \sim P(x)$	[Rule $\forall_{get}$ from 13 & 17]
Step 19.	$(\forall x) \sim P(x) \wedge (\sim (\forall x) \sim P(x))$ (*contradiction*)	[Rule $\wedge_{get}$ from 11 & 18]
Step 20.	$(\exists x)P(x)$	[Rule 2, from 12 & 19]
Step 21.	$(\sim (\forall x) \sim P(x)) \Rightarrow (\exists x)P(x)$	[Rule $\Rightarrow_{get}$ from 11 & 20]
Step 22.	$(\exists x)P(x) \Leftrightarrow (\sim (\forall x) \sim P(x))$	[Rule $\Leftrightarrow_{get}$ from 10 & 21]

THE END

Example 9. Prove the following:

$$(\forall x)(\forall y)(\forall z)((x = y \wedge y = z) \Rightarrow x = z) .$$

SOLUTION: Here is a proof:

Step 1.	Let a be arbitrary	[Declaration]
Step 2.	Let b be arbitrary	[Declaration]
Step 3.	Let c be arbitrary	[Declaration]
Step 4.	Assume $a = b \wedge b = c$	[Assumption]
Step 5.	$a = b$	[Rule $\wedge_{use}$, from 4]
Step 6.	$b = c$	[Rule $\wedge_{use}$, from 4]
Step 7.	$a = c$	[Rule SEE, from 5 & 6]
Step 8.	$(a = b \wedge b = c) \Rightarrow a = c$	[Rule $\Rightarrow_{get}$, from 4 & 7]
Step 9.	$(\forall z)((a = b \wedge b = z) \Rightarrow a = z)$	[Rule $\forall_{get}$, from 3 & 8]
Step 10.	$(\forall y)(\forall z)((a = y \wedge y = z) \Rightarrow a = z)$	[Rule $\forall_{get}$, from 2 & 9]
Step 11.	$(\forall x)(\forall y)(\forall z)((x = y \wedge y = z) \Rightarrow x = z)$	[Rule $\forall_{get}$, from 1 & 10]
		THE END

7.4 Getting rid of some rules

So far, we have given 14 logical rules of inference, plus one rule (Rule SEE) involving the equal sign. (Actually, four of our rules are two-part rules, so in fact we have 18 logical rules plus Rule SEE.)

Do we need so many rules? The answer is **"no"**. We could get away with a lot fewer rules. For example, suppose you wanted to avoid using Rule 6 (that is, Rule $\wedge_{get}$). Let me show you how you can always avoid using this Rule 5. Suppose you find yourself in a situation where you have statements P and Q and you would like to go to $P \wedge Q$. If you could apply Rule 6 then of course you can do that. But suppose you want to do it without using Rule 6. Here is what you could do:

1. P
2. Q
3. $P \Rightarrow (Q \Longrightarrow (P \wedge Q))$
4. $Q \Longrightarrow (P \wedge Q)$
5. $P \wedge Q$.

(In Step 3 we brought in a tautology. In Steps 4 and 5 we used Modus Ponens, i.e., Rule $\Rightarrow_{use}$.)

Similarly, suppose you wanted to do proofs by contradiction without using Rule 2. Suppose you know how to prove a contradiction C from $\sim P$, and you want to go to P, without invoking Rule 2.

Here is what you could do:

Assume P

$\vdots$

C

$P \Rightarrow C$

$(P \Rightarrow C) \Rightarrow (\sim P)$

$\sim P$.

(The key step here is the fact that, since C is a contradiction, $(P \Rightarrow C) \Rightarrow (\sim P)$ is a tautology, because for $(P \Rightarrow C) \Rightarrow (\sim P)$ to be false $P \Rightarrow C$ has to be true and $\sim P$ has to be false, so P has to be true; but then P has to be false, because if P was true then $P \Rightarrow C$ would be false, since C is a contradiction; so P has to be true and P has to be false, which is impossible. In the last step 3 we used Modus Ponens, i.e., Rule $\Rightarrow_{use}$.)

PROBLEM: Show that the following seven rules would suffice: Rules 1, 7, 8, 10, 11, 12 and 13.

8 Homework assignment no. 4, due on Wednesday February 15

1. Suppose $P(x)$ is a one-variable predicate. Prove the following:

$$(\forall x)P(x) \Leftrightarrow (\sim (\exists x) \sim P(x)) .$$

2. Suppose $P(x)$ and $Q(x)$ are one-variable predicates. Prove the following:

$$(\forall x)(P(x) \vee Q(x)) \Leftrightarrow ((\forall x)P(x) \vee (\forall x)Q(x)) .$$

3. Suppose $P(x, y)$ is a two-variable predicate. Prove the following:

$$(\exists y)(\forall x)P(x, y) \Rightarrow (\forall x)(\exists y)P(x, y) .$$

4. Suppose $P(x, y)$ is a two-variable predicate. Prove the following:

$$(\forall x)(\exists y)P(x, y) \Rightarrow (\exists y)(\forall x)P(x, y)$$

5. Here are five sentences about giraffes, cows, sheep, Olivia, Dolly, and the binary relation "taller than."

(1) Cows are taller than sheep. (That is, "every cow is taller than every sheep," or, if you prefer, "for every x and every y, if x is a cow and y is a sheep, then x is taller than y.")

(2) Giraffes are taller than cows.

(3) If something is taller than something else which is in turn taller than a third thing, then the first one is taller than the third one. (That is "for every x, every y and every z, if x is taller than y and y is taller than z, then x is taller than z.")

(4) Olivia is a giraffe.

(5) Dolly is a sheep.

Using sentences (1), (2), (3), (4), (5), *and* **no other fact** *about giraffes, cows, sheep, Olivia, Dolly, and the binary relation "taller than,"* prove that Olivia is taller than Dolly.

6. Book, Exercises 1.6 (pages 53-54-55-56): Problems 1 (non-starred parts), 2 (non-starred parts), and 8 (non-starred parts).

9 Definitions: why they matter and how you should write them

An example. Suppose you are asked whether the numbers 6 and 12 are "perfect". Then the first thing you need to know is what it means for a number to be "perfect". Without that information, you cannot do anything. Here is the definition:

DEFINITION OF "PERFECT NUMBER"

Let n be a natural number. We say that n is ***perfect*** if n is equal to the sum of all the natural numbers other than n that divide n.

Armed with this definition, we can answer our questions about 6 and 12.

Is 6 *perfect?* Here is the list of all the natural numbers other than 6 that divide 6: 1, 2, and 3. Clearly, $1 + 2 + 3 = 6$, so 6 ***is perfect***.

Is 12 *perfect?* Here is the list of all the natural numbers other than 12 that divide 12: 1, 2, 3, 4, and 6. Since $1 + 2 + 3 + 4 + 6 = 16$, and $16 \neq 12$, we can conclude that 12 ***is not perfect***.

Problem. Find a perfect number n such that $n > 6$. (This is easy.)

Problem. Find two perfect numbers m, n such that $m > n$ and $n > 6$. (This is not so easy.)

A second example. Suppose you are asked whether the real number 0.000000000000000001 is "small? Here we have the same problem as before. To answer the question we need the definition of "small". And it turns out that I do not know what "small" means, and I bet you do not know either. (*If you think you know, then please tell me!*) Actually, nobody knows what "small" means[11], so the word "small" is not used in rigorous mathematics

If you are worried, and you think that you know what "small" means, try to imagine, for example, the State Legislature of New Jersey passing a bill decreeing that "the asbestos level in all building materials has to be small", and imposing a penalty on violators. Does that make sense? Obviously not, because there is no way to apply this in any concrete situation. Any time a law-enforcement agency tries to argue that the asbestos level of a particular material is not "small", the alleged violator will retort that it *is* small, and will demand where in the law it says what "small" means. "Small" is meaningless unless you specify *how* small.

A third example. Suppose you are asked "is the number 18 even?". This time you *can* answer, because you have a precise definition of "even":

DEFINITION OF "EVEN"

Let n be an integer. We say that n is ***even*** if there exists an integer k such that $n = 2k$.

or, if you prefer,

[11] We all know what "smaller than" means, but that's a totally different thing!

DEFINITION OF "EVEN"

Let n be an integer. We say that n is ***even*** if $n = 2k$ for some integer k.

We can also say this (but we don't have to) using symbolic language:

DEFINITION OF "EVEN"

$$(\forall n \in \mathbb{Z})(n \text{ is } \mathbf{even} \ \Leftrightarrow (\exists k \in \mathbb{Z})n = 2.k)\,,$$

or, if we have already somehow stipulated that our universe of discourse is $\mathbb{Z}$ (that is, that our letter variables take values in $\mathbb{Z}$)

DEFINITION OF "EVEN"

(if the universe of discourse has been declared to be $\mathbb{Z}$)

$$(\forall n)(n \text{ is } \mathbf{even} \ \Leftrightarrow (\exists k)n = 2.k)\,.$$

To prove that 18 is even we apply the definition. Since the n of the definition is an ***arbitrary***[12] integer, we can certainly take $n = 18$. Then we conclude that "18 is even provided that there is an integer k such that $2k = 18$." So now all we need is to prove that "there is an integer k such that $2k = 18$." That is, we have to prove that $(\exists k \in \mathbb{Z})2k = 18$. (Notice that here k is a ***dummy variable***, because it is a ***bound variable***, occurring in a quantified statement under the scope of a quantifier. We could equally well have written this statement as

$$(\exists x \in \mathbb{Z})2x = 18\ ,$$

or

$$(\exists a \in \mathbb{Z})2a = 18\ \ ,$$

or

$$(\exists q \in \mathbb{Z})2q = 18\ \ ,$$

[12] Recall that one of the many ways to read $(\forall n \in \mathbb{Z})\cdots$ is "Let n be an arbitrary integer. Then $\cdots$."

or

$$(\exists \alpha \in \mathbb{Z}) 2\alpha = 18 \ ,$$

or

$$(\exists \diamondsuit \in \mathbb{Z}) 2\diamondsuit = 18 \ ,$$

or

$$(\exists \clubsuit \in \mathbb{Z}) 2\clubsuit = 18 \ ,$$

or

$$(\exists \aleph \in \mathbb{Z}) 2\aleph = 18 \ ,$$

or

$$(\exists something \in \mathbb{Z}) 2something = 18 \ ,$$

or

$$(\exists gnu \in \mathbb{Z}) 2gnu = 18 \ ,$$

or

$$(\exists Ethel\text{-}the\text{-}frog \in \mathbb{Z}) 2Ethel\text{-}the\text{-}frog = 18 \ .$$

The predicate "$(\exists k \in \mathbb{Z}) n = 2.k$" is a ***one variable predicate***—the variable being n—because in order to decide whether "$(\exists k \in \mathbb{Z}) n = 2.k$" is true you need to ask me what n is. And the predicate "$(\exists k \in \mathbb{Z}) 18 = 2.k$" is a ***zero variables predicate***—i.e., a proposition—because in order to decide whether "$(\exists k \in \mathbb{Z}) 18 = 2.k$" is true you don't need to ask me anything, because you can figure out whether the sentence is true or not all by yourself.)

To prove that $(\exists k \in \mathbb{Z}) 18 = 2.k$ we obviously need a rule that will enable us to *get* an *existential sentence*. Not surprisingly, we have such a rule, and it is called[13] "Rule $\exists_{get}$" (or the "witness rule"):

[13]Students often tell me that they are having a lot of trouble remembering the rules. Honestly, I do not understand why. What could be more natural, and easier to remember, than calling the rule for *getting* an "$\exists$" sentence "Rule $\exists_{get}$"? If you find that this is difficult, read a Logic book and look at the names of the rules there (for example, Modus Ponens, Modus Tollens, Conjunction introduction, Disjunction introduction, Simplification, Disjunctive syllogism, Hypothetical syllogism, Constructive dilemma, Destructive dilemma, Resolution). To me, those names are hard to remember, but the ones I am giving you are easy.

To prove that there exists a thing such that something involving this thing happens, you show one (that is, you exhibit a witness).
For example: to prove that there exists a town in New Jersey with a population larger that 10,000, you say "for instance, Piscataway has more than 10,000 people." (Naturally, you could also have used Trenton, or Princeton, or New Brunswick.)

So, to prove that $(\exists k \in \mathbb{Z})2k = 18$ you must exhibit an integer k such that $2k = 18$. The obvious choice (in fact the only choice) is 9. Since $2.9 = 18$, and 9 is an integer, it is true that $(\exists k \in \mathbb{Z})2k = 18$. So 18 is even.

This definition takes care, in a completely unambiguous way, of questions that students sometimes ask in class. For example, students sometimes ask "is 0 even?" or, even worse[14], "is 0 considered even?" My answer to that question is "if the definition of even implies that 0 is even then 0 is even; if the definition of even implies that 0 is not even then 0 is not even; to decide whether 0 is or is not even, apply the definition." So, you see, *having a precise definition of "even" enables you to settle the question whether something is even, even in cases when you are in doubt.*

A fourth example. Let us now consider the definition of "prime." Is 3 prime? Is 6 prime? Is 1 prime? Is π prime?

Students often say vague, fuzzy things such as "a prime number is a number that has no factors." Now, *this purported definition is either wrong or so vague that you cannot work with it.* Actually, every integer has "factors", since, for example, every integer is divisible by itself and by 1. So if one takes the definition literally, then no integer is prime, and the definition is wrong, because this is obviously, not what you want! So maybe you didn't quite mean that. So, what ***did*** you mean? Maybe when you said "no factors" you meant "no factors other than itself and 1." But then, again, that would not work, because every integer is also divisible by -1. So maybe you mean "a

[14]Why "worse"? Because whether 0 is even or not has nothing to do with me or you anybody "considering" anything! Zero ***is*** even, or ***it isn't***, and what determines whether it is or it is not is not what I may "consider", but what the definition says. Once you have the definition of "even" you have to be able to decide by yourself if 0 is even or not.

prime number is a natural number that has no natural number factors other than 1 and itself." Now, this is a precise definition, but turns out not to be a good one, because according to this definition 1 would be prime, and there are millions of reasons why we do not want to count 1 as prime. (For example: we want every natural number > 1 to be uniquely expressible as a prime or a product of primes. If 1 was a prime, then we would have $6 = 2.3$, but also $6 = 1.2.3$, and $6 = 1.1.1.1.1.1.1.1.2.3$, and this would violate the uniqueness of the factorization.)

So, the usual ways of defining "prime" that students are used to are too vague to be useful. That's why we give a precise definition:

DEFINITION OF "PRIME"

Let n be an integer. We say that n is ***prime*** if $n > 1$ and there do not exist integers p, q such that $n = p.q$ and $1 < p < n$.

We can also say this (but we don't have to) using symbolic language:

DEFINITION OF "PRIME"

$$(\forall n \in \mathbb{Z})\Big(n \text{ is } \mathbf{prime} \Leftrightarrow (n > 1 \wedge \sim (\exists p \in \mathbb{Z})(\exists q \in \mathbb{Z})(n = p.q \wedge 1 < p < n))\Big).$$

This definition is truly useful, in the sense that you can work with it. If I give you any integer, you can actually use the definition and decide whether the given integer is or is not prime.

A fifth example. Suppose you are asked whether Star Trek's Mr. Spock has a brother. To asnwer this question, you need a definition of "brother" that you can work with. If you try to write down such a definition, you will be faced with the problem that the word "brother", as is commonly used, is ambiguous, because sometimes we want to allow half brothers to count as brothers and sometimes don't[15]. So we have two possible "formal" definitions of "brother":

[15]And we also have to decide whether we are just dealing with human beings or we also count animals. Here, for simplicity, I will just work with humans. Kinship in the animal kingdom can be a complicated thing, as shown by the example of bees!

FIRST DEFINITION OF "BROTHER"

Let n, m be human beings. We say that n is a ***brother*** of m if n is male, $n \neq m$, and the two parents of n are also the parents of m.

We can also say this using symbolic language:

FIRST DEFINITION OF "BROTHER"

(using $\mathbb{H}$ to denote the set of all human beings)

$$(\forall n \in \mathbb{H})(\forall m \in \mathbb{H})\Big(n \text{ is a } \textbf{brother} \text{ of } m \iff ((n \text{ is male} \wedge n \neq m) \wedge (\forall k \in \mathbb{H})(k \text{ is a parent of } n \Leftrightarrow k \text{ is a parent of } m))\Big)$$

The second definition is different:

SECOND DEFINITION OF "BROTHER"

Let n, m be human beings. We say that n is a ***brother*** of m if n is male, $n \neq m$, and at least one of the two parents of n is also a parent of m.

Again, we can say this using symbolic language:

SECOND DEFINITION OF "BROTHER"

(using $\mathbb{H}$ to denote the set of all human beings)

$$(\forall n \in \mathbb{H})(\forall m \in \mathbb{H})\Big(n \text{ is a } \textbf{brother} \text{ of } m \iff ((n \text{ is male} \wedge n \neq m) \wedge (\exists k \in \mathbb{H})(k \text{ is a parent of } n \wedge k \text{ is a parent of } m))\Big)$$

These definitions are truly useful. And now we can decide whether Mr. Spock has a brother: if we adopt the first definition, he does not, but if we use the second definition he does. (To be even more precise: everybody knows that Mr. Spock has an evil half-brother, so he does have a "brother" in the sense of the second definition. But I am not aware of Mr. Spock having a brother in the sense of the first definition.)

A sixth example. Suppose you are asked the question "Are John Kerry and Laura Bush married?" If I try to understand what this means, precisely, I run into the fact that the predicate "married" is ambiguous, because when you are talking about two people, "being married" could mean "being married to each other," or "being married each one separately." So the ambiguity here arises because, *there really are two predicates "married": one is the one-variable predicated "begin married to somebody", and the other one is the two-variable predicate "being married to each other."* Let us call these predicates "married$_1$" and "married$_2$". Then we can give formal definitions:

DEFINITION OF "MARRIED$_2$"

Let n, m be human beings. We say that n and m are ***married***$_2$ if they have been legally declared spouses of each other.

DEFINITION OF "MARRIED$_1$"

Let n be a human being. We say that n is ***married***$_1$ if there exists m such that n and m are married$_2$.

Problem. Let us use a language in which there is a one-variable predicate $F(x)$ meaning "x is female", a two-variable predicate $P(x, y)$ meaning "x is a parent[16] of y", and the two-variable predicate "$x = y$", with its usual meaning. Assume the universe of discourse is the set of all people.

In this language, give definitions of (1) father, (2) mother, (3) son, (4) daughter, (5) sister, (6) uncle, (7) grandfather. Do it both ways: with words, as in our first definition of "prime", and in symbolic notation.

Here is, as an example, the answer to (1):

Definition of "father": Let x, y be people. We say that x is y's ***father*** if x is a parent of y and x is not female.

Definition of "father", in symbolic language:

$$(\forall x)(\forall y)(x \text{ is } y\text{'s } \textbf{\textit{father}} \Leftrightarrow (P(x, y) \wedge \sim F(x)))$$

[16] That is, father or mother.

9.1 Definitions and arguments

From the previous examples, you can see that

> Predicates have ***arguments***, so when you define a predicate you have to begin by specifying what the arguments are, and in particular it has to be clear from your definition how many arguments there are. These arguments connect the definition with the rest of the world. For example, the definitions of "even," "prime," and "married$_1$" have **one** argument each, so they enable you to plug in **one** object and get a true-false conclusion. The definitions of "divisible," "brother," and "married$_2$ " have **two** arguments. You plug in **two** things to get a true-false conclusion.

When you write a definition you should first of all figure out how many arguments will be involved, and then you should make sure that the definition begins by introducing these arguments.

Example. Let us figure out on our own, step by step, how to define "divisible." First of all, "divisible" is a word that talks about two numbers. (We do not talk about one number being "divisible." We talk about one number being "divisible" by another number.) So if we set out to write a definition of "divisible" we have to start by introducing our two arguments: "Let a and b be numbers." Moreover, the "numbers" involved, cannot just be any numbers. They have to be *integers*. So we really have to start with "Let a and b be integers." Now that we know who we are talking about (that is, we have properly introduced our two arguments) we are ready to say what we want to say. We want to explain what it means for a to be divisible by b. So we write "We say that a is *divisible* by b if (or 'provided that') XXXXXXXXXXX." Now what is missing is XXXXXXXXXXX. We already have the *structure* of our definition:

> Let a and b be integers. We say that a
> is *divisible* by b if XXXXXXXXXXX.

and we have to fill in the contents.

So far, all that mattered is that "divisible" is something about two integers. Now we have to say what that "something" is. In our case, the thing to put in the XXXXXXXXX slot is "$(\exists c \in \mathbb{Z})bc = a$," and we end up with

Let a and b be integers. We say that a is
divisible by b if $(\exists c \in \mathbb{Z})bc = a$.

Another example. Let us figure out on our own, step by step, how to define "grandson" for the benefit of someone who knows what "father," "mother" and "male" mean. First of all, "grandson" is a word that talks about two people. (We do not talk about one person being "a grandson." We talk about one person being another person's "grandson.") So if we set out to write a definition of "grandson" we have to start by introducing our two arguments: "Let a and b be persons." Now that we know who we are talking about (that is, we have introduced our two arguments) we are ready to say what we want to say. We want to explain what it means for a to be a grandson of b. So we write "We say that a is a *grandson* of b if (or 'provided that') XXXXXXXXX." Now what is missing is XXXXXXXXX. We already have the *structure* of our definition:

Let a and b be persons. We say that a is a *grandson* of b
if XXXXXXXX.

and we have to fill in the contents. (So far, all that mattered is that "grandson" is something about two persons. Now we must say what that "something" is.)

In our case, the thing to put in the XXXXXX slot seems to be "b is a parent of someone who is a parent of a," that is,

"$(\exists c)(c$ is a person and c is a parent of a and b is a parent of $c)$."

But a moment's thought shows that this is not enough. We are trying to define *grandson*, not *grandchild*. So we have to make sure that a is male.

The final result is

Let a and b be persons. We say that a is a *grandson* of b if
a is male and $(\exists c)(c$ is a person and c is a parent of a and b is a parent of $c)$.

9.2 Always highlight the definiendum

When you write a definition, you are defining a particular word or phrase. That word or phrase is called the *definiendum*. (This just means "the thing being defined.") **The definiendum should always be highlighted.** In books, the authors do this by using Italics, or Boldface. (Look, for example, at any definitions you want in our textboook) When you write your homework or your exams, or when I write on the blackboard, it's hard to do Italics, so we use underlining instead.

9.3 Always make sure to specify the kind of thing or things that your definition is about

When you are asked to define "prime", the first question you have to ask yourself is: what kind of things is "being prime" about? Do we talk about *numbers* being prime, or about *animals* begin prime, or about *people* being prime, or about *pieces of furniture* being prime? Clearly, the answer is that we talk about *numbers* being prime. Furthermore, is it any kind of number that can be prime, or does the notion of prime only make sense of some very special kind of "numbers". The answer is: it makes sense of *integers only*. So when we define "prime" our definition will have to start by introducing an integer, by saying "Let p be an integer." Then the definition may move on to tell me under what conditions we will call n prime.

Similarly, when we define "brother", our first question should be what kind of things is the predicate "brother of" about? And the answer is that it is about two people, so you have to start your definition by introducing those two people, by saying: "Let a, b be human beings". Once you have done that, you would go on to explain what it means for a to be b's brother.

9.4 An example': the definitions of "tautology" and "contradiction"

Recall that we have given a precise defintion of "propositional form" (also known as "sentence form," or "statement form") in these notes. As explained there, a propositional form contains letters known as *propositional variables*, and if you give truth values (T or F) to each such variable then the propositional form has a truth value.

Definition 1. A ***tautology*** is a propositional form $\mathcal{F}$ such that $\mathcal{F}$ has the truth value T for every possible way of assigning truth values to the propositional variables that occur in $\mathcal{F}$.

Definition 2. A ***contradiction*** is a propositional form $\mathcal{F}$ such that $\mathcal{F}$ has the truth value F for every possible way of assigning truth values to the propositional variables that occur in $\mathcal{F}$.

Notice that the definitions begin by telling us clearly what kind of thing can be a tautology or a contradiction to begin with: it's not a person, or an animal, or a number. Being a tautology or a contradiction is something that can be true of a ***propositional form***.

In particular, a tautology or a contradiction is ***not*** a particular kind of statement or proposition. Students often make the mistake of saying that "a tautology is a true statement", or "a tautology is a statement which is always true". The first one is just plain wrong. (For example, "H. J. Sussmann is the best teacher in the whole universe" is obviously a true statement, but it is not a tautology.) As for the second one, it is meaningless. What does "always" mean here? Take the statement "H. J. Sussmann is the best teacher in the whole universe". Is this "always true", or is is just true. And what on Earth is the difference between being "true" and being "always true"?

"Always true" makes sense of ***propositional forms***, but not of statements. For example, the propositional form $P \Rightarrow (Q \Rightarrow (P \wedge Q))$ is true no matter which propositions you plug in for p and Q. That is why it makes sens to say that $P \Rightarrow (Q \Rightarrow (P \wedge Q))$ is *always* true.

9.5 More than two variables?

As you probably have guessed by now, there are three-variable predicates, four-variable predicates, and so on. For example, "common divisor" is a three-variable predicate. Here is the definition.

DEFINITION OF "COMMON DIVISOR"

Let a, b, c be integers; we say that a is a ***common divisor of*** b ***and*** c if b is divisible by a and c is divisible by a.

Or, if you prefer, you could have used symbolic notation:

DEFINITION OF "COMMON DIVISOR"

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(a$ is a **common divisor of** b **and** c
$\Leftrightarrow (\exists k \in \mathbb{Z})b = ak \wedge (\exists k \in \mathbb{Z})c = ak)$.

Question. Is it O.K. to write "$(\exists k \in \mathbb{Z})b = ak \wedge (\exists k \in \mathbb{Z})c = ak)$, as I just did? Doesn't this cause a problem, by somehow saying that "the k such that $b = ak$ and the k such that $c = ak$ are the same? Discuss.

10 Homework assignment no. 5, due on Feb. 22

1. Book, Exercises 1.7, pages 64-67, Problems 1, 2, 3, 6, 10.

2. Give a complete formal proof, using the axioms, the rules of inference (including Rule SEE, of course), the definition of 2, and nothing else, of the following two statements:

$$\sim 2 = 0\,,$$

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})(x + y) \cdot z = x \cdot z + y \cdot z\,.$$

(NOTE: The definition of 2 is: $2 = 1 + 1$.)

11 Arithmetic

We would now like to be able to prove various properties of natural numbers, integers, and real numbers. Our first step will be to introduce the ***vocabulary of arithmetic***, so that we can say things about these numbers. Then we will state the ***axioms*** (also known as ***postulates***), that is, the statements that we can bring into a proof any time we want. Finally, we will give some proofs, using the axioms.

11.1 The basic vocabulary of arithmetic

The basic vocabulary of real arithmetic consists of

I. The **logical connectives:**

1. The **propositional connectives:**
   a. the *negation symbol* ("$\sim \ldots$", read as "not ...", or "it is not the case that ..."),
   b. the *conjunction symbol* ("$\ldots \wedge \ldots$", read as "... and ..."),
   c. the *disjunction symbol* ("$\ldots \vee \ldots$", read as "... or ..."),
   d. the *implication symbol* ("$\ldots \Longrightarrow \ldots$", read as "... implies ...", or "if ... then ..."),
   e. the *biconditional symbol* ("$\ldots \Longleftrightarrow \ldots$", read as "... if and only if ..."),
2. The **quantifiers:**
   a. the *existential quantifier* ("$\exists \ldots$", read as "there exists ... such that");
   b. the *universal quantifier* ("$\forall \ldots$", read as "for all ...");
3. The **right and left parentheses.**

II. The **letter variables and individual symbols:** a, b, ..., i, j, k, ..., m, n, p, q, ..., x, y, z, ... (In principle, any symbol or string of symbols—not containing a blank space— can be used as a variable, provided you declare it as such. This includes Greek letters such as α, β, etc., Hebrew or Arabic letters, weird symbols such as $\diamondsuit$ or $\clubsuit$, and strings such as *googoo* and *Ethel-the-frog*.)

III. **The equal sign:** "=" ("is equal to", or "equals") ,

IV. **The arithmetical symbols:**

a. the *constants* "0" ("zero") and "1" ("one");

b. the *symbols for the arithmetical operations*:
   * "+" ("plus"),
   * "." ("times", sometimes written "×"),
   * "−" "minus"),

* "—" ("over", or "divided by");

c. the *arithmetical predicate symbols:*

* "$<$" ("is less than", or "is smaller than"),
* "$>$" ("is larger than"),
* "$\leq$" ("is less than or equal to", or "is not greater than"),
* "$\geq$" ("is greater than or equal to", or "is not smaller than"),
* "$\in \mathbb{N}$" ("is a natural number"),
* "$\in \mathbb{Z}$" ("is an integer"),
* "$\in \mathbb{R}$" ("is a real number").

THE BASIC VOCABULARY OF ARITHMETIC

$$\sim \quad \wedge \quad \vee \Rightarrow \quad \Leftrightarrow \quad \exists \quad \forall \quad (\quad) \quad =$$

$$0 \quad 1 \quad < \quad > \quad \leq \quad \geq \quad + \quad - \quad \cdot \quad —$$

$$\in \mathbb{N} \qquad \in \mathbb{Z} \qquad \in \mathbb{R}$$

and the letter variables and individual symbols.

11.2 How the basic symbols are used

We have already discussed how to use the logical connectives, so I will not repeat that.

Now let us look at the equal sign, the symbols for the arithmetical operations, and the arithmetical predicate symbols.

The ***symbols for the arithmetical operations*** are used, together with the constants and letter variables, to form ***terms***. The way this is done is as follows:

- a constant is a term;
- a variable is a term;

- if t, s are terms, then $t+s$, $t-s$, $t \cdot s$, and $\frac{t}{s}$ are terms; furthermore, we can also write ts or $t \times s$ instead of $t \cdot s$; .
- only those expressions constructed by repeated use of the above rules are terms.

Remark (*on the very unpleasant issue of parentheses*). The above rules for term formation are not yet complete and precise, because they ignore a question which is extremely unpleasant but very important:

Where do we put parentheses?

It is clear that we do need parentheses, because we want to distinguish, for example, between $(x+y) \cdot z$ and $x + (y \cdot z)$. How do we use them? Where do we put them?

Here is one possible precise rule, that I am going to call the "maximalist parenthesis rule for terms", because this rule basically tells you that you have to put parentheses all over the place.

The maximalist parenthesis rule for terms

Let us call a term

- a ***simple term*** if it is a constant or a variable;
- a ***compound term*** if it is of the form $t+s$ or $t-s$ or $t \cdot s$ or $\frac{t}{s}$, where t and s are terms.

Then, when you form a compound term from terms t and s, which may themselves be simple or compound:

- if t and s are simple, then you write $t+s$, $t-s$, $t \cdot s$, $\frac{t}{s}$;
- if t is simple and s is compound, you write $t+(s)$, $t-(s)$, $t \cdot (s)$, $\frac{t}{s}$;
- if t is compound and s is simple, you write $(t)+s$, $(t)-s$, $(t) \cdot s$, $\frac{t}{s}$;
- if t and s are both compound, you write $(t)+(s)$, $(t)-(s)$, $(t) \cdot (s)$, $\frac{t}{s}$.

For example, according to this rule, the following are terms:

x	3	$x+3$
$x \cdot 3$	$(x+3) \cdot x$	$x + (3 \cdot 7)$
$\frac{x+3}{7}$	$((x+3) \cdot x) \cdot (x+1)$	$(x + (3 \cdot 7)) \cdot (x \times 1)$
$\left(\frac{x+3}{7}\right) \cdot (x-1)$	$\left(\frac{x+3}{7}\right) - \left(\frac{x-3}{3x+7}\right)$	$x \cdot (((x \cdot x) \cdot x + 7) \cdot x)$.

This is too much, of course. You are used to putting fewer parentheses, and writing, for example, $x + 3 \cdot 7$ rather than $x + (3 \cdot 7)$. I could write a set of rules that will give you exactly the parentheses that you are used to having, but I will not do it here because it is a complicated thing to do. (If you think this is easy, try doing it, and show me the result!!!! The rules should be such that you can program them into a computer: that is, you should be able to write a computer program that, if you input a string of arithmetical symbols and specify which are the variables[17], then the program will answer correctly, with "yes" or "no", the question "is this string a term?")

So here I am going to use the maximalist parenthesis rule for terms. $\diamondsuit$

Now that we know (more or less, except for that annoying issue of the parentheses) how to form terms, the next question is how to form ***arithmetical atomic predicates***. For that purpose, we use the symbols $=$, $<$, $>$, $\leq$, $\geq$. The rule is quite simple: if t and s are terms, then $t = s$, $t > s$, $t < s$, $t \leq s$, $t \geq s$ $t \in \mathbb{R}$, $t \in \mathbb{N}$, $t \in \mathbb{Z}$, are atomic predicates.

Finally, once we have atomic predicates, we can form more general predicates, using the logical connectives. So, for example, the following are predicates:

$$(p \in \mathbb{Z} \wedge p > 1) \wedge \sim (\exists k)(\exists l)(((k \in \mathbb{Z} \wedge \ell \in \mathbb{Z}) \wedge (k > 1 \wedge \ell > 1)) \wedge p = k \cdot \ell) \ ,$$

$$(x \in \mathbb{Z} \wedge y \in \mathbb{Z}) \wedge (\exists p)(((p \in \mathbb{Z} \wedge p > 1) \wedge \sim (\exists k)(\exists l)(((k \in \mathbb{Z} \wedge \ell \in \mathbb{Z})$$
$$\wedge (k > 1 \wedge \ell > 1)) \wedge p = k \cdot \ell)) \wedge (\exists m)(\exists n)((m \in \mathbb{Z} \wedge n \in \mathbb{Z}) \wedge (x = m \cdot p \wedge y = n \cdot p))) \ .$$

(The first one says "p is prime". The second one says "x and y are integers that have a common prime factor".)

[17] This little detail is important. You can declare "Ethel-the-frog" to be a variable, if you want to, but the computer will not know that unless you tell it.

11.3 The axioms of arithmetic

THE AXIOMS OF ARITHMETIC, PART I

ADDITION AXIOMS

Add1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x + y \in \mathbb{R}$.

Add2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x + y = y + x$.

Add3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x + y) + z = x + (y + z)$.

SUBTRACTION AXIOMS

Sub1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x - y \in \mathbb{R}$.

Sub2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x - y = z \Leftrightarrow x = y + z)$

MULTIPLICATION AXIOMS

Mul1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x \cdot y \in \mathbb{R}$.

Mul2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x \cdot y = y \cdot x$.

Mul3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

DIVISION AXIOMS

Div1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((\sim y = 0) \Rightarrow \frac{x}{y} \in \mathbb{R})$.

Div2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((\sim y = 0) \Rightarrow (\frac{x}{y} = z \Leftrightarrow x = y \cdot z))$.

DISTRIBUTIVE LAW

DIS. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x \cdot (y + z) = x \cdot y + x \cdot z$

ZERO AND ONE AXIOMS

ZO1. $(\forall x \in \mathbb{R})x + 0 = x$

ZO2. $(\forall x \in \mathbb{R})x \cdot 1 = x$

ZO3. $\sim 0 = 1$

THE AXIOMS OF ARITHMETIC, PART II

ORDER AXIOMS

Or1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x > y \Leftrightarrow y < x)$

Or2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x \leq y \Leftrightarrow (x < y \vee x = y))$

Or3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x \geq y \Leftrightarrow y \leq x)$

Or4. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((x < y \vee x > y) \vee x = y)$

Or5. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \sim (x < y \wedge x \geq y)$

Or6. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((x < y \wedge y < z) \Rightarrow x < z)$

Or7. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x < y \Rightarrow x + z < y + z)$

Or8. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((x < y \wedge z > 0) \Rightarrow x \cdot z < y \cdot z)$

AXIOMS ABOUT INTEGERS AND NATURAL NUMBERS

NZ1. $(\forall x \in \mathbb{N})x \in \mathbb{Z}$

NZ2. $(\forall x \in \mathbb{Z})x \in \mathbb{R}$

NZ3. $0 \in \mathbb{Z}$

NZ4. $1 \in \mathbb{N}$

NZ5. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x + y \in \mathbb{Z}$

NZ6. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x - y \in \mathbb{Z}$

NZ7. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x \cdot y \in \mathbb{Z}$

NZ8. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})x + y \in \mathbb{N}$

NZ9. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})x \cdot y \in \mathbb{N}$

NZ10. $(\forall x \in \mathbb{Z})(x \in \mathbb{N} \Leftrightarrow x > 0)$

NZ11. $(\forall x \in \mathbb{Z})(x \leq 0 \vee x \geq 1)$

NZ12. Let u be a variable, and let $P(u)$ be a formula that contains no u-quantifiers. Then

$$(\exists u \in \mathbb{N})P(u) \Rightarrow ((\exists u \in \mathbb{N})(P(u) \wedge (\forall v \in \mathbb{N})(P(v) \Rightarrow v \geq u)))$$

11.4 Some horrible examples of arithmetic proofs, whitout shortcuts

I am now going to show you a couple of examples of proofs in arithmetic written fully according to our rules and using the axioms. In reality, nobody ever writes proof that way, and I will not expect you to do it either. But it is important that you should know that, when you write proofs in a shorter, more narrative form, there is supposed to be a truly formal proof behind what you wrote. You skip lots of steps ***because you know that the steps could be put in if necessary.*** If what you wrote is unclear, confusing, or lacking in precision, then I will tell you so. If you insist that your proof is O.K., that what you wrote is perfectly clear to you, then I will use the ultimate criterion to settle the question: I will ask you to write a formal proof. If you cannot do it, then you probably don't have a proof. (I am being careful here! It's also possible that you do have a proof but you do not know how to do it formally. Maybe you just do not know how to say certain things in formal language, for example.) But the criterion I have given you works in the other direction: ***if you give me a formal proof, and all the steps are correctly justified, then I cannot refuse to accept it***.

When I give you the rules and the axioms, I am making a commitment: **as long as you follow the rules and use the axioms I promise to accept your proofs as valid**. *I cannot "change the rules in the middle of the game" by saying, for example, "you have just used Rule $\Rightarrow_{use}$, but I don't accept this because I do not know that Rule $\Rightarrow_{use}$ is valid; you say it is, but why should I believe you? How do I know the rule is valid?" The answer you should give if I say that is "It was* ***you*** *who gave me these rules, so now you have to accept whatever I do following the rules."*

As you will see, these fully formal proofs are awful, extremely long, and very boring. After we have gone through the unpleasantness of writing fully

formal proofs, you will be ready for the next step, namely, finding ways to shorten what we write and making it more lively and readable. This will lead us to ur next chapter: shortcuts and how to skip millions of steps.

11.4.1 An example of a formal proof: $1 > 0$

You know, of course, that $1 > 0$. But none of our axioms says exactly that. So we should be able to prove it. Here we go.

Proof that $1 > 0$***.***

Step 1.	$1 \in \mathbb{N}$	[Axiom NZ4]
Step 2.	$(\forall x \in \mathbb{N}) x \in \mathbb{Z}$	[Axiom NZ2]
Step 3.	$1 \in \mathbb{Z}$	[Rule $\forall_{use}$, from 1 & 2]
Step 4.	$(\forall x \in \mathbb{Z})(x \in \mathbb{N} \Leftrightarrow x > 0)$	[Axiom NZ10]
Step 5.	$1 \in \mathbb{N} \Leftrightarrow 1 > 0$	[Rule $\forall_{use}$, from 3 & 4]
Step 6.	$1 \in \mathbb{N} \Rightarrow 1 > 0$	[Rule $\Leftrightarrow_{use}$, from 5]
Step 7.	$1 > 0$	[Rule $\Rightarrow_{use}$, from 1 & 6]

END

11.4.2 A second example of a formal proof

Let us prove the ***cancellation law of addition***:

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x + z = y + z \Rightarrow x = y) \ .$$

Again, this is something that you know is true, but it is not one of our axioms, so either we can prove it or we need a new axiom.

The intuitive idea is trivial: we assume that $x + z = y + z$, subtract z from both sides (or add $-z$ to both sides), and get $x = y$. Let us write this down as a formal proof,

Step 1.	Let $a \in \mathbb{R}$ be arbitrary.	[Declaration]
Step 2.	Let $b \in \mathbb{R}$ be arbitrary.	[Declaration]
Step 3.	Let $c \in \mathbb{R}$ be arbitrary.	[Declaration]
Step 4.	Assume $a + c = b + c$.	[Assumption]
Step 5.	Let $d = 0 - c$.	[Declaration]
Step 6.	$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x - y = z \Leftrightarrow x = y + z)$.	[Ax. Sub2]
Step 7.	$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x - y \in \mathbb{R}$	[Axiom Sub2]
Step 8.	$0 \in \mathbb{Z}$	[Axiom NZ3]
Step 9.	$(\forall x \in \mathbb{Z}) x \in \mathbb{R}$	[Axiom NZ]
Step 10.	$0 \in \mathbb{R}$	[Rule $\forall_{use}$, from 8 & 9]

Step 11. $(\forall y \in \mathbb{R})0 - y \in \mathbb{R}$ [Rule $\forall_{use}$ from 7 & 10]
Step 12. $0 - c \in \mathbb{R}$ [Rule $\forall_{use}$ from 3 & 11]
Step 13. $d \in \mathbb{R}$ [Rule SEE, from 5 & 12]
Step 14. $(\forall x)x = x$ [Axiom EEI]
Step 15. $d = d$ [Rule SEE, from 14]
Step 16. $0 - c = d$ [Rule SEE, from 15 & 5]
Step 17. $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(0 - y = z \Leftrightarrow 0 = y + z)$. [Rule $\forall_{use}$ fr.6 & 10]
Step 18. $(\forall z \in \mathbb{R})(0 - c = z \Leftrightarrow 0 = c + z)$. [Rule $\forall_{use}$ from 3 & 17]
Step 19. $0 - c = d \Leftrightarrow 0 = c + d$. [Rule $\forall_{use}$ from 13 & 18]
Step 20. $0 - c = d \Rightarrow 0 = c + d$. [Rule $\Leftrightarrow_{use}$ from 19]
Step 21. $0 = c + d$. [Rule $\Rightarrow_{use}$ from 16 & 20]
Step 22. $(\forall x \in \mathbb{R})x + 0 = x$. [Axiom ZO1]
Step 23. $a + 0 = a$. [Rule $\forall_{use}$ from 1 & 22]
Step 23. $a + (c + d) = a$. [Rule SEE from 21 & 23]
Step 24. $b + 0 = b$. [Rule $\forall_{use}$ from 2 & 22]
Step 25. $b + (c + d) = b$. [Rule SEE from 21 & 24]
Step 26. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x + y) + z = x + (y + z)$. [Ax. Add3]
Step 27. $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(a + y) + z = a + (y + z)$. [Rule $\forall_{use}$ from 1 & 26]
Step 28. $(\forall z \in \mathbb{R})(a + c) + z = a + (c + z)$. [Rule $\forall_{use}$ from 3 & 27]
Step 29. $(a + c) + d = a + (c + d)$. [Rule $\forall_{use}$ from 13 & 28]
Step 30. $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(b + y) + z = b + (y + z)$. [Rule $\forall_{use}$ from 2 & 26]
Step 31. $(\forall z \in \mathbb{R})(b + c) + z = b + (c + z)$. [Rule $\forall_{use}$ from 3 & 30]
Step 32. $(b + c) + d = b + (c + d)$. [Rule $\forall_{use}$ from 13 & 31]
Step 33. $(b + c) + d = b$. [Rule SEE from 25 & 32]
Step 34. $(a + c) + d = b$. [Rule SEE from 4 & 33]
Step 35. $a = b$. [Rule SEE from 23 & 34]
Step 36. $a + c = b + c \Rightarrow a = b$. [Rule $\Rightarrow_{get}$ from 4 & 35]
Step 37. $(\forall z \in \mathbb{R})(a + z = b + z \Rightarrow a = b)$. [Rule $\forall_{get}$ from 3 & 36]
Step 38. $(\forall z \in \mathbb{R})(\forall y \in \mathbb{R})(a + z = y + z \Rightarrow a = y)$. [Rule $\forall_{get}$ from 2 & 37]
Step 39. $(\forall x \in \mathbb{R})(\forall z \in \mathbb{R})(\forall y \in \mathbb{R})(x + z = y + z \Rightarrow x = y)$. [Rule $\forall_{get}$ from 1 & 38]

END

11.4.3 A third example of a formal proof

Let us prove that

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \sim (x > y \wedge x \leq y) \ .$$

This is completely obvious. In addition, this is almost the same as Axiom Or5. Bit it isn't *exactly* Axiom Or5, so it needs a proof. (As we will see soon, once you allow reasonable shortcuts, the proof can just be done in one or two lines, but at this point I want you to see what a true formal proof is like.)

Step 1.	$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \sim (x < y \wedge x \geq y)$	[Axiom Or5]
Step 2.	Let $a \in \mathbb{R}$ be arbitrary.	[Declaration]
Step 3.	Let $b \in \mathbb{R}$ be arbitrary.	[Declaration]
Step 4.	Assume $a > b \wedge a \leq b$.	[Assumption]
Step 5.	$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x > y \Leftrightarrow y < x)$.	[Axiom Or1]
Step 6.	$(\forall y \in \mathbb{R})(a > y \Leftrightarrow y < a)$.	[Rule $\forall_{use}$, from 5]
Step 7.	$a > b \Leftrightarrow b < a)$.	[Rule $\forall_{use}$, from 6]
Step 8.	$a > b \Rightarrow b < a$.	[Rule $\Leftrightarrow_{use}$, from 7]
Step 9.	$a > b$.	[Rule $\wedge_{use}$, from 4]
Step 10.	$b < a$.	[Rule $\Rightarrow_{use}$, from 8 & 9]
Step 11.	$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x \geq y \Leftrightarrow y \leq x)$.	[Axiom Or3]
Step 12.	$(\forall y \in \mathbb{R})(b \geq y \Leftrightarrow y \leq b)$.	[Rule $\forall_{use}$, from 11]
Step 13.	$b \geq a \Leftrightarrow a \leq b$.	[Rule $\forall_{use}$, from 12]
Step 14.	$a \leq b \Rightarrow b \geq a$.	[Rule $\Leftrightarrow_{use}$, from 13]
Step 15.	$a \leq b$.	[Rule $\wedge_{use}$, from 14]
Step 16.	$b \geq a$.	[Rule $\Rightarrow_{use}$, from 14 & 15]
Step 17.	$b < a \wedge b \geq a$.	[Rule $\wedge_{get}$, from 10 & 16]
Step 18.	$(\forall y \in \mathbb{R}) \sim (x < a \wedge a \geq y)$	[Rule $\forall_{use}$, from 1]
Step 19.	$\sim (b < a \wedge a \geq b)$	[Rule $\forall_{use}$, from 18]
Step 20.	$(b < a \wedge b \geq a) \wedge \sim (b < a \wedge a \geq b)$	(contradiction) [Rule $\wedge_{get}$, from 17 & 19]
Step 21.	$\sim (a > b \wedge a \leq b)$.	[Rule 2, from 4 & 20]
Step 22.	$(\forall y \in \mathbb{R}) \sim (a > y \wedge a \leq y)$.	[Rule $\forall_{get}$, from 3 & 21]
Step 23.	$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \sim (x > y \wedge x \leq y)$.	[Rule $\forall_{get}$, from 2 & 22]

END

These proofs were truly horrible, weren't they? It took us 39 steps and 23 steps to do things that could have been done in just a couple of lines by writing more informally! Why do we have to go through this? I have already given you some reasons. ***Tune in to next week's handout for even more reasons, and also more examples.***

12 The Principle of Mathematical Induction and the Well-Ordering Principle

So far, we have not discussed or used Axiom NZ12. It turns out that this axiom is extremely imprtant, and most interesting properties of natural numbers require this axiom. In other words, without this axiom there is very little that you can prove, Suppose, for example, that you want to prove that

Every natural number is even or odd.

or, in symbolic notation,

$$(\forall n \in \mathbb{N})((\exists k \in \mathbb{Z})(n = 2k) \vee (\exists k \in \mathbb{Z})(n = 2k + 1)) .$$

How can you prove that? It turns out that ***you cannot do it unless you use Axiom NZ12***. Let me show you how this works.

To prove that "Every natural number is even or odd" you can do the following:

1. You try to prove this by contradiction.
2. So you assume that the desired conclusion is not true.
3. This means that there exists a natural number n which is neither even nor odd.
4. Could n be 1? The answer is "no", because 1 is odd.
5. So $n > 1$.
6. Let $\nu_1 = n - 1$. Then ν_1 is also a natural number. (Notice that here we have used the fact that $n > 1$. If n was 1 then ν_1 would have been 0, which is ***not*** a natural number.)
7. Could ν_1 be even? The answer is "no", because if ν_1 was even, then n would be odd.
8. Could ν_1 be odd? Again, the answer is "no", because if ν_1 was odd, then n would be even.
9. So ν_1 is neither even nor odd.
10. Now we can repeat the same argument: let $\nu_2 = \nu_1 - 1$ (that is, $\nu_2 = n-2$); then ν_2 is neither even nor odd; let $\nu_3 = \nu_2 - 1$, then ν_3 is neither even nor odd; let $\nu_4 = \nu_3 - 1$, then ν_4 is neither even nor odd, and so on.
11. This process has to stop at some point, because eventually we will get $\nu_k = 1$. (This will happen for $k = n - 1$.) And, when we get there, we will have shown that 1 is neither even nor odd. But we know that 1 is odd. So we got a contradiction.**END OF PROOF**

Now, if you look at the above proof, it looks perfectly sound, and it seems that we have never used Axiom NZ12. Yet, if you think about this for a few minutes, you will see that there is one thing in our argument that is hard to justify precisely. What is the precise meaning of the statement that "this process has to stop"? And how do we justify this in terms of our axioms?

The answer to these questions is that there is only one way to make the argument precise and rigorous, and it is by using Axiom NZ12. (If you do not believe me, try to write a formal version of the above proof, without using Axiom NZ12. You should not be able to do it!)

What does Axiom NZ12 say, and how do we use it?

Axiom NZ12 is the "well-ordering principle". It says, basically, that any time you single out a property of natural numbers, ***if there exists a natural number that has the property, then there is a smallest one.***

Below, I am going to give you several different versions of this principle, using symbolic language and plain English, talking about predicates or about sets. But before I do that let me go back to our theorem, and write down the proof using Axiom NZ12.

Theorem 1. *Every natural number is even or odd. (In other words,* $(\forall n \in \mathbb{N})((\exists k \in \mathbb{Z})(n = 2k) \vee (\exists k \in \mathbb{Z})(n = 2k + 1))$ *.)*

Proof:

1. We will prove this by contradiction.
2. So we assume that the desired conclusion is not true.
3. This means that there exists a natural number u which is neither even nor odd.
4. Let us apply Axiom NZ12 to the predicate "u is neither even nor odd." In view of Step 3, there exists a $u \in \mathbb{N}$ for which the predicate is true. Axiom NZ12 then tells us that there exists a smallest such u.
5. Pick a smallest natural number u which is neither even nor odd, and call it a.
6. Then $a \in \mathbb{N}$, a is not even, a is not odd, and there is no $b \in \mathbb{N}$, such that b is not even, b is not odd, and $b < a$.

7. Can a be 1? No, because 1 is odd, and a isn't.
8. So $a > 1$.
9. Then $a - 1 \in \mathbb{N}$. , 10. Could $a - 1$ be even? No, because if $a - 1$ was even, then a would be odd.
11. Could $a - 1$ be odd? No, because if $a - 1$ was odd, then a would be even.
12. So $a - 1 \in \mathbb{N}$ (Step 9) and $a - 1$ is neither even nor odd (Steps 10, 11).
13. So we have reached a contradiction because, on the one hand $a - 1$ is a natural number which is neither even nor odd, and $a - 1 < a$, but in Step 6 we observed that such a number cannot exist. **END OF PROOF**

Now let us try another example. Let us prove

Theorem 2. *Every natural number greater than* 1 *has a prime divisor. In other words,*

$(\forall n \in \mathbb{N})(n > 1 \Rightarrow (\exists p \in \mathbb{N})(p \text{ is prime} \wedge (\exists k \in \mathbb{N})n = k \cdot p))$.

Proof:

1. We try to prove our result by contradiction.
2. So we assume that the desired conclusion is not true.
3. This means that there exists a natural number u such that $u > 1$ and u does not have any prime divisors.
4. Let us apply Axiom NZ12 to the predicate "$u > 1$ and u is does not have a prime divisor". In view of Step 3, there exists a $u \in \mathbb{N}$ for which the predicate is true. Axiom NZ12 then tells us that there exists a smallest such u.
5. Pick a smallest natural number u such that $u > 1$ and u does not have a prime divisor, and call it a.
6. Then $a \in \mathbb{N}$, $a > 1$, a does not divisible a prime divisor, and there does not exist a $b \in \mathbb{N}$ such that $b > 1$, b does not have a prime divisor, and $b < a$.
7. Could a be prime? No, because a is not divisible by any prime, whereas if a was prime then a would be divisible by a prime, namely, a.
8. Since a is not prime, it follows from the definition of "prime" and the fact that $a > 1$ that we may pick two natural numbers j, k such that $a = j \cdot k$, $j > 1$ and $k > 1$. (***Warning! The fact that*** $a > 1$ ***is crucial here! Make sure you see how this fact is being used.***)
9. The number j is a natural number.
10. Also, $j < a$, because $a = j \cdot k$ and $k > 1$.

11. Moreover, we know that $j > 1$.
12. Could j have a prime divisor? No, because if j was divisible by a prime p, then a would also be divisible by p, since $a = j \cdot k$.
13. So j is a natural number such that $j > 1$, j does not have a prime divisor, and $j < a$. But is Step 6 we observed that such a number cannot exist. So we hace reached a contradiction. **END OF PROOF**

Theorem 3. *Every natural number greater than* 1 *is a product of prime numbers. In other words,*

$$(\forall n \in \mathbb{N})(n > 1 \Rightarrow (\exists k \in \mathbb{N})(\exists p_1, \ldots, p_k \in \mathbb{N})(n = p_1 p_2 \cdots p_k \\ \wedge (\forall j \in \mathbb{N})((1 \leq j \wedge j \leq k) \Rightarrow p_j \text{ is prime}))$$

Proof:

1. We try to prove our result by contradiction.
2. So we assume that the desired conclusion is not true.
3. This means that there exists a natural number u such that $u > 1$ and u is not a product of primes.
4. Let us apply Axiom NZ12 to the predicate "$u > 1$ and u is not a product of primes". In view of Step 3, there exists a $u \in \mathbb{N}$ for which the predicate is true. Axiom NZ12 then tells us that there exists a smallest such u.
5. Pick a smallest natural number u such that $u > 1$ and u is not a prodeuct of primes, and call it a.
6. Then $a \in \mathbb{N}$, $a > 1$, a is not a product of primes, and there does not exist a $b \in \mathbb{N}$ such that $b > 1$, b is not a product of primes, and $b < a$.
7. Could a be prime? No, because if a was prime then a would be product of primes (with just one factor).
8. Since a is not prime, it follows from the definition of "prime" and the fact that $a > 1$ that we may pick two natural numbers j, k such that $a = j \cdot k$, $j > 1$ and $k > 1$. (***Warning! The fact that*** $a > 1$ ***is crucial here! Make sure you see how this fact is being used.***)
9. The numbers j, k are natural numbers.
10. Also, $j < a$, because $a = j \cdot k$ and $k > 1$.
11. Similarly, $k < a$, because $a = j \cdot k$ and $j > 1$.
12. Moreover, we know that $j > 1$ and $k > 1$ and
13. Is it possible that j is not a product of primes? No! Why? Because if j was not a product of primes then we would have: $j \in \mathbb{N}$, $j > 1$, $j < a$, and j is not a product of primes. But in Step 6 we observed that such a number cannot exist. So j is a product of primes.

14. Similarly, k is a product of primes.
15. Since j and k are both products of primes, a is also a product of primes, because $a = j \cdot k$. But in Step 6 we said that a is not a product of primes, So we hace reached a contradiction. **END OF PROOF**

Theorem 4. *For all natural numbers n, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.*

Proof.

The basic idea is this: ***we will show that,***

(A1) the formula we are trying to prove is true for $n = 1$***;***

(A2) if the formula we are trying to prove is true for a particular n***, then it is true for*** $n + 1$***.***

Once we have done these two things, Axiom NZ12 will enable us to prove that the formula is true for all $n \in \mathbb{N}$, as follows. Let us call those n's for which the formula isn;t true the "bad" n's. We want to prove that there aren't any bad n's. Suppose there existed a bad n. Then Axiom NZ12 tell us that there exists a smallest bad n. Could this smallest bad n be 1? No, because (A1) tells us that 1 is not bad. But then $n > 1$, so $n - 1 \in \mathbb{N}$. Could $n - 1$ be bad? No, because n is the smallest bad number. So $n - 1$ isn;t bad. But this means that our formula holds for $n - 1$. By (A2), the formula holds for n. So n isn;t bad either! This contradicts the fact that n is bad, and our proof is finished.

So now we are going to prove (A1) and (A2). Statement (A1) is easy, because it just says that

$$\sum_{i=1}^{1} i = \frac{1(1+1)}{2},$$

which is obviously true, since bith sides are equal to 1.

Now we prove (A2), which is a little bit harder. Before we actually do the proof, let us look at a few examples. Why is is true that "if the formula holds for $n = 4$ then it holds for $n = 5$? Let us prove it. We want to prove that

$$\sum_{i=1}^{5} i = \frac{5(5+1)}{2},$$

assuming that

$$\sum_{i=1}^{4} i = \frac{4(4+1)}{2}\,.$$

Notice that

$$\sum_{i=1}^{5} i = 5 + \sum_{i=1}^{4} i\,.$$

So using the assumption that $\sum_{i=1}^{4} i = \frac{4(4+1)}{2}$, we deduce

$$\sum_{i=1}^{5} i = 5 + 4(4+1)/2\,,$$

and this is equal to $5(5+1)/2$. (Why? Well, you can compute $4(4+1)/2$, and find that it is equal to 10, while on the other hand $5(5+1)/2 = 15$, so indeed $5 + 4(4+1)/2 = 5(5+1)/2$. But this is not the nicest way to do it, because if you try to use the same method to show, say, that $395 + 394(394+1)/2 = 395(395+1)/2$, you would have to do a lot of computing. So it is much better to compute $5 + 4(4+1)/2$ "without using the fact that 4 is 4". What I mean by this weird statement is, write

$$5 + 4(4+1)/2 = n + 1 + \frac{n(n+1)}{2}$$

where n happens to be 4, but compute it forgetting that $n = 4$. The result is

$$n+1+\frac{n(n+1)}{2} = \frac{2(n+1)}{2} + \frac{n(n+1)}{2} = \frac{2(n+1)+n(n+1)}{2} = \frac{(n+1)(n+2)}{2}\,.$$

When $n = 4$ this gives us $5 + 4(4+1)/2 = 5(5+1)/2$, but the formula also works for all values of n. For example, for $n = 394$, it tells us that

$$395 + 394(394+1)/2 = 395(395+1)/2\,,$$

without having to compute the values of both sides.)

The proof of (A2) in general n is exactly as we have just indicated, Assume that the formula we want is true for n, i.e., that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\,.$$

Let us prove that it is true for $n+1$. For this purpose, we compute $\sum_{i=1}^{n+1} i$, and find

$$\sum_{i=1}^{n+1} i = n+1+\sum_{i=1}^{n} i = n+1+\frac{n(n+1)}{2}\,,$$

and we already know that $n+1+\frac{n(n+1)}{2} = \frac{(n+1)(n+2)}{2}$. So we have proved that $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$, which is exactly the formula we wanted, with $n+1$ instead of n. This was proved under the assumption that our formula holds for n. So we have proved (A2).

Summarizing: we have proved (A1) and (A2), and we have proved that if we have (A1) and (A2) then our conclusion follows. So we have finished proving our conclusion.

Before we go on, here is a precise statement of the well-ordering principle, i.e., Axiom NZ12. I will state it for you in six different ways.

THE WELL-ORDERING PRINCIPLE

(predicate version, written in symbolic notation)

NZ12. Let u be a variable, and let $P(u)$ be an expression having u as a free variable. Then

$$(\exists u \in \mathbb{N})P(u) \Rightarrow ((\exists u \in \mathbb{N})(P(u) \wedge (\forall v \in \mathbb{N})(P(v) \Rightarrow v \geq u)))$$

THE WELL-ORDERING PRINCIPLE

(predicate version, written in ordinary English)

NZ12. Suppose we are given a property that particular objects may or may not have. Suppose there exists a natural number that has the property. Then there exists a natural number which is the smallest of all the natural numbers having the property.

THE WELL-ORDERING PRINCIPLE
(set version, partially written in symbolic notation)

NZ12. Let S be a set of natural numbers. Then

$$((\exists u)u \in S) \Rightarrow ((\exists u)(u \in S \wedge (\forall v)(v \in S \Rightarrow v \geq u)))$$

THE WELL-ORDERING PRINCIPLE
(set version, partially written in symbolic notation in a slightly different way)

NZ12. Let S be a set of natural numbers. Then

$$S \neq \emptyset \Rightarrow ((\exists u)(u \in S \wedge (\forall v)(v \in S \Rightarrow v \geq u)))$$

THE WELL-ORDERING PRINCIPLE
(set version, completely written in symbolic notation)

NZ12. $(\forall S)((S \subseteq \mathbb{N} \wedge S \neq \emptyset) \Rightarrow ((\exists u)(u \in S \wedge (\forall v)(v \in S \Rightarrow v \geq u))))$

THE WELL-ORDERING PRINCIPLE
(set version, written in ordinary English)

NZ12. Every nonempty set of natural numbers has a smallest member.

Proofs that use Axiom NZ12 are called "proofs by induction" or "proofs by well-ordering". More precisely, a "proof by induction" is a proof in which, in order to prove that something is true for all $n \in \mathbb{N}$, we establish

(A1) that the statement we are trying to prove is true for $n = 1$;

(A2) that ***if*** the statement we are trying to prove is true for a particular n ***then*** it is true for $n + 1$.

So our proof of Theorem 4 is a proof by induction, but the proofs of Theorem 1, 2, and 3 are proofs by well-ordering. As I showed in the specific example of our proof of Theorem 4, any time you have a proof by induction you can always reword it as proof by well-ordering.

The book presents what the authors call "The Principle of Mathematical Induction (PMI)" on page 92 and "The Principle of Complete Induction (PCI)" on page 104. It then also discusses the well-ordering principle, on page ????

My advice is: **use well-ordering all the time**. It is much easier, and you do not need to remember different forms of "induction". In some cases, it may be easy to do a proof by induction (i.e., to prove (A1) and (A2)), so in those cases you may find it convenient to do it that way, but even in those cases well-ordering will usuallhy work equally well.

Naturally, you are free to use induction as presented in the book, if you like it that way. But, as I said, I do not recommend that.

Here is one more example. Let us prove

Theorem 5. *If $x \in \mathbb{R}$ and $x \geq 0$, then $(1+x)^n \geq 1+nx$ for every $n \in \mathbb{N}$. (That is, $(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})(1+x)^n \geq 1+nx$.)*

Proof.
Since we want to prove a universal sentence ("for all x ..."), we start with

1. Let x be an arbitrary real number.

Now we want to prove $(\forall n \in \mathbb{N})(1+x)^n \geq 1+nx$. This is the kind of statement for which the well-ordering principle is going to help us. So we

2. Assume that "$(\forall n \in \mathbb{N})(1+x)^n \geq 1+nx$" is not true.
3. Then there exists an $n \in \mathbb{N}$ such that $(1+x)^n < 1+nx$.
4. By the well-ordering principle, there exists a smallest $n \in \mathbb{N}$ such that $(1+x)^n < 1+nx$.
5. Could n be 1? No, because if n was 1 then the condition "$(1+x)^n < 1+nx$" would say that "$1+x < 1+x$", which isn't true.
6. So $n > 1$.
7. Then $n-1 \in \mathbb{N}$.

8. Since n was the smallest of all natural numbers that satisfy the inequality $(1+x)^n < 1+nx$, and $n-1$ is a smaller natural number, it follows that

$$(1+x)^{n-1} \geq 1 + (n-1)x\,.$$

9. Multiply both sides of the above inequality by $1+x$. The result is

$$(1+x)^n \geq (1+x)(1+(n-1)x)\,.$$

10. But

$$\begin{aligned}(1+x)(1+(n-1)x) &= 1 + x + (n-1)x + (n-1)x^2 \\ &= 1 + nx + (n-1)x^2 \\ &\geq 1 + nx\,.\end{aligned}$$

So

$$(1+x)(1+(n-1)x) \geq 1 + nx\,.$$

11. Then

$$(1+x)^n \geq 1 + nx\,.$$

12. We have shown in Step 12 that $(1+x)^n \geq 1+nx$, while in Step 5 we said that $(1+x)^n < 1+nx$. So we have shown that $(\sim((1+x)^n < 1+nx)) \wedge (1+x)^n < 1+nx$, which is a contradiction.

13. Hence $(\forall n \in \mathbb{N})(1+x)^n \geq 1+nx$.

14. Since x was an arbitrary real number, we can conclude that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})(1+x)^n \geq 1+nx\,.$$

END OF PROOF

Two questions about the above proof. Exactly where was the hypothesis that $x \geq 0$ used? Would it be possible to replace this condition by a more general one, such as, for example, x an arbitrary real number? What is the best you can do? (That is, can you describe the set of ***all*** the xs for which the assertion of the previous theorem is true?)